Federal Office
for Information Security

Status of quantum computer development

Entwicklungsstand Quantencomputer

Document history

Version	*Date*	*Editor*	*Description*
1.0	May 2018		Document status after main phase of project
1.1	July 2019		First update containing both new material and improved readability.
1.2	June 2020		Second update containing new algorithmic developments, details summarized in Reference [WSL+20]
2.0	August 2023		First major revision of previous study. Changes include a restructuring, and an incorporation of progressing hardware and novel NISQ developments.
2.1	August 2024		First update of the revised study. Major updates in the status of fault-tolerant quantum computing with several technical obstacles cleared.

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Email: qc@bsi.bund.de
Internet: https://www.bsi.bund.de

Introduction

This study discusses the current state of affairs in the theoretical aspects and physical implementation of quantum computing, with a focus on applications in cryptanalysis. It is designed to be an orientation for scientists with a connection to one of the fields involved—such as mathematicians, computer scientists. These will find the treatment of their own field slightly superficial but benefit from the discussion in the other sections. The executive summary and the conclusions to each chapter provide actionable information to decision makers.

Authors

Frank K. Wilhelm, Forschungszentrum Jülich

Rainer Steinwandt, University of Alabama in Huntsville, USA

Daniel Zeuch, Forschungszentrum Jülich

Paul Lageyre, Forschungszentrum Jülich

Susanna Kirchhoff, Forschungszentrum Jülich

Previous authors

Jurek Frey, Forschungszentrum Jülich

Brandon Langenberg, Florida Atlantic University, USA

Per J. Liebermann, Saarland University

Anette Messinger, Saarland University

Peter K. Schuhmacher, Saarland University

Aditi Misra-Spieldenner, Saarland University

Copyright

BSI-Reference

BSI Title: Aktualisierung der Studie „Entwicklungsstand Quantencomputer“

BSI Project Number: 477

Index of Figures

Index of Tables

PART I: Synopsis and introduction

In this first part, we provide an executive summary of the study and define the underlying evaluation systems. To summarize, we introduce quantum computing and describe its relevance for cryptanalysis. Upon sketching the nature of quantum computing hardware and quantum algorithms, we discuss noteworthy recent developments and end with the study's conclusions. While the bulk of the study is composed in English, we provide both a German summary (Chapter 1) and an English summary (Chapter 2). Subsequently, Chapter 3 presents evaluation systems used for categorizing quantum hardware and algorithms.

1 Deutsche Zusammenfassung

1.1 Was ist ein Quantencomputer?

Heutige Computer behandeln Informationen gemäß den Gesetzen der klassischen Physik: Register und Speicherinhalte haben zu jedem Zeitpunkt einen einzigen Wert. Dies gilt ungeachtet der Tatsache, dass die Bauelemente eines Computers wie Transistoren auf den Gesetzen der Quantenphysik basieren.

In einem Quantencomputer wird die Information selbst quantenmechanisch behandelt: Register und Speicherinhalte können mehrere Werte gleichzeitig in Überlagerung enthalten, und Maschinenbefehle wirken sich simultan auf all diese Werte aus. Damit arbeitet bereits ein einziger Quantenprozessor intrinsisch hochgradig parallel, ohne parallelisierte Hardware wie mehrere Prozessorkerne zu benötigen. Dadurch lässt sich prinzipiell eine Quantenbeschleunigung, auch Quantenüberlegenheit genannt, erreichen. Diese bezeichnet die Realisierung von Berechnungen auf einem Quantencomputer, die von klassischen Rechnern nur unter exorbitantem Aufwand reproduziert werden können.

Nutzung dieser Parallelität erfordert allerdings Umgang mit dem probabilistischen Charakter der Quantenphysik und das Kompilieren von Algorithmen in quantenmechanisch erlaubte Gatter (Quantenschaltkreise). Aus diesem Grund erfordert die Nutzung der Quantenbeschleunigung zunächst die Entdeckung geeigneter Algorithmen. Zu diesen gehören bisher die schnelle Datenbanksuche, das Durchsuchen von Graphen, die Lösung linearer Gleichungssysteme, Anwendungen der schnellen Fouriertransformation einschließlich Faktorisierung und Berechnung diskreter Logarithmen, und die Simulation von Quantensystemen einschließlich Chemikalien und neuer Materialien, sowie Maschinenlernen und Optimierung. Für einige dieser Anwendungen, insbesondere die letztgenannten, ist die Quantifizierung der erreichbaren Quantenbeschleunigung noch Gegenstand aktueller Forschung. Quantencomputer sind – aufgrund der möglichen Anwendungen aber auch aufgrund der aufwändigen Hardware – auf der Ebene von Rechenzentrumstechnologie und Höchstleistungsrechnen anzusiedeln und keine Büro- oder gar mobile Technologie. Entsprechend sind die leistungsfähigsten Quantencomputer unserer Tage Großgeräte für Forschung und Entwicklung – sie erlauben die Entwicklung und Validierung von Algorithmen, sind aber (noch) nicht jenseits der Wissenschaft disruptiv.

Quantencomputer wurden zunächst als hypothetische, theoretische Konstruktion eingeführt. Inzwischen, nach mehr als 25 Jahren Entwicklung seit den ersten Laborexperimenten, konsolidiert sich das Feld der Hardwareplattformen. Zugriff auf Quantenprozessoren wird als Dienstleistung von mehreren Firmen angeboten, einige Hersteller verkaufen auch bereits on-premise Hardware an Rechenzentren. Obgleich noch in einem frühen Entwicklungsstadium, erlauben all diese Quantenprozessoren die Entwicklung und Evaluation von Quantenalgorithmen.

Der Stand des Gebietes kann als Ära der frühen Quantenüberlegenheit bezeichnet werden. Diese Überlegenheit wurde an mehreren Stellen für sehr spezielle Benchmarkingprobleme erreicht. Nach aktuellem Wissensstand sind die Anforderungen, um bei anwendungsorientierten Problemen Quantenüberlegenheit zu erreichen deutlich höher. Unsere Studie untersucht diese Fragestellung für die Kryptoanalyse.

1.2 Relevanz von Quantencomputern für die Kryptoanalyse

Ein Großteil der heute auf breiter Basis eingesetzten asymmetrischen kryptographischen Verfahren kann nicht mehr als sicher betrachtet werden, sobald die Faktorisierung großer Ganzzahlen und die Berechnung sogenannter diskreter Logarithmen effizient möglich ist. Dies erklärt das signifikante Interesse an Quantencomputern in der kryptoanalytischen Forschung – Peter Shor zeigte Mitte der 90er Jahre erstmals, dass beide Probleme asymptotisch effizient gelöst werden können, wenn ein hinreichend großer und verlässlicher Quantencomputer verfügbar ist. Die Effizienz der Shor-Algorithmen beruht unter anderem auf der geschickten Nutzung von quantenmechanischer Überlagerung mehrerer Werte, einer Technik, die mit klassischen Bits nicht realisierbar ist. Quantencomputer verwenden als elementare Einheit Quantenbits, kurz Qubits, bei denen den klassischen Werten 0 und 1 lediglich die Rolle von Basiswerten zukommt, und der Wert eines Qubits gewichtete Anteile beider Basiswerte simultan innehaben kann. In ähnlicher Weise

werden klassische Bitregister durch komplexe Quantenregister ersetzt, die effiziente hochdimensionale Berechnungen ermöglichen. Aus praktischer Sicht stellt sich die Frage, wie groß ein Quantencomputer sein muss, um real eingesetzte kryptographische Verfahren, etwa die RSA-Verfahren oder solche basierend auf elliptischen Kurven, zu gefährden. Hierzu ist eine genaue Analyse bekannter Quantenalgorithmen erforderlich. Die abstrakten Schritte eines Quantenalgorithmus müssen für das konkret angegriffene Verfahren (effizient) in Elementarschritte umgesetzt werden, die wiederum auf realer Hardware abbildbar sind.

Seit der Einführung von Peter Shors Verfahren im letzten Jahrhundert gab es algorithmische Forstschritte, die für konkrete Ressourcenabschätzungen relevant sind. Insbesondere Ergebnisse von Craig Gidney und Martin Ekerå sowie eine Faktorisierungsmethode von Oded Regev aus dem letzten Jahr sollten hier genannt werden. Ähnlich wie bei klassischen Verfahren scheint die Berechnung diskreter Logarithmen auf elliptischen Kurven und in endlichen Primkörpern quantenkryptoanalytische Unterschiede aufzuweisen: Shors Verfahren (und Verbesserungen hiervon) sind direkt auf alle kryptographisch gängig eingesetzten zyklischen Gruppen anwendbar, während eine Anpassung von Regevs Ansatz an die Berechnung diskreter Logarithmen auf elliptischen Kurven auf Unwägbarkeiten stößt. Detaillierte Kostenanalysen für relevante kryptographische Parameter sind in moderatem Umfang in der Literatur verfügbar, aber die Literatur zur Quantenressourcenoptimierung bleibt sehr aktiv und das praktische Potential der neuesten Ideen für effiziente Arithmetik bedarf noch weitergehender quantitativer Analyse. Es ist anzunehmen, dass die bislang veröffentlichten Quantenschaltkreise und der zur Fehlerbehandlung erforderliche Mehraufwand weiter optimiert werden können. Die bereits verfügbaren Arbeiten lassen es machbar erscheinen, die Shor-Algorithmen (oder ihre Erweiterungen) für kryptographisch interessante Parameterwahlen in Quantenschaltkreise moderater Komplexität zu übersetzen. Konkret werden nach aktuellem Forschungsstand für einen Angriff auf 2048 Bit RSA insgesamt $1.4 \cdot 10^{15}$ Elementarschritte auf 4098 logischen Qubits benötigt, (vgl. Kapitel 4); andere Trade-offs zwischen der Anzahl der Rechenschritte und der Anzahl der Qubits sind möglich. Wiederum nach aktuellem Forschungsstand für den diskreten Logarithmus auf einer elliptischen Kurve über 256 Bit werden etwa 10^{11} Rechenschritte auf 2330 logischen Qubits benötigt, vgl. Kapitel 4 (Table 4.6). Logische Qubits sollten nicht mit physikalischen Qubits verwechselt werden, deren Konzept und Bedeutung wir in Abschnitt 1.3 besprechen. Nach einer aktuellen Abschätzung werden 20.000.000 physikalische Qubits als hinreichend für einen Angriff auf 2048 Bit RSA mit einer Laufzeit von acht Stunden betrachtet [GE21].

Für die symmetrische Kryptographie bieten Quantencomputer ebenfalls neue kryptoanalytische Möglichkeiten, aber mit den momentan bekannten Algorithmen sind die Auswirkungen deutlich weniger spektakulär als im asymmetrischen Fall. Auch hier kann davon ausgegangen werden, dass die besten vorhandenen quantitativen Aussagen, etwa zur Schlüsselsuche bei AES-128, noch verbessert werden (es wurden bereits mehrere Optimierungen vorgeschlagen), aber eine Vergrößerung der Schlüssellänge auf 256 Bit erscheint momentan eine wirksame Gegenmaßnahme zu sein. Die Optimierung von Quantenschaltkreisen, um moderne Hashverfahren wie SHA-2 und SHA-3 anzugreifen, bleibt ein aktives Forschungsgebiet, aber die bekannten algorithmischen Ansätze zur Kollisions- und Urbildsuche mit Quantenrechnern sind noch immer ineffizient und vorrangig von akademischem Interesse. Weitere Quantenangriffe auf symmetrische Primitive sind bekannt, aber hierbei werden zum Teil Angriffsmodelle verwendet, die bei heute genutzten Implementierungen nicht realistisch sind.

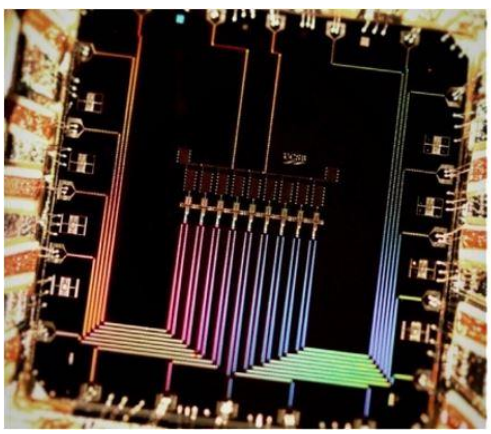
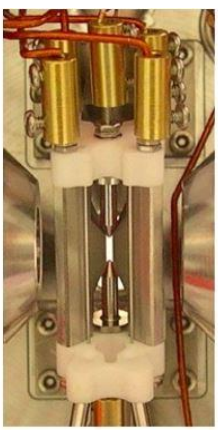
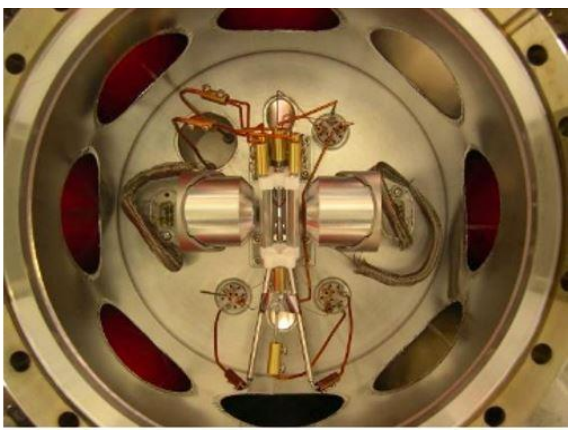

Abbildung 1.1: Die augenblicklich führenden Quantencomputing-Plattformen – mikroskopische Perspektive. Links: Prozessor bestehend aus integrierten supraleitenden Schaltkreisen. (Foto links: Julian Kelly, Google.) Mitte: Lineare Ionenfalle; Elektroden zum Fangen (Stäbe) und Linsen zum Einstrahlen von Lasern für Quantenlogik (links und rechts). Rechts: Die gleiche Ionenfalle eingebettet in ihre Vakuumapparatur. (Fotos mittig und rechts: Jürgen Eschner, Universität des Saarlandes.)

1.3 Hardware und Algorithmen für Quantencomputer

Die gesicherten Erkenntnisse über Quantenalgorithmen wären nicht relevant, würde nicht gleichzeitig Hardware entwickelt werden. Weltweit wird bei der Entwicklung von Hardwareplattformen eine Reihe sehr unterschiedlicher Ansätze verfolgt – etwa vergleichbar mit dem Übergang von mechanischen zu elektronischen Computern. Die augenblicklich führenden Plattformen (siehe Abbildung 1.1) sind

1. Ionenfallen – eine Plattform die u.a. mit der Technologie von Atomuhren verwandt ist.
2. Neutrale Atome in Lichtfeldern, typischerweise über hochangeregte Rydberg-Zustände gekoppelt
3. Integrierte Schaltkreise aus Supraleitern – eine Plattform, die Ähnlichkeit mit aktuellen Computerchips hat, jedoch aus anderen Materialien besteht und bei sehr tiefen Temperaturen betrieben wird. Hier ist vor allem eine spezielle Variante, nämlich das sogenannte zweidimensionale (2D) Transmon, ein Vorreiter.

Es wird eine Vielzahl weiterer Plattformen erforscht, die zwar im Augenblick weniger weit fortgeschritten sind, aber teils eine steile Entwicklung zeigen. Dazu gehören Donatoren in Silizium-Strukturen, Quantenpunkte in Halbleitern, gezielt dotierte künstliche Diamanten, auch Farbzentren genannt, und photonische Systeme. Es sei darauf hingewiesen, dass Technologien, die derzeit nicht in großem Umfang verfolgt werden, wie molekulare Qubits oder Elektronen, die auf Helium gefangen sind, in einer alten Version dieser Studie behandelt sind [WSL+20].

Die führenden Plattformen werden zunehmend in industriellen oder öffentlich-privaten Partnerschaften erforscht und entwickelt. Dies spiegelt einerseits die Notwendigkeit fortlaufender Grundlagenforschung wider, ermöglicht aber andererseits die Entwicklung von funktionalen und vielschichtigen integrierten Systemen mit Prototypcharakter. Leider sind Teile der industriellen Forschung als Geschäftsgeheimnisse nicht zur Bewertung zugänglich.

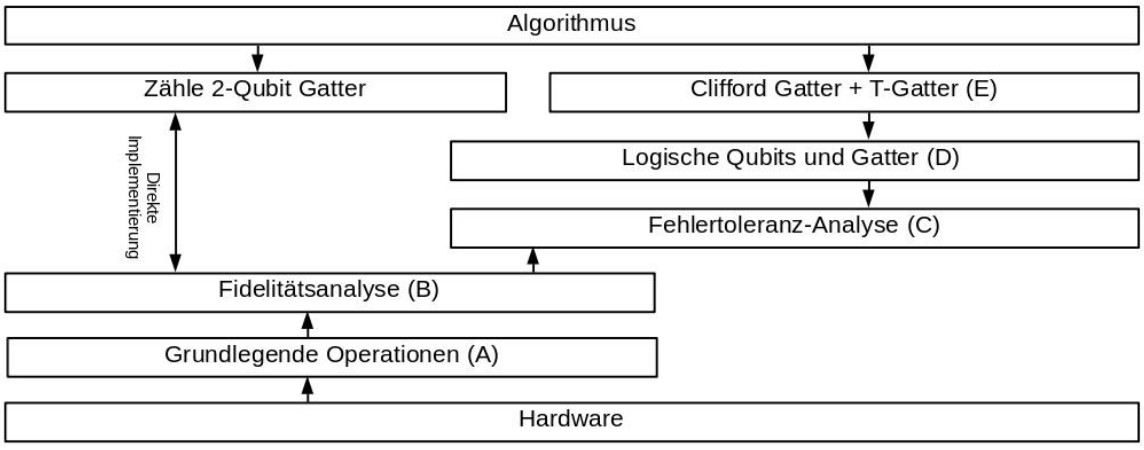

Abbildung 1.2: Abhängigkeitsgraph für Quantencomputer zwischen Algorithmen und Hardware. Daraus ergibt sich das hier verwendete Schichtenmodell zur Bewertung von Quantencomputerplattformen basierend auf NISQ [links, Stufen (A) und (B)] bzw. anhand demonstrierter Schritte zur Fehlertoleranz [rechts, Stufen (A) bis (E)]. Dieses Modell wird in Kapitel 3 im Detail eingeführt.

Die wichtigste strukturelle Herausforderung des Gebietes ist dabei die Fehleranfälligkeit von Quantencomputern. Diese geht über das rein Technologische hinaus und ist grundsätzlicher Natur – der besondere Glücksfall der geringen Fehleranfälligkeit von klassischen Digitalrechnern tritt hier nicht ein. Auf

der einen Seite zeigen belastbare Theorien, dass Quantencomputer kryptoanalytische Aufgaben bewältigen können, wenn sie aktiv fehlerkorrigiert werden. Auf der anderen Seite steht eine jüngere Erforschung kryptoanalytischer Anwendungen mit Quantencomputern, die nicht fehlerkorrigiert werden – auf diese Entwicklung gehen wir weiter unten ein. Ein konsistentes theoretisches Gerüst der Fehlerkorrektur wurde entwickelt. Seine praktische Umsetzung ist Gegenstand intensiver Forschung und erste Erfolge wurden bereits erzielt. Diese Fehlerkorrektur beeinträchtigt die grundsätzliche Effizienz von Quantencomputing nicht, ist aber trotzdem durch einen enormen Overhead gekennzeichnet – die *logischen* Qubits, die einen Algorithmus beschreiben, bestehen aus einer großen Zahl von Bauelementen, die *physikalische* Qubits darstellen. Auch bei großem Fortschritt ist davon auszugehen, dass der Bau eines leistungsfähigen fehlertoleranten Quantencomputers nicht nur eine wissenschaftlich-technische Herausforderung darstellt, sondern im Ergebnis eine Großanlage vom Umfang eines Rechenzentrums wäre.

Fehlerkorrektur ist dann effektiv, wenn alle Elemente der Hardware unter einer nativen Fehlerschwelle bleiben, welche je nach Methode und in den günstigsten Fällen zwischen 0.1% und 1% liegt. Dies wurde für Quantenspeicher inzwischen durch Google vollumfänglich experimentell validiert, siehe Kapitel **8.5.2.**. Forschungsergebnisse und die sie begleitenden Schlagzeilen können im Kontext der benötigten aktiven Fehlerkorrektur evaluiert werden. Diese Studie enthält darum ein Schichtenmodell zur Bewertung von Quantencomputer-Kandidaten, veranschaulicht in Abbildung 1.2. Es beginnt mit der Demonstration von Grundfunktionen (Schicht A) bis hin zur fehlertoleranten Implementierung von Algorithmen (Schicht E).

Wie Abbildung 1.3 verdeutlicht, ist das Feld an Plattformen dicht, und eine schnelle Veränderung der Bewertung wird erwartet – in der Tat, klare Fortschritte wurden innerhalb weniger Jahre erreicht (vgl. Abbildung 1.3 mit der äquivalenten Abbildung aus einer vorherigen Version dieser Studie [WSL+20]). Nach wie vor wird das Feld von Ionenfallen und 2D-Transmonen angeführt, in denen Schicht C demonstriert und Elemente von Schicht D realisiert werden. Die Fertigung supraleitender Schaltkreise ist, u.a. durch langjährige Erfahrung mit verwandten Silizium-Strukturen, technologisch weit entwickelt, und lässt sich gut optimieren. Dies führt zu verfügbaren Quantenprozessoren mit über 1100 Qubits. Diese größten Quantencomputer-Systeme beruhen dabei auf 2D-Transmonen, alternative Qubit-Schaltkreise werden aber weiterhin verfolgt und machen nennenswerte Fortschritte in der Entwicklung. Rydberg Atome haben bereits beeindruckende Zahlen fehlerkorrigierter Qubits realisiert, aber noch nicht alle Elemente von Schicht C demonstriert, dies wird jedoch aufgrund deren schneller Entwicklung und deren hoher Rekonfigurierbarkeit erwartet.

Auf die drei führenden Plattformen folgen Farbzentren, Halbleiter-Quantenpunkte und Silizium-Donatoren, sowie die Photonen. Letztgenannte weisen eine große Unsicherheit – dargestellt über die Breite in Abbildung 1.3 – im Entwicklungsstadium auf, was vor allem auf die bereits oben angesprochene Verschlossenheit von privaten Unternehmen in diesem Bereich zurückführen ist.

Darüber hinaus enthält diese Studie ein Schichtenmodell zur Einstufung von Quantenalgorithmen, das in Abbildung 1.4 gezeigt ist. Darin werden Algorithmen zunächst in zwei Kategorien unterteilt: einerseits diejenigen, deren Laufzeitverhalten für große Eingaben unbekannt sind und deren Leistung durch Heuristiken bestimmt werden müssen, andererseits solche Algorithmen, für die ein hinreichend solides Grundverständnis vorliegt, sodass eine Leistungsvorhersage für beliebig große Eingabewerte möglich ist. In beiden Fällen ist eine Analyse vonnöten, um die Relevanz des Algorithmus in Bezug auf derzeit eingesetzte kryptographische Verfahren vorherzusagen.

Vor der Etablierung fehlerkorrigierter Quantencomputer steht die Ära der “Noisy Intermediate-Scale Quantum (NISQ) Technologies", in der man die Fehler nicht korrigiert (aber ggf. durch hardwarenahe Methoden mitigiert) und darum nur auf eine begrenzte algorithmische Tiefe zurückgreifen kann, die durch die Fehlerwahrscheinlichkeit limitiert wird. In dieser Domäne werden native Freiheitsgrade der Hardware und alternative Programmierparadigmen kreativ genutzt. Die entstehenden Lösungen sind im Allgemeinen von heuristischer Natur und haben keinen mathematischen Konvergenzbeweis oder gar eine daraus abgeleitete Ressourcenanalyse. Um das Gebiet der NISQ-Algorithmen weiter beobachten zu können, schlagen wir ein separates Bewertungsschema vor. Da numerische Experimente in manchen Fällen Hinweise liefern können, sind NISQ-Algorithmen in unserer Algorithmus-Bewertung häufig Kandidaten für den “linken Zweig” in Abbildung 1.4. Die geringe vorliegende Evidenz lässt bisher keine abschließende Bewertung zu, erlaubt aber die vorsichtige Vermutung geringer Relevanz für die Kryptoanalyse. Da dieses Gebiet weniger klar gegliedert ist als fehlertolerantes Quantencomputing, müssten hier etwaige disruptive Algorithmen direkt nach dem Passieren von Schicht B evaluiert werden.

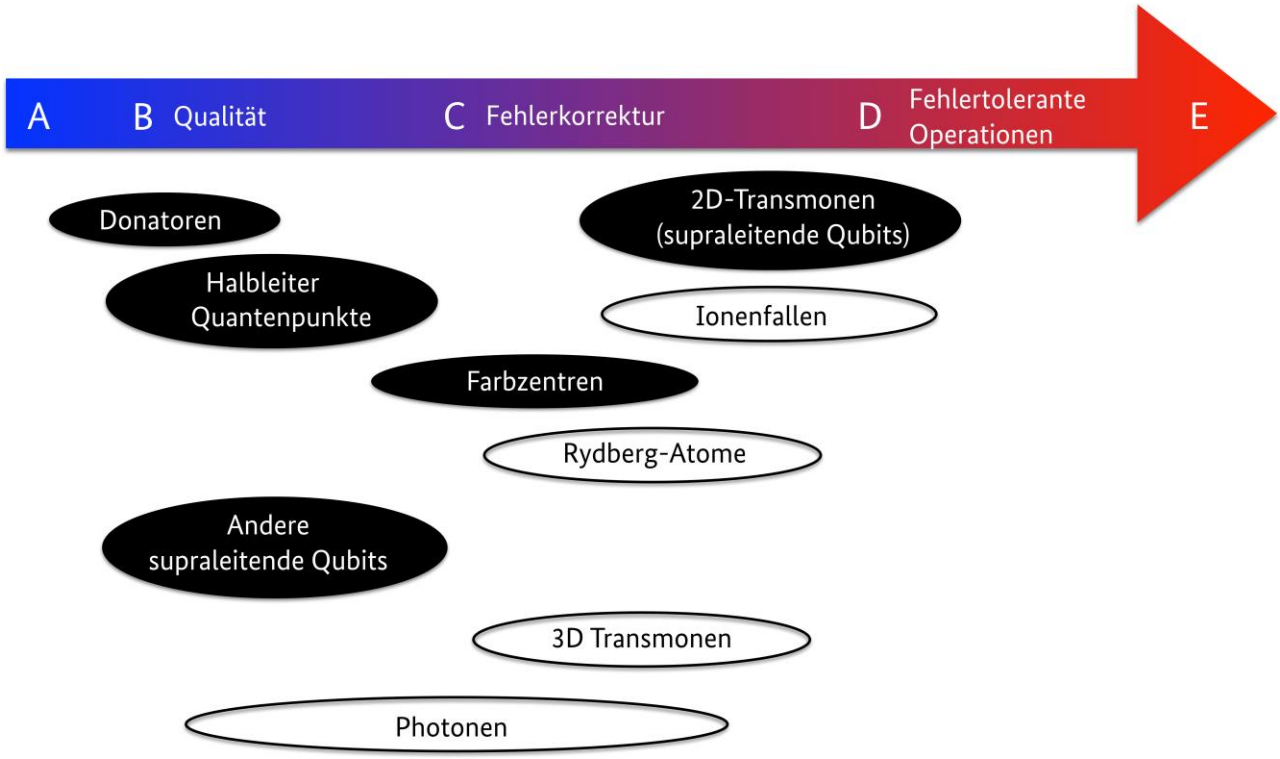

Abbildung 1.3 Einordnung verschiedener Plattformen im Schichtenmodell (siehe Abbildung 1.2). Die Breite der Ovale quantifiziert die Variabilität und die Ungewissheit (bspw. aufgrund fehlender belastbarer Veröffentlichungen von Daten) der verschiedenen Plattformen. Atomphysikalisch/optische Systeme sind weiß und Festkörpersysteme schwarz hinterlegt.

Im Kontext des fehlertoleranten Quantencomputing sind noch viele Entwicklungsschritte nötig. Das Framing eines "Rennens" in der Quantencomputerentwicklung in der Öffentlichkeit ist darum nicht sachgerecht: Es sind noch viele Schritte zu gehen, die idealerweise durch Kooperation erreicht würden – mit Wettbewerb allenfalls in den Sprints bis zum nächsten Meilenstein.

Es ist zu beachten, dass inzwischen deutlich mehr alternative Entwicklungspfade und technologische Optionen verfolgt werden als zur Zeit der vorherigen Versionen dieser Studie. Im Bereich Hardware werden einerseits die bisher führenden Plattformen (Supraleiter und Ionenfallen mit Surface- oder Color-Code) kontinuierlich weiterentwickelt. Andererseits haben neue Hardwareplattformen (z.B. Rydberg-Atome) die in einigen Aspekten aufgeholt haben und führen z.B. in der Zahl der fehlerkorrigierten Qubits, andererseits aber auch neue Fehlerkorrekturmethoden (bosonische Codes und effiziente LDPC-Codes). Diese Alternativen haben das Potenzial, schon bald eine Führungsrolle einzunehmen – es aber noch nicht realisiert. Ferner ist die Bewertung teilweise dadurch erschwert, dass viele Akteure aus der Industrie wenig publizieren.

Der große Aufwand der Fehlerkorrektur macht es für akademische und industrielle Labors auf absehbare Zeit unwahrscheinlich und vermutlich auch wirtschaftlich uninteressant, einen kryptographisch relevanten Quantencomputer zu realisieren. Wenn jedoch eine große Industrienation ihre Forschungsanstrengungen auf dieses Ziel konzentrieren würde, ähnlich den Manhattan- und Apollo-Projekten des 20. Jahrhunderts, so erscheint ein Quantencomputer mit wenigen Millionen physikalischer Qubits, der zumindest in 100 Tagen 2048-Bit RSA brechen kann, erreichbar, wenn auch die physikalische Fehlerrate angemessen sinkt und in einen Bereich von 1:10000 gebracht werden kann. Dies wäre eine Großanlage, die in mehrerlei Hinsicht technologische Rekorde benötigen würde und ggf. Zugriff auf seltene Materialien erfordert.

Die Forschung an Quantencomputern entwickelt sich sehr schnell, allerdings vor allen Dingen im Bereich der Qubit-Zahl, während Fortschritt bei den Fehlerraten deutlich langsamer ist. Letzterer ist aber entscheidend, um überhaupt von der Fehlerkorrektur profitieren zu können – wie sich gerade an den neuen Experimenten zeigt, die sich an den Details der Fehlerschwelle abarbeiten.

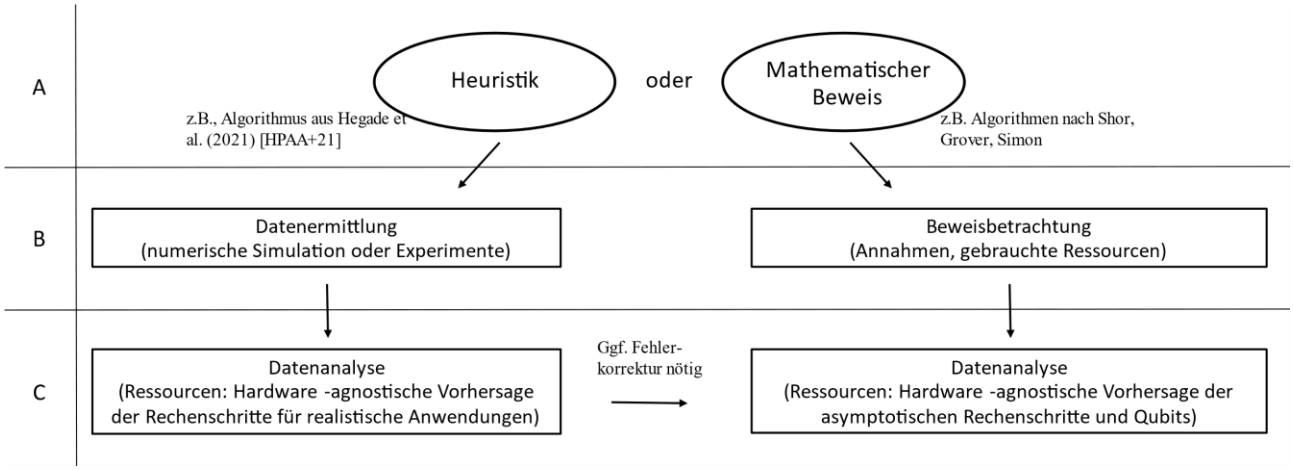

Abbildung 1.4: Schichtenmodell zur Bewertung von Quantencomputer-Algorithmen basierend auf fehlertolerantem Quantencomputing (recht) bzw. NISQ (links).

1.4 Jüngste Entwicklungen

Die rasche Entwicklung von Quantencomputern hat ihre Bewertung anhand der Anforderungen der Kryptoanalyse zu einem mehrdimensionalen Unterfangen gemacht.

Auf der Seite der Algorithmen sind (Verbesserungen der) Methoden von Peter Shor immer noch die Hauptkandidaten mit einer rigorosen Laufzeitanalyse im Hinblick auf einen zugänglichen Quantenvorteil. Regevs Ansatz zur Faktorisierung aus dem letzten Jahr (mit nachfolgenden Verbesserungen) bietet eine asymptotisch interessante Alternative, aber aktuell ist nicht klar, dass diese neuere Methode für kryptographisch relevante Faktorisierungen tatsächlich einen Effizienzgewinn ermöglicht. Stetige Fortschritte bei der Implementierung notwendiger Arithmetik und Kompilierung führen zu einer schrittweisen Verringerung der Hardwareanforderungen, erfordern aber immer noch unpraktikable Gattertiefen für RSA 2048-Instanzen. Bei diskreten Logarithmen auf 256-Bit elliptischen Kurven ist die Situation ähnlich, und eine effiziente Anpassung von Regevs Verfahren auf die Berechnung diskreter Logarithmen in solchen Gruppen ist nicht bekannt. Andererseits gibt es inzwischen eine breite Palette neuer heuristischer Algorithmen, die oft an bestimmte Rechenmodelle angepasst sind, z. B. adiabatische Quantenberechnungen oder Algorithmen mit geringer Tiefe für kurzfristig realisierbare Hardware, die nicht aktiv fehlerkorrigiert wird. Diese werden zwar oft mit markigen Behauptungen angekündigt, aber keiner von ihnen wird mit einem Konvergenznachweis geliefert, der ein zentraler Bestandteil einer quantitativen Leistungsanalyse wäre. Das beste Surrogat dafür, eine gründliche heuristische Skalierungsanalyse, ist ebenfalls für keinen dieser Algorithmen veröffentlicht worden. Auch wenn sich viele dieser neuen Algorithmen möglicherweise als Nebenprodukt des Quantenhypes herausstellen werden, ist es wichtig, sie weiter zu beobachten und zu bewerten, möglicherweise in einer unabhängigen Benchmarking-Aktivität.

Auf der Seite der Berechnungsmodelle, d. h. der mathematischen Modelle für die Durchführung einer Berechnung, stellen das gatterbasierte und das adiabatische Quantencomputing nach wie vor die wichtigsten Pole dar, doch haben Variationen und Mischformen dieser beiden Modelle an Bedeutung gewonnen, oft in Verbindung mit den Hardware-Plattformen, an die sie angepasst sind. Die meisten dieser Modelle sind in Bezug auf ihre Berechnungskomplexität gleichwertig. Allerdings ist die quantitative Leistungsanalyse eine größere Herausforderung, insbesondere die Identifikation von Komponenten-Leistungsdaten, die es erlauben, größere Systeme beliebiger Plattformen zu vergleichen. Besonders erwähnenswert unter diesen alternativen Rechenmodellen sind diejenigen, die mit dem photonischen Quantencomputing in Verbindung gebracht werden, wie das Gaußsche Boson-Sampling und das fusionsbasierte Quantencomputing.

Selbst innerhalb des Modells der gatterbasierten Quantenrechner ist die Unterscheidung zwischen fehlertoleranten Quantencomputern auf der Grundlage der Quantenfehlerkorrektur und der verrauschten Quanteninformatik im mittleren Maßstab (NISQ) entscheidend. Ersteres hat eine gut etablierte Leistung, aber einen großen Overhead, während letzteres effiziente nicht-fehlerkorrigierte Algorithmen von geringer

Tiefe beschreibt, die in der Regel eine externe klassische Optimierung beinhalten. Letztere ermöglichen den Zugang zu einer reichhaltigeren Gattermenge und die gemeinsame Entwicklung von Software und Hardware, was bei kleinen Problemfällen oft zu einer überraschend guten Leistung führen kann. Aufgrund der unbekannten Skalierung dieser Algorithmen und auf der Grundlage größerer theoretischer Argumente ist es jedoch unwahrscheinlich, dass im NISQ-Bereich ein kryptoanalytischer Quantenvorteil erreicht werden kann. Dies unterstreicht den allgemeinen Punkt, dass Fehler derzeit das begrenzende Merkmal der gatterbasierten Quantencomputertechnologie sind – und nicht die Anzahl der Qubits.

Der Bereich der Quantenfehlerkorrektur-Theorie wurden seit der letzten Ausgabe der Studie sehr viele technische Fortschritte erreicht. Diese betreffen technische Verbesserungen in den Decodern von Surface-Color- und Low-Density Parity-Check-Codes sowie große Schritte bei bosonischen Codes, die jetzt ihr eigenes Kapitel in der Studie haben. Der größte Fortschritt wurde jedoch durch Experimente gezeigt: Mehrere Plattformen haben mit verschiedenen Fehlerkorrekturtechniken inzwischen alle Elemente der Korrektur von Quantenspeicher gezeigt - in der vorangegangenen Ausgabe war dort noch ein Kriterium offen. Damit wurde die prinzipielle Umsetzbarkeit von Quantenfehlerkorrektur demonstriert. Nach aktuellem Stand ist der Surface Code der optimale Fehlerkorrekturcode für supraleitende Qubits. Für ionische Systeme ist der Color Code gegenüber dem Surface Code vorteilhaft. Es gibt zwar vielversprechende Entwicklungen bei den LDPC-Codes, die aber noch nicht vollständig ausgearbeitet sind – wenn die Lücke auch schrumpft. Nur wenn derartige Lücken geschlossen werden, können solche neuartigen Codes einen Einfluss auf die Entwicklung von fehlertolerantem Quantencomputing haben. Entwicklungen aus dem NISQ-Bereich wie Fehlermitigation skalieren nicht in dem Sinn, dass sie nach aktuellem Stand für die großen Aufgaben der Kryptoanalyse nennenswerte Alternativen darstellen würden.

Die Demonstrationen von Quantenvorteil im NISQ-Bereich werden zahlreicher und wurden u.a. von Google im Jahr 2024 weiter verbessert. Dies ist parallel zur Verbesserung bei der Fehlerkorrektur zu sehen, es ist aber weiterhin nicht davon auszugehen, dass NISQ-Systeme die Leistungsfähigkeit erreichen werden, relevante Kryptosysteme zu entschlüsseln [KEA+23,TFSS23,BC23,KTC+19]. Auf dem Gebiet der Plattformen für Quantencomputer sind Prozessoren basierend auf Supraleitern bzw. gefangenen Ionen immer noch unter den Spitzenreitern, jedoch haben Rydberg-Atome (in Lichtfeldern gefangene neutrale Atome, die über Rydberg-Zustände gekoppelt werden, ursprünglich eine Plattform für die Quantensimulation) im Winter 2023/24 erstmals auch für Quantencomputing Augenhöhe erreicht – wer innerhalb dieser Spitzengruppe führt ist auch eine Frage des Stichtags der Studie relativ zu großen Konferenzen. Die anderen starken Plattformen, NV-Zentren und Spins in Halbleitern haben sich ebenfalls weiterentwickelt. Die Entwicklungen bei photonischen Qubits sind weiterhin im Bereich des Gauß-Boson-Samplings und leiden weiterhin darunter, dass relevante Akteure Komponentenbenchmarks nicht veröffentlichen. Die Normung von Quantentechnologien wird auf europäischer und internationaler Ebene von mehreren Standardisierungsorganisationen vorangetrieben, wobei die Aktivitäten in den letzten Jahren stark zugenommen haben. Diese Initiativen bestehen aus offenen Gemeinschaften mit Vertretern aus dem privaten und öffentlichen Sektor, die die Perspektiven von Wissenschaft, Industrie und Politik abdecken. So hat beispielsweise die Focus Group on Quantum Technologies von CEN/CENELEC vor kurzem ihre Roadmap zu Quantentechnologien veröffentlicht.[1] Auf der Grundlage dieser Arbeit wurde im Jahr 2023 das neue CEN/CENELEC JTC 22 gegründet, das nun Normen aus der Bedarfsanalyse ableitet. Zusammen mit Aktivitäten von ETSI werden diese europäischen Normungsinitiativen dazu beitragen, auf internationaler Ebene in bestehenden und zukünftigen Komitees bei ISO/IEC, ITU, IEEE und anderen Standardisierungsorganisationen mitzuwirken und somit eine starke Vertretung Europas zu schaffen. Ein Teil der Normungsarbeit zu Quantencomputern ist auf Benchmarks ausgerichtet, die in dieser Studie diskutiert werden (siehe Kapitel 7), sowie auf eine Aufschlüsselung der einzelnen Komponenten, die sich auf die Diskussion der technischen Anforderungen an Quantencomputer in dieser Studie bezieht (siehe Teil IV).

Die Quanteninformatik wird derzeit in öffentlich-privaten Partnerschaften verschiedener Art betrieben. Starke kommerzielle Akteure, die in der Lage (und willens) sind, die Systemintegration in großem Maßstab selbst durchzuführen, stehen auf den Schultern von Programmen des öffentlichen Sektors. An diesen Programmen sind Universitäten und Forschungsinstitute, aber auch Unternehmen beteiligt. Erfolgreiche

[1] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

Akteure bringen eine integrierte Sichtweise auf Software und Hardware mit, was für frühe Technologien wichtig ist, und die Fähigkeit, schrittweises Engineering mit risikoreicher Forschung zu verbinden. Sie benötigen Personen, die in der Lage sind, hochwertige Ingenieurleistungen mit Quantenkenntnissen und der erforderlichen interdisziplinären Denkweise zu verbinden, was im Allgemeinen schwer zu finden ist. Geografisch gesehen kommen die beeindruckendsten Ergebnisse von nordamerikanischen Akteuren. Europa kommt schnell voran und nutzt sein technologisches Potenzial seit dem Start des EU-Quantenflaggschiffs und der damit verbundenen nationalen Initiativen viel besser als in der Vergangenheit. Vor allem in China sind inzwischen viele beeindruckende Leistungen zu verzeichnen, die oft quantitativ weltweit führend sind, auch wenn sie qualitativ (noch) kein Neuland betreten. Australien und Japan sind starke Akteure in bestimmten Bereichen, und es gibt eine Reihe bemerkenswerter Aktivitäten in anderen Ländern, darunter Indien, Brasilien, Argentinien und Südafrika. Das russische Quantenprogramm hat (recht vernünftig) versucht, die traditionelle Stärke der Wissenschaft aus der Sowjetära mit der Zusammenarbeit mit Forschern aus anderen Ländern zu verbinden. Dieses wurde 2022 eingestellt, und Russland ist jetzt bestenfalls ein kleiner Akteur.

1.5 Fazit

Mit Blick auf die Zukunft lautet die Schlussfolgerung der Studie, dass die Quanteninformatik stetige Fortschritte in Richtung kryptoanalytische Relevanz macht. Es gibt einen etablierten Mainstream: fehlertoleranter (verbesserter) Shor-Algorithmus, der entweder auf einem supraleitenden System mit dem Surface-Code oder einem ionenbasierten System mit dem Color-Code ausgeführt wird. Die Grundannahmen der Quantenfehlerkorrektur wurden im Jahr 2024 endlich vollständig verifiziert. So wurden Verzögerungen der letzten Jahre überwunden. Damit ist es wahrscheinlich, dass selbst ohne Disruptionen ein krypotanalytisch relevanter Quantencomputer in höchstens 16 Jahre realisierbar ist – es wurde also in einem Kalenderjahr die Distanz um etwa vier Jahre verkürzt.

Zudem gibt es inzwischen eine Fülle neuer Entwicklungen bei der Fehlerkorrektur und -mitigation sowie der Hardware, die dies deutlich auf knapp zehn Jahre beschleunigen könnten, aber noch nicht durchgängig verifiziert sind.

Auch die Vielfalt der Akteure und Ansätze macht Vorhersagen schwierig. Unternehmen hüten einige Komponenten ihrer Technologie als Geschäftsgeheimnis – einige, selbst große Unternehmen, arbeiten im Stealth-Modus. Die Quanteninformatik wird aus Gründen der Wettbewerbsfähigkeit oder der nationalen Sicherheit gehütet, so dass einige Entwicklungen natürlich vertraulich bleiben. Es ist zwar unwahrscheinlich, dass die als geheim eingestufte Forschung in qualitativer Hinsicht weit voraus ist, doch könnte sich dies in Zukunft ändern.

2 Synopsis

2.1 Basic idea

The often counterintuitive concepts of quantum physics are well understood and precisely confirmed in science. The first applications of simple quantum physics have been known for a long time—transistor, laser, magnetic resonance, nuclear technology, and others. These applications use a few quantum properties of an otherwise macroscopic system (Quantum Technology 1.0). Currently, a new generation of Quantum Technologies 2.0 is emerging, which uses many more unique properties of quantum physics and addresses single quantum systems—one of them is the concept of a quantum computer. Quantum computers use the feature of quantum physics like superposition – the system state can simultaneously occupy many if not all classically permitted states – and entanglement – a correlation manifesting the non-locality of quantum physics – to speedup computations.

There is an assortment of known quantum algorithms for cryptographic tasks. Most prominent are Shor's algorithms for factoring integers and for the computation of discrete logarithms. Shor's algorithms represent significant progress for standard *asymmetric* cryptographic protocols (including RSA and common elliptic curve-based methods). In principle they permit the efficient reconstruction of a secret key from public data. Quantum algorithms also permit improvements compared to classical techniques when analyzing *symmetric* cryptographic protocols. Grover's method for the acceleration of a complete key search is probably the most well-known of such algorithms. Nevertheless, cryptanalytic progress through quantum algorithms is significantly less spectacular in the field of symmetric methods if one remains restricted to established threats, and they do not endanger existing symmetric protocols from what is currently known. Besides the established threats (which often rely on Grover’s algorithm), several quantum algorithms have been proposed, for which the computational complexity—and thus a potential quantum speedup—is not established from a theoretical point of view. As long as no theoretical proof of the complexity is known, an evaluation of these algorithms must be based on heuristics. This study puts such algorithms into perspective.

Quantum computing was first proposed by Nobel laureate Richard Feynman in 1982 as a tool to simulate quantum systems. This research field has expanded since the discovery of Shor's factoring algorithm in 1995, which can be viewed as the starting point of the global activities towards constructing a quantum computer. Since then, various physical platforms to realize such a computer are being pursued. Quantum computing is an interdisciplinary research area between physics, computer science, and engineering, which is being pursued in universities, research centers, and companies. Milestones such as the establishment of a division for quantum information in the American Physical Society, or the establishment of a European Quantum Technology Flagship program, have made quantum computing an established research discipline. A wealth of commercial offerings from both startups and established companies has created a quantum industry.

2.2 Hardware platforms

Similar to the early days of classical computing, there exists a wide variety of hardware platform candidates for quantum computing today. These, on the one hand, need to display detectable quantum effects—which means they need to be small and isolated. On the other hand, they need to be operated as computers, i.e., their technology needs to be scalable and permit access to write, read, and control. This brings together challenges within science and engineering—isolation and access need to be provided simultaneously.

The structuring element for the selection of platforms by researchers and their evaluation is their sensitivity to operational errors. The field of quantum error correction is driving architectures and overhead.

2.2.1 Global categories

Atomic platforms use elementary quantum systems such as single atoms, in which the laws of quantum mechanics can be naturally resolved but where scaling and control are a challenge.

Solid-state platforms use various types of integrated circuits which are naturally scalable and controllable, in which the main challenge is the realization of quantum effects and their stabilization over a long time.

Momentarily, the most advanced platforms in atomic physics trapped ions and neutral atoms using Rydberg states. This technology is related to the development of atomic clocks and inherits high precision resulting in low error rates. In the area of solid-state platforms, the currently leading approach lies in the implementation of Josephson qubits—integrated circuits made from superconducting metals such as Aluminum or Niobium.

Beyond those current leaders, there is a range of candidates that have the potential to catch up and overtake. Most notably, these include silicon-based nanotechnology and trapped neutral atoms.

2.3 Algorithmic goals

Attacks using quantum computers frequently aim at the direct reconstruction of a secret key under rather moderate assumptions—only access to a public key or a few plaintext-ciphertext pairs is assumed. Beyond that, also complex attacks using quantum technologies have been proposed, which on the one hand have impressive potential, but on the other hand are based on assumptions that are not satisfied by real implementations. If one allows the attacker to run the targeted implementation with inputs in superpositions, theoretically interesting models of attack can be formulated, but this type of access is not given in classical implementations.

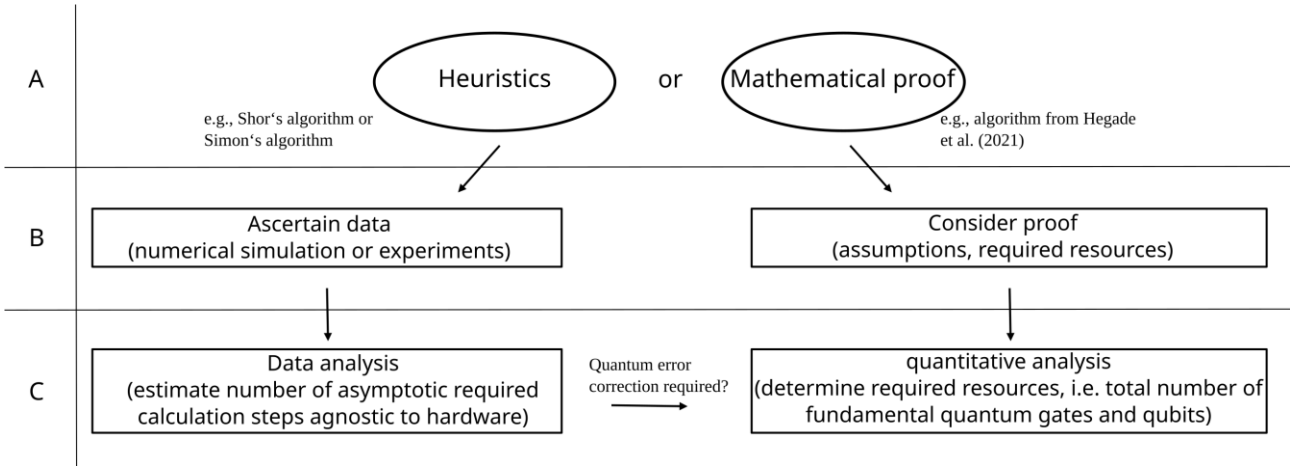

Figure 2.1: Evaluation scheme for quantum algorithms introduced in Chapter 3. Three levels A-C denote the algorithm's maturity, which is based on the current state of knowledge. There are two main types of algorithms, since an algorithm can be based on mathematical proof or, if no proof is known, on heuristics. Section 3.2 gives a detailed description of the evaluation levels.

A current focus in the literature on quantum cryptanalysis is a detailed cost analysis of (abstractly) known attacks applied to relevant cryptographic instances (such as 2048-bit RSA, 256-bit elliptic curves, AES, or SHA-2). Grover's algorithm, Shor's algorithms and their improvements, as well as Regev's approach and its improvements, are fundamentally based on performing computations within the symmetric primitive under attack or within the algebraic structure behind an asymmetric method on a quantum computer. The relevant computations are expressed as quantum gates. The quantum gate model can then be the interface to the underlying computational models. Even though the fundamental efficiency of Shor's algorithms and its improvements is not based on the details of the cryptographic protocol under attack, the details of the underlying quantum circuit are essential for a quantitative cost estimate. In the case of computing a discrete logarithm on an elliptic curve, for example, the curve arithmetic is mapped on quantum gates, which can be done in different ways. Analogously, in factoring with Shor's or Regev's method it is necessary

to implement (modular) integer arithmetic with quantum gates and in a Grover-based key search for AES, AES-encryption is implemented with quantum gates. .

Typical optimization goals are the reduction of the qubit number, the circuit depth, and/or the gate count. In the last case, one typically differentiates between gate types to consider different complexities in physical implementations. We list relevant cost estimates from the literature. If robust quantum processors are provided, it is realistic to realize cryptographically relevant computations of discrete logarithms. Also, factoring of larger integers using (improvements of) Shor's algorithm appears realistic. It is not clear that Regev's more recent proposal for factoring (and its improvements) offers an efficiency gain for practical cryptographic parameter sizes, but this is an active area of research that should be monitored. Key search in AES on the other hand appears to remain a large challenge even with reliable quantum processors—the asymptotically exponential scaling of Grover's algorithms represents a serious obstacle.

A few novel algorithmic ideas take the hardware adaptation to a different regime in proposing shallow algorithms that could be executed on near-term hardware. "Shallow" refers to having a low number of necessary time steps. These are typically quantum variational approaches (see Section 5.2.3), which are heuristic in nature, i.e., there is no proof of convergence with associated models of computational cost that would allow a precise extrapolation to large problem sizes. In the field of cryptanalysis, most algorithms of this kind have been applied to integer factorization. For their evaluation, one must rely on scaling data, which—unfortunately—are not frequently provided in sufficient quantity. We summarize the evaluation model in Figure 2.1.

2.4 Computational models

The concrete realization of quantum algorithms is discussed in different computational models. The most relevant model for cryptanalysis is the *fault tolerant implementation* of the *quantum gate model*.

The quantum gate model resembles the operation of a classical computer: A sequence of logical operations, or gates, taken from a universal gate set in a simple machine code is applied on a data register, which is read out at the end of the computation. For an ideal implementation of this model, quantum speedup is mathematically proven. Since a perfect, error-free implementation of such an algorithm is impossible, however, it is the goal of a physical realization to approximate it as close as possible.

The fault-tolerant implementation of the gate model relates to the observation that quantum operations and hardware are much more susceptible to error than their classical counterparts. It is thus necessary to correct errors repeatedly during operation. This can in principle reduce the probability of an error in the result to an acceptable, predetermined size. Quantum error correction has several peculiarities based on the analog character of quantum operations and the invasive nature of quantum measurements. Still, a mathematical framework of quantum error correction has been formulated, culminating in the use of the surface and color codes. The overhead imposed by quantum error correction is significant and determines size and speed of potential quantum computers without challenging basic speedup. Quantum error correction further sets a threshold for the physical error rate, below which error correction is possible and effective. Hardware below this threshold can thus be used to simulate an ideal quantum algorithm using error correction.

Before the realization of fault-tolerant quantum computation stands the era of Noisy Intermediate-Scale Quantum (NISQ) Technologies. On these platforms errors are not actively corrected, because of which one can only execute algorithms with a limited number of gates. Applications of such processors on non-self-referential problems are currently being developed. They are found in the area of quantum simulation where on classical architectures the memory needs are a limiting resource. These results have motivated the heuristic algorithms mentioned above. In this framework, results on quantum advantage or quantum supremacy currently make frequent headlines. Quantum advantage describes imminently reaching a state in which quantum computers can no longer be simulated by current classical supercomputers. This point has been reached in 2019 using synthetic benchmarks, later efforts for more efficient classical simulation notwithstanding.

The technique of quantum annealing, a variant of adiabatic quantum computing, is less demanding on hardware than that of the gate model, and large processors up to 5000 units have been realized. The products of the company D-Wave Systems are designed for a class of optimization problems and can be

programmed in a versatile way. In principle, quantum annealing can be applied to cryptanalytic problems and can lead to acceleration, but a key hardware element necessary for that has so far not been realized. Several platform-specific models, such as one-way quantum computing, are evaluated separately.

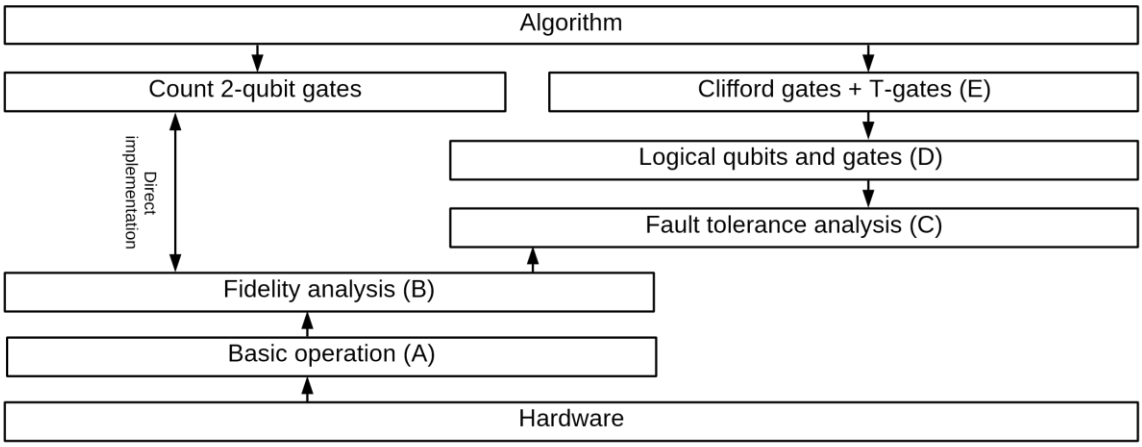

Figure 2.2: Sketch of interdependencies of our evaluation scheme. Hardware needs to pass checkpoints from below, software is compiled from above. These checkpoints, labeled (A) through (E), form the levels of our hardware evaluation scheme introduced in Chapter 3.

2.5 Evaluation along computational models

Similar to the software stack of modern computer architectures (from machine code to a user interface), we can organize quantum computer evaluation from the bottom up: We propose to use five levels A through E, cf. Figure 2.1. As indicated in the figure, if the quality of operations identified on level B allows to implement cryptanalysis without error correction, the subsequent levels might be omitted via a direct (NISQ) implementation.

- **A: Basic functionality.** Has the quantum computer candidate demonstrated all basic functionalities of quantum processor (qubits, gates, initialization, coherence, readouts)? Were all these functionalities demonstrated in the same experiment containing more than two qubits?
- **B: Quality of operations.** Has the error rate of all relevant operations been measured? Are they compatible with error correction thresholds? Have all ingredients of a fault-tolerant architecture been demonstrated?
- **C: Error correction.** Has quantum error correction been demonstrated and is it effective? Are logical error rates smaller than physical error rates?
- **D: Fault tolerant operation.** Have operations on logical qubits been implemented in a fault-tolerant way? Has this been achieved for a universal set of gates (Clifford+T)?
- **E: Algorithms.** Have complex fault-tolerant algorithms and operations been implemented? Quantum error correction requires spatial and temporal redundancy without reducing the efficiency of quantum computers. Information gleaned on levels B and C allows to project the size and temporal overhead of future quantum computers—this overhead is directly determined through the error rate of the underlying operations.

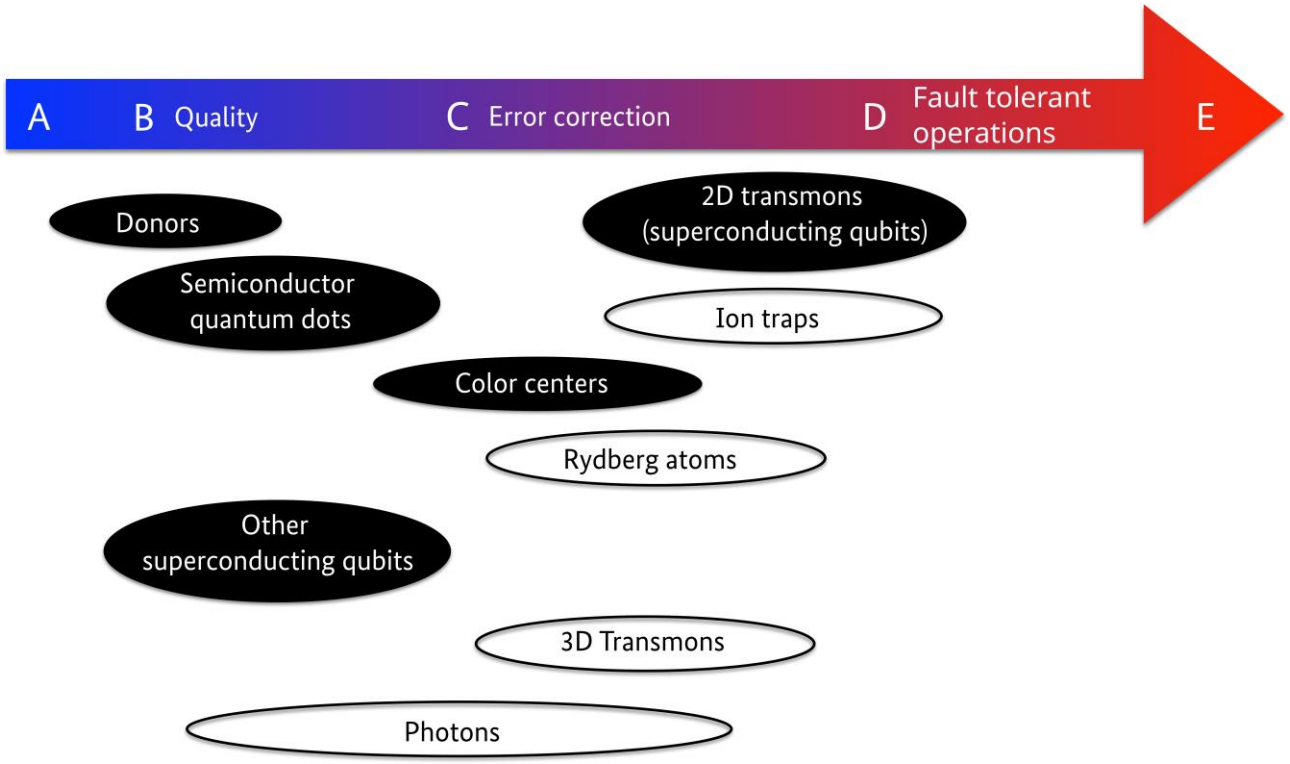

Figure 2.3: Evaluation of the main platforms following the developed scheme. Each oval's width quantifies the variability and uncertainty (e.g., due to the lack of peer-reviewed data) associated with the given platform. Entries based on atomic/optical systems are shaded in white, while solid state systems are shaded in black.

Very recently, multiple platforms have completed level C. Some of them have achieved elements of level D.

2.6 Evaluation of platforms

To evaluate the potential of different platforms, this study describes a variety of known platforms for quantum computing and categorizes them into the above scheme. Figure 2.3 summarizes the results of the current evaluation. Part of the experimental setup of the leading platforms, superconducting qubits and atomic qubits, are shown in Figure 2.4 and Figure 2.5.

We note that various platforms, which are currently not being widely pursued in the laboratory, are described and evaluated in an older version of this study [WSL+20]. Among these are molecular qubits, and qubits based on electrons captured on fluid helium.

2.6.1 Trapped ions

This is an atomic platform, in which single ions float in ultra-high vacuum held by slowly varying electric fields. It is a well-controlled and strongly isolated quantum system. Research on trapped ions has already been applied previously, e.g., in metrology in atomic clocks—an ideal starting point for low-level error operation. The quantum information is stored in loosely bound outer electrons, whose states can be manipulated through laser or microwave fields. Ions can be trapped in chains of mutually repelling objects, and they can interact through vibrations to implement multi-qubit logic operations. This is possible with high quality. Further scaling requires changing from chains to complex two-dimensional arrays, for which the electrostatic trap is implemented as a chip surface. All ingredients of a quantum processor and high

operational quality along with simple error corrections have been demonstrated, this platform has completed level C of our evaluation scheme and shown elements of level D

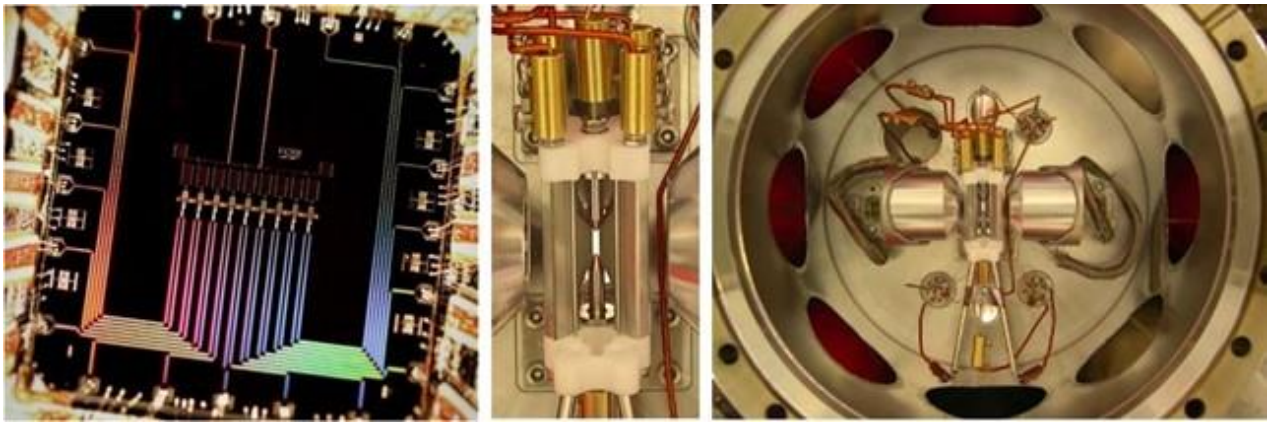

Figure 2.4: The currently leading quantum computing platforms - microscopic perspective. Left: Josephson processor (image: Julian Kelly, Google). A linear array of 9 qubits (crosses) with nearest-neighbor coupling; explicitly shown are the control lines (bottom) and readout lines (top). Middle: Linear ion traps: trap electrodes (rods) and lenses for laser irradiation to implement quantum logic. Right: The same ion trap setup with its vacuum apparatus. (Image of ion trap: Jürgen Eschner, Saarland University.)

2.6.2 Superconducting circuits

This is a solid-state platform. It consists of integrated circuits made from superconducting metals and hence must be operated at extremely low temperatures near absolute zero. Its key element is the superconducting Josephson junction. Their typical size is in the range of a micrometer or below—orders of magnitude larger than current transistors. This basic technology is also rooted in metrology, which again provides a good starting point for reaching high operational quality. Superconducting elements can be assembled into different quantum processor architectures, whose evolution has largely been driven by the requirement to maintain quantum coherence as a necessary ingredient for error avoidance. Next to the necessary cooling infrastructure (which is not an obstacle per se, but a complication) they have the control by microwaves in common. This platform is currently attracting the most industrial interest.

Flux qubits are superconducting loops in which logical states are represented by circulating currents. They resemble classical superconducting electronics more than other architectures. In some cases, flux qubits can reach very long coherence times, and they can be easily coupled. It is challenging to fabricate these qubits consistently and with predictable properties, which makes realizing the gate model a challenge. Their superior connectivity makes them the leading platform for adiabatic quantum computing. For gate-based computing they are on level B.

Planar transmons are single-Josephson junction resonators, whose electromagnetic oscillation states carry the quantum information. This design is an evolutionary development from charge qubits. It allows coupling through microwave resonators. Planar transmons reach very long coherence and can be flexibly coupled. They are planar on a chip surface and so far, chains and simple networks have been demonstrated. Further integration requires building control and read-out lines into the third dimension. Planar transmons have demonstrated fully error corrected quantum memory and some fault-tolerant gate, so they have completed level C and have entered D.

2.6.3 Neural atoms

Three dimensional transmons are resonators like their planar version, but they are surrounded by a superconducting cavity at all sides. This increases coherence times, but also makes control more complicated and gates slower. They are used to implement a special type of error correction called Bosonic code which has just completed all aspects of level C.

2.6.4 Semiconductors

In contrast to ions, charge-neutral atoms cannot be trapped by electrical fields alone. However, trapping is possible with much weaker, light-induced forces in optical tweezers. Especially Rydberg states—atomic states with huge outer shell radii—allow for long distance interactions. These platforms contain many qubits and feature low-error rates. Within the last year, they have demonstrated full programmability and demonstrated a large number of error-corrected qubits as well as full NISQ-programmability – they are in level C.

Semiconductor technology – as an industrially relevant, spectacularly miniaturized, and highly integrated platform – has a strong potential for quantum computer development. There is a variety of semiconductor platforms. We describe the currently most promising types in this synopsis.

Semiconductor quantum dots are small, isolated areas, "artificial atoms," in which single electrons can be trapped so their spin degree of freedom can be used as a quantum bit. Multi-qubit logic can be realized with interactions similar to those in magnetic materials. This platform has operational similarity with superconducting circuits. They have now achieved high performance in small systems, too small for demonstration of convincing error correction: level B.

Color centers are isolated defects in artificial diamonds. They can be used similarly to trapped ions, where the diamond crystal acts as a trap. These defects carry a nuclear and an electronic degree of freedom, i.e., a single center potentially contains two qubits and, in some cases, up to four. Color centers lead in quantum sensing, and they are an important platform in quantum photonics. Having shown error correction puts NV centers into level C, however, scaling beyond this may be a major obstacle due to currently non-scalable fabrication.

Single donors in Silicon have shown excellent single-qubit properties, and have reached good two-qubit operations: level B.

2.6.5 Photonic platforms

Light cannot only be used as a control and communication channel for quantum computers but also to host quantum information. Several important ingredients for quantum photonics have been developed in neighboring areas. Its key challenge is the implementation of two-qubit gates, given that quanta of light (photons) do not interact. Several indirect strategies can simulate this interaction, such as the use of special media or measurement and post-processing. In one photon-adapted synthetic benchmark, quantum supremacy as the pinnacle of level B has been reached. This peculiar balance of resources has led to a range of alternative quantum computing protocols such as one-way or continuous variable quantum computing, which are better adapted to the physical situation of this platform and are evaluated outside our main scheme.

2.6.6 State of the art

In 2024, the leading platforms have demonstrated that they can pass the threshold to the break-even point of error correction while having verified most other concepts of fault-tolerant computation. This is a milestone, validating the concept of quantum error correction as a whole.

Currently, such a quantum computer would be, even with an optimistic view of the near-term progress, a major piece of research infrastructure—such as a soccer-field size hall with vibration-controlled optical tables or a large array of cryostats containing the scarce isotope Helium 3.

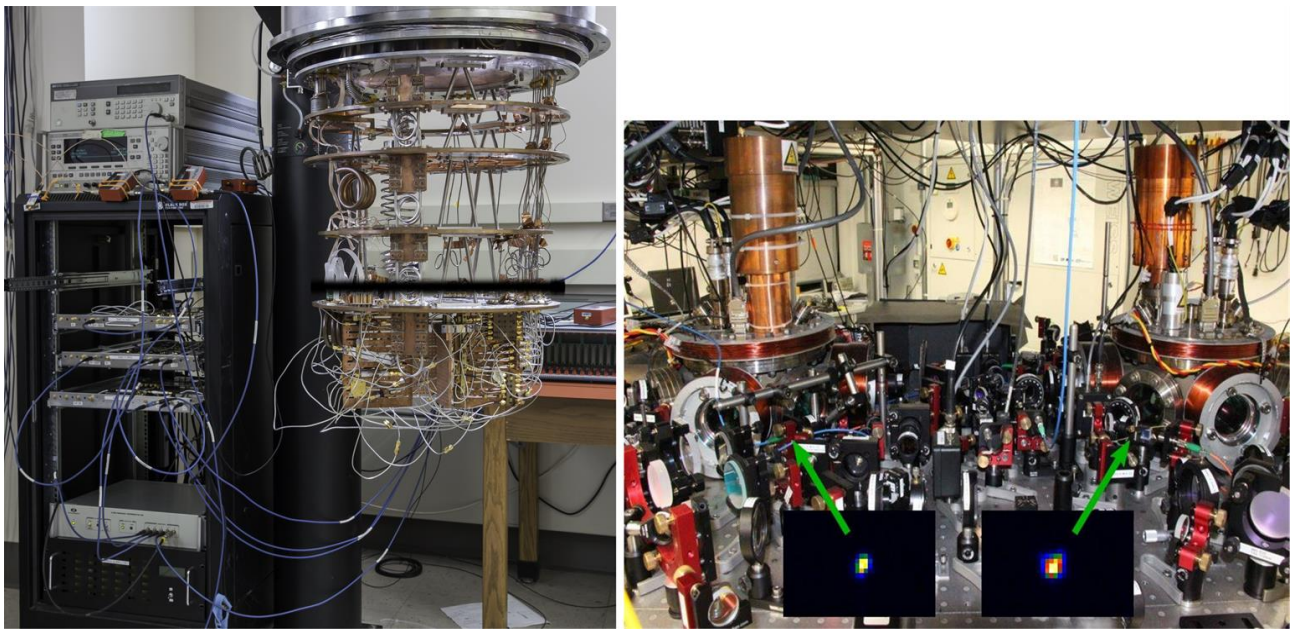

Figure 2.5: Infrastructure units for quantum computers in leading platforms. Left: Dilution cryostat optimized for large cooling power and large wire-count for the operation of Josephson qubits (opened); qubits and other electronics units are mounted on the copper plates on different temperatures, the rack on the left contains control electronics. (Image: Edward Leonard Jr., University of Wisconsin-Madison); Right: Parts of a vibration-controlled optical table containing two vacuum chambers for separate ion traps (Image: Jürgen Eschner, Saarland University).

It is an interesting exercise to extrapolate what a concerted research program for building a quantum computer could reach within the foreseeable future. With “concerted program” we mean that an industrialized nation pools a lot of its research and development effort into such a project, comparable with the Apollo and Manhattan programs in the US. Assuming that the current technical challenges are met—somewhat better operations, sparse use of voluminous periphery, larger chip areas, inter-chip connects and upgrades to cryogenic technology—it seems to be possible to have a computer with a Million planar transmons and a physical error rate of 1:10000. This would allow to attack 2048 Bit RSA in a few hundred days. A faster attack (in one day) would require connecting up to 1000 such units. This would require new technological solutions to connect these units—which have been demonstrated but currently would be too slow. Also, the initial filling of these machines with Helium 3 would require roughly the full annual industrial demand of Helium 3, likely requiring new nuclear facilities to produce this isotope. The financial and human investment in such an effort would be by far larger than current efforts in quantum computing. Progress in materials research towards lower errors would bring these numbers down significantly.

An analogous activity in ion taps would require bringing the currently developed scalable trap technology to the same quality as linear traps. If successful, building the required quantum processor occupying roughly a soccer field would again require a concerted program.

2.7 Global activities and potential for development

Quantum computing is progressing fast. Traditionally, this area has been sponsored by the funding agencies of the US military and intelligence community (IARPA, ARO, DARPA). There, one can perceive an increased focus on very few leading platforms and larger research teams, as well as an increasing role of government laboratories.

The engineering challenges starting (at the latest) at level C go, in most places, beyond the capabilities of usual university research. It is thus even more important for quantum computing development that laboratories outside universities and companies enter the field, which are currently driving progress in particular for Josephson qubits. These are large established technology corporations (IBM, Google) as well as financially strong startups and SMEs and a range of small companies. There is some, though significantly less, business interest in other platforms. This should however not lead to the conclusion that the

technological challenges for ion traps cannot be mastered—but industry is less experienced in integrating such systems.

Significant investment of Intel goes into semiconductor platforms, which may lead to rapid process in the future.

There are notable government investments in quantum computers in a few countries. Australia continuously invests in semiconductor platforms. The EU operates the flagship initiative for quantum technologies, one of which is quantum computing, which is accompanied by large national programs such as the German, French, and Dutch ones. One of the largest government programs for development of quantum technologies is implemented in China.

These have in common that they typically do not directly aim at cryptanalysis, but in many cases a universal, fault tolerant quantum computer is the long-term goal, which can be used for cryptanalytic applications.

2.8 Risks

The evaluations and conclusions of this study reflect the current state of knowledge and assume continuous progress. There can be disruptive discoveries that would dramatically change the study's evaluation. Most importantly, novel cryptographic algorithms that can be run on NISQ machines or dramatic breakthroughs in the error rate of some platforms could act as a game changer. The latter has gotten more likely over the last years given the development of the community.

2.9 Recent developments

The rapid development of quantum computers has turned its evaluation against the requirements of cryptanalysis into a multidimensional undertaking.

On the side of algorithms, (improved versions) of Shor's algorithms are the main candidate with a rigorous runtime analysis in terms of having an accessible quantum advantage. Regev's approach to factoring, put forward last year, and its improvements offers an interesting alternative. It is not clear, however, that this new method leads to an efficiency gain for cryptographically relevant problem sizes. Steady progress in the implementation of pertinent arithmetic and compilation lead to gradually reduced hardware requirements, but we are still facing impractical gate depths for RSA 2048 instances. For discrete logarithms on 256-bit elliptic curves, the situation is similar, and an efficient adaptation of Regev's method to computing discrete logarithms in such groups is not known. On the other hand, there is now a wide range of new heuristic algorithms that are often adapted to specific computational models, e.g., adiabatic quantum computing or low-depth algorithms for near-term hardware. While these are often announced with large fanfare, none of them comes with a proof of convergence, which would be a central ingredient for a quantitative performance analysis. The best surrogate for this, a thorough heuristic scaling analysis, has also not been published for any of these algorithms. While it is conceivable that these new algorithms are merely a result of the euphoria experienced during the early rise of quantum computing, it is important to further watch and evaluate them, potentially in an independent benchmarking activity.

On the side of computational models, i.e., mathematical models of how a computation is carried out, gate-based and adiabatic quantum computing still mark the most important extremes, but variations of these are being explored. While most of these models are equivalent to one another in terms of their computational complexity, detailed mappings for performance indicators that are needed for an absolute performance analysis are more challenging. Particularly noteworthy among these nonstandard computational models are specifically those associated with photonic quantum computing, such as Gaussian Boson sampling and fusion based quantum computing.

Even within the model of gate-based quantum computing, the distinction between fault-tolerant quantum computers based on quantum error correction and noisy intermediate-scale quantum (NISQ) computing is crucial. The former has well-established performance but large overhead, whereas the latter describes efficient non-error corrected algorithms of low depth that usually involve external classical optimization. The latter allows access to a richer gate-set and co-design of software and hardware that can often lead to

surprisingly good performance on small problem instances, yet, due to the unknown scaling of these algorithms and based on larger theoretical arguments it is not likely that cryptanalytic quantum advantage can be reached in the NISQ domain. This emphasizes the general point that errors are the limiting feature of gate-based quantum computing technology currently – rather than qubit number.

The field of error correction has similarly made advances in breadth: Drivers of large-scale development, the surface code and the color codes get gradually improved in terms of better decoders reducing their overhead and improving details. On the other hand, new codes out of the family of low-density parity-check codes or bosonic codes could lead to more rapid progress in this field with a dramatic impact on our extrapolation. On the experimental side, these error correction codes are being tested in larger and larger setups, and the error correction roadmap is being implemented further and further. The most advanced experiments demonstrate the effectiveness of enlarging error correction codes and show some first error-corrected gate operations. They do, remarkably, not reach break-even, i.e., lead to a gate error of the corrected gate (or memory) lower than that of the physical operation. This means the field is slightly behind schedule but did not suffer a setback as the next technological steps towards that goal are well laid out. This reveals the subtlety of comparing realistic error rates with a multitude of error mechanisms to a single average error as it is assumed in error correction theory. Matching these activities is on its way, and the next few years will provide information to evaluate this more realistically.

According to current literature, the surface code is the optimal error correction code for superconducting qubits. For ionic systems, the color code has an edge over the surface code. While there are promising developments in LDPC codes, essential components and analyses are missing for a clear comparison – in particular, evaluations of suitable decoders and thus reliable threshold estimates. Such novel codes can only have an impact on the development of fault tolerant quantum computing if these gaps are closed. Error mitigation methods as proposed in NISQ do not scale in a way that is sufficient for the high demands of cryptanalysis.

In June 2023, IBM has significantly advanced the state of the art in demonstrating quantum advantage [KEA+23] on many levels; its direct impact with respect to quantum advantage is being debated [TFSS23, BC23]. IBM has used a fully programmable processor of unprecedented size (127 qubits) with a consistently very low two qubit error. Instead of a fully synthetic circuit sampling problem, they have used a problem from the simulation of quantum magnets as a benchmark algorithm - which is still rather well adapted to the classical hardware. Most notably, they have used techniques of error mitigation rather than error correction to enhance their results. Error mitigation is a method that allows to reduce the error of NISQ quantum processors without resorting to full fault tolerance by diagnosing the error of the algorithm through running multiple versions of it and then using this information to correct the output. As mentioned above, the known error mitigation methods do not scale. In [KEA+23] the pioneering method of [KTC+19] was applied and taken to new levels. This result highlights the necessity of combining low error rate with processor size to make error mitigation efficient. At the same error rate, more qubits would not have improved the result.

This work is a significant technical advancement on many levels. Most notably, it shows the potential of error mitigation to improve the break-even point of quantum computing significantly. It is not expected that this would go so far that an error-mitigated Shor algorithm affects cryptography in the NISQ era, but if there was a more NISQ-friendly alternative (which we have not identified so far) it would advance the field and create a further dimension in our evaluation system.

In the area of platforms for quantum computers, processors based on superconducting circuits and trapped ions are still front-runners, but Rydberg atoms are now very close and (depending on the cutoff date) have even been leading the field at some point. Despite having similar base parameters – superconducting processors have shorter coherence times but faster operations than ion trap-based processors – their algorithmic performance is surprisingly similar. Both platforms have been making progress – superconducting circuits are showing steady progress as systems with only mild progress in coherence times, ion traps are working on scaling in the sense of reproducing their strong performance in linear traps also in two-dimensional setups. It is a main current trend that more platforms are catching up. On the solid-state side, semiconductor qubits are reaching high fidelities in small systems that do not yet translate to scaling (and they are remarkable diverse in identifying which semiconductor platform is leading) but now seem to be at the level where there are no basic obstacles. Finally, there have been strong progress reports from photonic qubits specifically in the field of Gaussian Boson sampling and potentially other photon-

adapted computational models like fusion gates - but they cannot be evaluated, since actors are very protective about component and subsystem performance. Topological qubits have suffered a setback after controversy over data selection in previously celebrated papers.

Standardization of quantum technologies is pursued on a European and on an international level by several standards development organizations (SDOs), with a strong increase of activity in recent years. These initiatives are comprised of open communities with representatives from both private and public sectors, covering perspectives from academia, industry, and policy makers. For instance, the Focus Group on Quantum Technologies of CEN/CENELEC recently published its roadmap on quantum technologies[2]. Based on this work in 2023 the new CEN/CENELEC JTC22 on QT was founded, now deriving standards from the needs analysis. Together with activities of ETSI, European standardization initiatives will contribute on an international level to existing and future committees at ISO/IEC, ITU, IEEE and other SDOs and thus create a strong representation of Europe. A part of the standardization work on quantum computers is geared towards benchmarks, which are discussed in this study (see Section 7), and a breakdown of the individual components, which relates to the discussion on technical requirements of quantum computers in this study (see Part IV).

Quantum computing is currently carried out in public-private partnerships of various kinds. Strong commercial actors that are able (and willing) to stem large-scale system integration on their own are standing on the shoulders of public-sector programs. Public sector-programs involve universities and research institutes but also companies. Successful actors bring together an integrated view on software and hardware, which is important for early technologies, and the capability to combine step-by-step engineering with high-risk research. They require people who can bring together high-quality engineering with quantum-awareness and the required interdisciplinary mindset, which are generally hard to come by. Geographically, the most impressive results come from North American actors. Europe is moving ahead quickly, realizing its inherent potential a lot better since the start of the EU Quantum Flagship and related national initiatives. Most notably, there are now a lot of impressive achievements in China which are often quantitatively world-leading, even they are not (yet) breaking qualitatively new ground. Australia and Japan are strong players in specific fields and there is a range of notable activities in other countries, including India, Brazil, Argentina, and South Africa. The Russian quantum program has attempted (quite sensibly) to combine the traditional strength in science dating back to the Soviet era with collaboration with researchers based in other countries. This has stopped in 2022 and they are now a small player at best.

2.10 Conclusions

Looking ahead, the conclusion of the study, on the one hand, is that quantum computing is making steady progress towards cryptanalytic relevance according to the reliable mainstream (fault-tolerant (improved) Shor algorithm, executed either on a superconducting system with the surface code or an ion-based system with the color code. Major roadblocks in this scenario were resolved in 2024, bringing us a lot closer to this goal even without large disruptions – we estimate that the conservative end is now at 16 years. On the other hand, there are now a plethora of new developments in error correction and mitigation as well as hardware with the large progress in neutral atoms, because of which one can be much less confident of the above result than only a few years ago – a lot more can move and surprise, and most of these results could accelerate the development to below a decade. .

The variety in actors is making predictions more difficult. Companies naturally guard some components of their technology trade secrets – some even large ones are operating in stealth mode. Quantum computing is guarded as a matter of competitiveness or national security, thus naturally keeping some developments confidential. While it is unlikely that classified research is far and qualitatively ahead, this could change in the future.
The variety in hardware platforms is not atypical even for classical computing. While the frontrunners have had quick wins, scaling at high quality is not straightforward:

[2] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

- Superconductors allow for step-by step engineering with constant challenges in material science and ultimately in scaling beyond the confines of a single cooling system
- Ions enjoy superb coherence and low errors but suffer from a low clock speed and the need to transition to more complex traps
- Neutral atoms have caught up due to their now reliable trapping and quick reconfigurability, and now need to consolidate
- Spins have strong scaling potential but are currently still plagued by noise and space issues
- NV centers show excellent performance and an optical interface, but are challenging to scale to multiple centers
- Photons are the ultimate coherent qubits but require extra steps to make multi-qubit gates

3 Evaluation systems for quantum hardware and quantum algorithms

In this chapter, two evaluation systems are introduced: one for quantum computing hardware and another for quantum algorithms. To this end, we first provide some background information on different models of quantum computation and quantum algorithms. The relevant background information covers quantum hardware and quantum algorithms, gate-based and adiabatic quantum computing, and the distinction between fault-tolerant vs Noisy Intermediate Scale Quantum (or NISQ) computing. At the end of this chapter, we also discuss certain risks that pertain to our evaluation scheme.

3.1 Structure and requirements of an evaluation system

3.1.1 Introduction

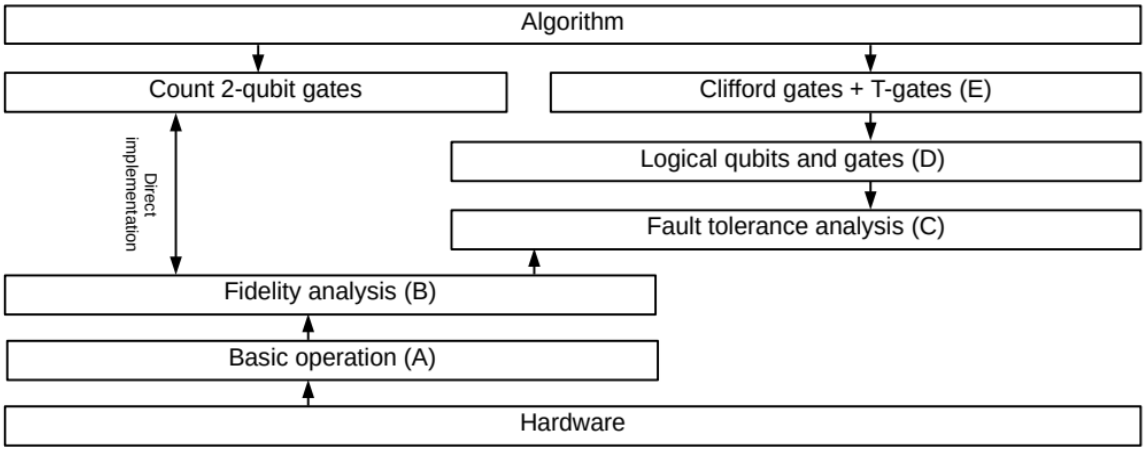

Figure 3.1: Sketch of interdependencies of our evaluation scheme. Hardware needs to pass checkpoints from below, software is compiled from above. These checkpoints, labeled (A) through (E), form the levels of our hardware evaluation scheme introduced in Section 3.3.

A quantum computer is a complex piece of technology that needs to function on many levels. Its basic components—qubits—are intricate physical objects based on pushing some experimental modality to its extremes. At the same time, quantum algorithms are quite complex structures to run, despite the expected power of quantum computers. Figure 3.1 shows how these two concepts are connected in a dependency graph. This graph shows a list of hardware levels, labeled (A) though (E), which are introduced below in Section 3.3. The challenge of evaluating the status of quantum computer development is essentially an exercise in evaluating the machine on all these levels and connecting them.

Over the last few years, the number of approaches to quantum computing has increased on the algorithmic side and consolidated on the hardware side. This is driven by the creativity of a growing community and an increasing hype. Specifically, the computational models in which algorithms can be formulated and the possibilities and limitations of quantum hardware inspire each other. While many of these computational models are in principle equivalent, precise determination of their potential for cryptanalysis and estimations of their development require a more detailed analysis. The concept of quantum computation is divided into several categories. One dividing line is the computational model, chiefly the distinction of adiabatic vs gate-based quantum computing (see Section 3.1.3.) The other one addresses the intrinsic errors in quantum computing and how to take them into account in the computing regimes of fault tolerant and NISQ computation (see Section 3.1.2).

3.1.2 Fault tolerant quantum computation vs NISQ computation

The predicted computational power of quantum computers comes with the drawback of being confronted with a wealth of error mechanisms. On the one hand, these are based on the analog character of stored data, on the other hand on the exponential capacity of quantum computers that allows for ma more places for errors to occur. The traditional remedy is to store each logical qubit using multiple physical qubits and thereby correct errors, thus enabling for the paradigm of *fault-tolerant quantum computation* (FTQC). This computation is based on the concept of quantum error correction, which makes the key prediction that the logical error rate can be reduced arbitrarily by introducing overhead if the physical error rate of a quantum computer is below a threshold p_{th}. This standard paradigm is the core of the hardware evaluation system introduced below and applied in Part IV.

In Ref. [Pre18], John Preskill describes the current experimentally available quantum computers as belonging to what he calls the *NISQ* era, where NISQ is short for *noisy intermediate scale quantum*. NISQ computing has since been broadly adopted as the name of the main alternative route for quantum computer applications, in which no quantum error correction is employed. The NISQ category is generally considered to comprise quantum computers with up to several hundreds of qubits [Pre18].

Preskill asked in as early as 2012, under what minimal requirements it is possible to outperform a classical supercomputer using a quantum computer, or, in other words, at what point one could reach quantum supremacy [Pre12]. As a benchmark, current supercomputers can maximally simulate the time evolution of about 50 qubits ([RMR+07,SSAG17,HS17,DRJ+19]). One would first expect these to be *logical* qubits in the sense of error correction.

The best error complete and scalable correction code (currently the surface code) has a threshold of $p_{th} \simeq 1\%$, which means that for manageable overhead the community aims for errors below 10^{-3}. Of course, moderate improvements beyond this number are conceivable, so we assume relevant errors to be upper bounded by $p \simeq 10^{-5}$ in the foreseeable future. We note that usually the largest errors occur during two-qubit gates. Since most errors will add up during the computation[3], the maximal number of gates, $N_{\max}$, is upper-bound by $p^{-1} \simeq 10^5$, because $N_{\max}$ gates create an error with probability p, such that in the expectation value is exactly one error.

The maximal number of gates is then further limited by decoherence, an effect that also targets idle qubits, which do not undergo a quantum gate. This maximal number moreover admits as upper bound $N_{\max} < T_2 / T_{\text{gate}}$, where T_{gate} is the duration of a two-qubit gate (as the most demanding elementary gate) and T_2 is the decoherence time of a qubit. We note that estimating the upper bound of $N_{\max}$ in this case is less useful, since both the gate durations and decoherence times vary strongly from one quantum computing platform to another.

One can thus ask whether quantum supremacy can be reached without error correction and by carrying out up to $p^{-1} \simeq 10^5$ gates. Indeed, [BIS+16] shows that such a quantum system can simulate quantum chaos in an exponentially large dimension, and that simulating quantum chaos, specifically sampling from the Porter-Thomas distribution is likely an NP-hard problem. In 2019, quantum supremacy along these lines has been experimentally demonstrated by Google [AAM+19]. Similar results have been obtained for variational quantum simulation [OBK+16, DDW16, BWM+16], where the quantum advantage comes from the need to store a complex quantum state (i.e., problems that on classical computers are memory-limited). Such developments, which highlight the potential power of quantum computers, are a strong driver of near-term quantum computer development.

Reliably executing a quantum algorithm requires running it at a fixed and usable error rate of the binary input and output of the algorithm. By *fixed* we mean that the error rate does not grow with a longer algorithm, by *usable* we mean that a small number of runs of the algorithms should lead to an acceptable result. The complexity of quantum algorithms that outperform classical supercomputers requires a large number of gates, hence the error per of logical quantum gate needs to be comparatively small. On the one hand, in classical computers, where data encoding is strictly binary during the entire computation and

[3]Under certain circumstances errors may cancel one another during the execution of a quantum algorithm, which would allow for longer gate sequences. Work on such error cancellation is discussed in Section 5.6.

energy barriers lower the error rates to nearly negligible values, this can be reached in hardware. Quantum computers on the other hand, while operating in a binary data space and having simple binary data as input and output, use superpositions and entangled states during the computation, which are fragile to continuous errors. Similar to classical computers, there is a quantum measurement of binary registers at the end of the calculation, and any accumulated errors will result in a finite probability of obtaining a wrong outcome. Since there is no self-correcting energy barrier for quantum computing (we will discuss a topological barrier below), intrinsic error rates of physical qubits cannot be expected to ever be as low as required by algorithms, so one stands before the challenge of executing an algorithm with faulty hardware.

This can be addressed with *fault-tolerant quantum computing.* Fault tolerant quantum computing draws a distinction between the faulty *physical qubits*, which are used in a laboratory, and the low-error *logical qubits* in which an algorithm is implemented. Logical qubits, each of which is redundantly encoded into multiple physical qubits, are steadily error-corrected, resulting in logical errors rates that are below those of the physical components. We will make sure that we clearly label—often by chapter—whether physical or logical qubits are addressed. We will analogously talk about physical and logical operations depending on whether these are operations on physical or logical qubits.

These two layers are connected by fault-tolerant quantum computing protocols. These have been developed for more than two decades and their basic ideas are written in textbooks [NC00]. The efficiency of these techniques has been dramatically improved by the introduction of the *surface code,* an error-correction scheme that uses topological ideas to protect data—only errors that change topological properties of a state are not noticed. Note that topological qubits (see end of Section 12.2.2.1) use these ideas on an elementary physical level, whereas the surface code is assembled from ordinary qubits.

We describe basic notions of fault-tolerant computation in the introduction of Chapter 8. Here we already highlight its main ingredients: i) error syndrome extraction and correction in a stabilized code space, which includes reducing analog error probabilities to digital errors, ii) storage of logical qubits, iii) implementation of "easy" logical operations (typically the full set of Clifford gates) and iv) implementation of the remaining gates for forming a physical gate set, typically the *T* gate. These operations generally introduce a large overhead—a logical gate requires repeated error correction and generally consists of many physical operations on many physical qubits, all of which are in general faulty. For a well-designed code, there is a *threshold theorem* stating that under generic assumptions of the error model, the logical error rate can be made arbitrarily small with finite overhead, as long as physical error rates are below a certain threshold.

3.1.3 Gate-based vs adiabatic quantum computation

In 1980, Paul Benioff introduced the first formal descriptions of a quantum computer as a quantum Turing machine [Ben80]. Several years later, David Deutsch formulated a description of a quantum computer that can be viewed as a quantum equivalent to the gate-based classical computer [Deu89], which has been adopted as a mainstream quantum computing paradigm [NC00]. The basic idea behind this *gate-based quantum computation* is that, while in a classical computer data is processed by the application of logic gates such as NOT, XOR and NAND, quantum generalizations thereof (universal gate sets) are used similarly to process quantum information.

An alternative computational model is called *adiabatic quantum computation* [AL18b]. The concept in this case is that the solution to a posed problem is encoded into the ground state of the quantum mechanical energy function of a system, i.e., a *Hamiltonian*. In the case of quantum cryptanalysis, these Hamiltonians will be diagonal in the computational basis – capturing the minimization of a binary function. If the problem in question is nontrivial, this ground state will be difficult to determine using conventional methods. Instead, it can be found using adiabatic quantum computation by first initializing a set of qubits into the ground state of a Hamiltonian that can be understood analytically, and then transforming this Hamiltonian slowly until it equals the Hamiltonian whose ground state we seek. Appendix 14 describes an exemplary adiabatic quantum algorithm for factoring, which is designed to be run on gate-based quantum computers in a scheme called *digitized adiabatic quantum computation*. To remain adiabatic, it is necessary that the runtime of the algorithm is long enough, controlled by the inverse spacing of the lowest two eigenvalues of the Hamiltonian during the computation (called the energy gap). Determining the runtime of an adiabatic algorithm is thus based on estimating the energy gap.

It has been known since 2001 that adiabatic quantum computing can be simulated efficiently by quantum circuits [vDMV01]. In 2007 Aharonov et al. established that the converse direction also holds, i.e., the quantum circuit model is polynomially equivalent to adiabatic quantum computation [AvDK+07]. This equivalence assumes certain hardware prerequisites as well as the polynomial computational overhead. Adiabatic quantum computing belongs to the larger class of Hamiltonian computing models [Ken20], which also contain quantum walks [Chi09], which can be invoked as a subroutine for some tasks in cryptanalysis. As there is hardly any quantum walk-specific hardware, we will address quantum walks in a version compiled to the gate model.

3.1.4 Variational quantum computing

The quantum approximate optimization algorithm / quantum alternating operator ansatz (QAOA) [MBB+18FGG14, FGG15 BBC+24] is an algorithmic heuristic that can be used to solve combinatorial optimization problems on a gate-based quantum computer. It is inspired by adiabatic quantum computing. The adiabatic time evolution is discretized in time by a Trotter decomposition into alternating layers of problem and driver Hamiltonians. Based on the output, a classical optimizer is used to optimize the duration of the different layers. This gives the algorithm a structure similar to a neural network. The QAOA allows to use the techniques developed for gate based quantum computing (compilation, error mitigation) in the context of optimization.

While large-depth QAOA - i.e. a fine-grained discretization of the time evolution - is equivalent to AQC, there is a hope that also low-depth / coarsely discretized QAOA leading to a low-depth, NISQ-friendly quantum algorithm could lead to applications and ultimately quantum advantage, making use of the classical training loop. QAOA is at the heart of optimization-type cryptanalytics quantum algorithms (see Sections 4.3.1, 5.2.3).

A procedure like this does not lend itself to a definitive proof of convergence. Indeed, a first analysis of speedup was refuted by a new classical algorithm [Has19]. A suitable criterion for the delineation between polynomial and exponential time is the occurrence of barren plateau (BP) [LTW+24] . These are situations in which the gradients of the cost function that the classical optimizer needs to converge are exponentially small in the problem size. That means, the time step of the optimizer used in QAOA becomes exponentially small, and the computation time exponentially scaling. This is a natural consequence of a small number of parameters steering an exponentially large space. So the occurrence of barren plateaus rules out fast convergence and hence at least clear quantum advantage.

Barren plateaus can be induced by noise - which can be used to evaluate implementations of QAOA, if QAOA provides quantum speedup at all. At the current stage, we are more concerned with intrinsic barren plateaus that occur even in perfect quantum computers. Here, there is mounting evidence in various forms that Barren plateaus are hindering quantum speedup of QAOA quite generally:

1. It has been shown that one needs to exploit additional structure of the problem in QAOA to avoid BPs and conjectured that these same structures render the problem classically simulatable [CLGM+23]

2. It has been shown that BPs are related to the underlying Lie-Algebraic structure of the problem. This is the primary avenue for simulability - if the structure is easily fragmented into small subspaces, the problem is easily solvable classically - if a large subalgebra remains, it will have barren plateaus. [RBS+24 ; R. Zeier, private communication]

3. A robust quantum-inspired classical algorithm as a limiting case of QAOA has been provided [MSBS+23]

The results described here allow for small loopholes in their assumptions. Nevertheless, we assume that QAOA can only provide a route to quantum advantage, if the occurrence of barren plateaus is explicitly addressed.

3.2 Evaluation scheme for quantum algorithms

Quantum algorithms can be grouped into different categories based on the following three properties. (i) For certain algorithms, the termination behavior is mathematically proven. For instance, it has been established that the required number of quantum gates for integer factoring represented by *n* digits using

Shor's algorithm (on an ideal quantum computer) is upper bounded by a polynomial in n. In contrast, for several more recent quantum algorithms for factoring integers, this scaling of the number of quantum gates is not known, and even termination may not be certain. (ii) A second property is that of the use of quantum gate types: The proposed set of gates for a given quantum algorithm can be a minimal set, which consists only of a few elementary gates, or it may require a substantial number of distinct gates – which could either be compiled to a minimal gate set or be directly provided by co-designed hardware. (iii) Finally, a third distinguishing characteristic of an algorithm is whether it is proposed to be run on a NISQ computer, or if the usage of a fault tolerant scheme is required to solve problems of relevant input sizes. This difference is not sharp, but in general NISQ-ready algorithms are aimed at low depth between different readout and initialization cycles. Our evaluation scheme for quantum algorithms described below distinguishes between quantum algorithms intended for either NISQ computing or fault tolerant gate-based quantum computing.

The performance of a quantum algorithm strongly depends on the available hardware – not only by a single performance parameter, but also in the sense that some algorithms are more suited to a specific hardware platform than others. The crucial hardware properties go beyond the error rate, number of used qubits and clock speed (or the duration of elementary quantum gates) of a quantum processor. The most important other factors are the types of native quantum gates that can be carried out and the inter-qubit connectivity of the device, which determines which qubits can be coupled.

In general, the ability to carry out many different native gates and to be able to connect many qubits is beneficial. However, different quantum algorithms usually have different requirements on native quantum gates and connectivities. In this context the notion of co-design comes into play, in which hardware and algorithms are designed alongside one another to realize a special-purpose quantum computer that excels in running certain types of algorithms. The principle of co-design is reviewed in Reference [LWS+21LWS+21]. Co-Design and hardware adaptation are crucial for the lowest software layer, i.e., for the error correction code in the case of fault-tolerant quantum computing and for the full algorithm in the case of NISQ.

Figure 3.2 gives an overview of our level-based evaluation scheme concerning soundness and criticality of quantum algorithms with relevance for cryptanalysis. As shown in Figure 3.2, this scheme consists of two vertical threads and three horizontal layers labeled A, B and C. In layer A, one first determines whether an algorithm belongs to the left or the right thread. This depends on the question if there is a known proof of the termination properties of the algorithm, or if these properties need to be inferred by heuristics. The former and latter types of algorithms will be assessed according to the left and right threads, respectively.

Algorithms with a known proof of termination, which belong to the thread on the left of Figure 3.2, are evaluated as follows:

- *A*: Consider the theoretical assumptions of the proof of termination. Is the proof based on any controversial unproven theorems or disputed conjectures?
- *B*: Consider the algorithm's assumptions on hardware resources, which are prerequisites to the result on termination. Are these assumptions compatible with hardware that is currently being developed?
- *C*: Carry out a rigorous resource analysis of the fault tolerant implementation of the algorithm. This will yield the required numbers of qubits and the run time of the algorithm as a function of input size and error rate of the quantum computer.

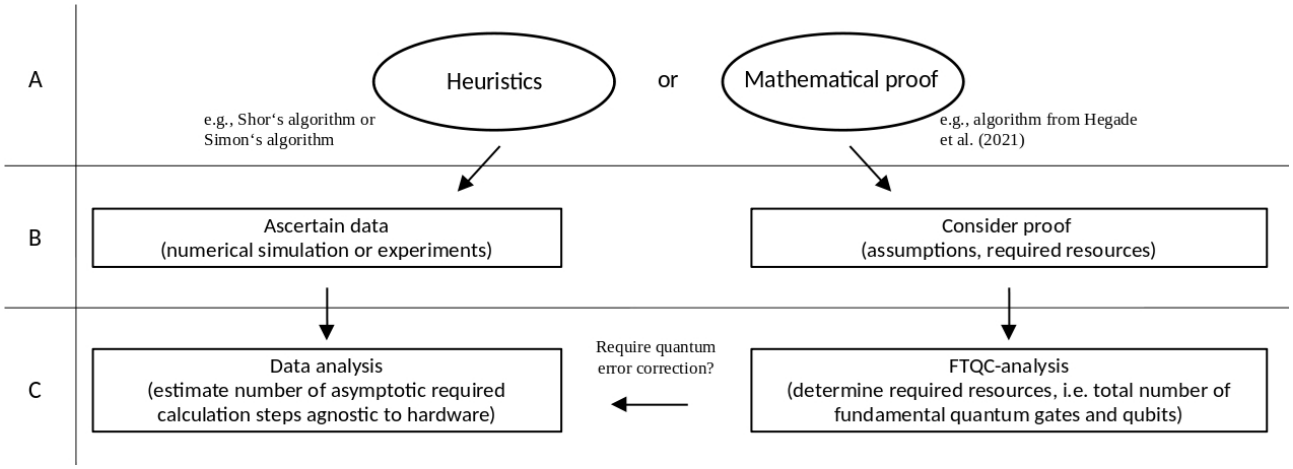

Figure 3.2: Evaluation scheme for quantum algorithms. Three levels A-C denote the algorithm's maturity, which is based on the current state of knowledge. There are two main types of algorithms, since an algorithm can be based on mathematical proof or, if no proof is known, on heuristics. Section 3.2 gives a detailed description of the evaluation levels.

Turning to algorithms without a known proof of termination, note that these algorithms may be tested using NISQ computation already. NISQ computers, described above Section 3.1.2, can only carry out a limited number of quantum gates in a single run, since the lack of error correction results in an inevitable accumulation of errors that will eventually spoil any calculation. After a maximum number $N_{\max}$ of gates has been applied, the qubits will be reset for the next run. As noted above, for a given gate error probability p, which is related to the fidelity $F = 1 - p$, the maximum number of quantum gates is of the order of $1/p$. For most quantum computing platforms, single-qubit gates exhibit significantly smaller errors than two-qubit gates, because of which usually two-qubit gate errors are used to estimate the number $N_{\max}$. As discussed above in Section 3.1.2, we assume the number of realizable gates $N_{\max}$ to be bounded by $p^{-1} \simeq 10^5$.

To repeat, a NISQ algorithm can only be experimentally feasible if the number of quantum gates per run does not exceed the current maximum number of implementable gate operations. As stated above, at the time being this number is upper bounded by $N_{\max} = 1000$. For example, to feasibly run a factoring algorithm for a 1000-bit integer N, $n = \log_2(N) = 10^3$, this implies that the number of gates should scale rather slowly. Indeed, if the number of quantum gates were to scale as in the case of Shor's algorithm (assuming perfect quantum gates) with n^3, this would result in $n^3 = 10^9$ gates, which lies many orders of magnitude outside the scope of current NISQ devices. While this notion seems to limit NISQ algorithms significantly, it should be noted that algorithms may feature multiple short runs (or gate sequences of *low depth*) on the quantum computer for a single calculation. Reinitialization between one run and the next allows reusing the qubits anew. A popular class of such algorithms, known as variational quantum algorithms, is reviewed in [CAB+21].

Based on the discussion above, we state the following set of criteria for our level-based evaluation scheme:

- A: Plausibility of NISQ algorithm.

First, the algorithm is evaluated based on its operating principles. Is the fundamental paradigm (e.g., adiabatic quantum computation, or variational quantum factorization) of the algorithm established? Are there technical difficulties with any part of the method? For example, if classical processing is a part of the algorithm, how efficient is this part?

- B: Is there enough data available for an analysis of the algorithm's asymptotic cost function?

Gather accessible data supporting the algorithm. The quantity of interest, the algorithm's hardware-agnostic cost function[4] is the number of required quantum gates as a function of input size. Such an

[4]For an impartial comparison, the cost function should be chosen agnostic to hardware. To this end, we choose the number of computation steps, or the ratio of the algorithm's run time and the duration of a clock cycle.

analysis only yields meaningful results if the amount of data (i) is large enough in number, and (ii) spans at least one decade on both axes (cost function and size of input).

- C: Does available data give an indication for critical asymptotic termination?

If there is adequate data, the scaling behavior of the cost function as a function of the input size can be estimated. Relevance can be considered, if the predicted number of required quantum gates for breaking relevant cryptography is within reach, i.e., of the order of $p^{-1} \simeq 10^5$ gates). Note that any such result must be treated merely as an *indication* of relevance, since numerical data cannot predict asymptotes with absolute certainty.

If the number of quantum gates for cryptographically relevant input values exceeds the expected capabilities of NISQ computers, the quantum algorithm may be executed on an error corrected quantum computer. This is indicated by the horizontal arrow in level C in Figure 3.2. In this case the evaluation will be carried out following our FTQC analysis.

3.3 Evaluation scheme for quantum hardware

The scheme proposed here is constructed *bottom up* in the sense that high-level features can only be successfully completed if all lower-level requirements have been met. We feel that this is important, given that some types of engagement in quantum computing research trigger hyperbole and press releases that often highlight advantages on one level only while omitting failure on other levels. Note that inside these levels there are often multiple requirements; however, passing these requirements in a certain order is usually not critical.

Our hardware evaluation scheme is driven by the demands of FTQC as this is identified as being necessary for proven cryptanalytic applications, but also contains the elements to evaluate NISQ. We now outline the structure of the scheme in a preview that highlights how its different components work together.

3.3.1 Lowest level (A): Basic operation—do we have working qubits?

At the lowest hardware level, physical modalities encoding qubits can and will be vastly different. To make them upwardly compatible, they need to function as qubits in the broadest sense. Here, the question is whether all basic functionalities are present, which allows one to consider running a low-level quantum algorithm. From a fault tolerant quantum computing point of view, these operations are deemed physical rather than logical. We propose a set of criteria in Chapter 6, which are an extension and quantification of the well-known DiVincenzo criteria. Platforms passing this test quantitatively will typically be able to demonstrate some basic quantum algorithms with two to five qubits. Most promising platforms considered in this study have passed this lowest level.

3.3.2 Intermediate level (B): Benchmarking—does our hardware meet fault tolerance criteria?

Once basic qubits functionality is established, it is important to *quantitatively* evaluate the performance of given hardware in a matter that is compatible with fault tolerance—but largely agnostic to hardware. Still, all operations discussed here are physical operations. Hardware may drive the choice of computational model (circuit based, adiabatic, cluster states) and fault tolerance scheme (surface or color code) but performance needs to be quantified in a way that is compatible with the analysis of fault tolerance. These numbers are essentially some qualitative statements about the architecture (how many operations can be parallelized? Can measurement be used as qubit reset?) but boils down to *fidelity measures* of the basic operations in fault tolerant computation—initialization, gate operations, and readout. There are established methods to extract these parameters [BKGN+13], though improving these is work in progress. As reliable estimation of these parameters requires a quantum processor with some basic functionality, in particular faithful measurement, and the ability to run at least in principle a long gate sequence, it is important that processors have passed the level A to make meaningful statements. Benchmarking not only allows passing level B, i.e., confirming error rates compatible with useful FTQC, but it also determines the design parameters of the fault-tolerance algorithms that are used in order to address level C. In NISQ

computation, we directly transition from this level to full algorithmic benchmarking, which can be estimated by counting the two-qubit gates in the algorithm which consistently are limiting the total fidelity (cf. Section 3.1.2).

It is remarkable that most platforms reach similar values of the limiting factor, two qubit gate fidelities, here, typically around 99.5% for the leading experiments, whereas single-qubit fidelities are in general higher for smaller qubits (single atoms or ions) than for larger qubits (superconductors).

3.3.3 Central element (C): Fault tolerance analysis—how much quantum volume can we execute?

Once fault tolerance criteria are met from the intermediate level, it is known that adding more error correction (i.e., larger codewords, larger code distances) will reduce the logical error rate. Thus, with information from the next higher level (number of logical qubits and logical gate count) as well as below (architectural constraints and operation fidelities of the physical qubits) we can estimate the number of physical qubits and the time to execute an algorithm on given hardware thus estimate the *effective physical size* of the quantum computer that can execute the *effective logical volume* of the algorithm of interest. We describe its principles along with the most commonly used technique, the surface code. We provide concrete numbers allowing physical resource estimates.

The improvement of logical error rate over the physical error rate can be achieved in different steps. This is because there are independent types of qubit errors, and because error correcting codes need to fulfill a certain error behavior as a function of the size of the code. Intermediate steps of level C are discussed in Section 8.5.1.

3.3.4 Compiled level (D): Elementary fault-tolerant gates

Transitioning to the software layer, algorithms need to be broken down into elementary gates on *logical* qubits. The gate set of interest depends on whether active error correction is required – this is, indeed, assumed throughout, except in the discussion of NISQ algorithms. The requirement is the ability to carry out a universal gate set. Many gates can be executed straightforwardly without leaving code space, and these are relatively easy to implement—in the case of the surface code, one of the best error correction codes known to date, these are all the Clifford gates. Executing a general quantum algorithm that *cannot* be classically simulated requires at least one non-Clifford gate that needs to be produced outside the code. As this is generally by far the most resource-intensive step, a single non-Clifford gate, typically the T gate (a phase shift of $\pi/4$ on one of the two basis states) is implemented. Accordingly, desired quantum algorithms are broken down into Clifford+T, i.e., gate counts for both Clifford and T gates are given.

The execution of fault tolerant gates can be realized in different scenarios worth mentioning. First, the realization of single qubit gates is simpler compared to two qubit gates. Second, the difficulty for carrying out Clifford gates is significantly simpler than that of non-Clifford gates. Intermediate steps of level D are discussed in Section 8.5.1.

3.3.5 Algorithmic level (E): Fault-tolerant algorithms

In this layer, meaningful algorithms can be executed fault-tolerantly. In a first step, cryptanalytic algorithms are commonly formulated at a high abstraction level. Details of implementing the necessary arithmetic, e.g., on an elliptic curve, or how to perform the round function of a block cipher with a superposition of inputs are not considered. To bring a quantum computer to use, the portions of the algorithm that cannot be run on classical hardware need to be identified, and design decisions on how to map abstract operations onto the available hardware need to be made. Just as with classical implementations, different algorithmic choices are possible, e.g., for computing an inversion modulo a prime number or for implementing an S-box. Different optimizations can be pursued—like minimizing the number of logical qubits or reducing the circuit depth of a computation. Cryptanalytic algorithms tend to involve complex operations, and as long as reliable libraries for elementary tasks are lacking, it seems prudent to organize the algorithm at hand in such a way that debugging remains feasible when passing to the gate level.

3.3.6 Conclusions and application

Once the numbers of required qubits and elementary quantum gates for a given task are determined, which means that we have a firm understanding of the algorithm's size, we can estimate extensive operational parameters (volume, heat dissipation, power consumption, amounts of rare substances etc.). Moreover, we can evaluate if scaling up requires hitherto non-existing technologies, for example if multiple experimental infrastructural units need to be connected (multiple cryostats, multiple optical tables, multiple UHV systems). This results in an assessment of the feasibility and scope of building such a machine, and according criteria for such a construction are laid out in Chapter 10.

3.4 Risks of our evaluation scheme

Our evaluation scheme rests on the status of current research and knowledge. Some of these results are extrapolations over many orders of magnitude in size and performance, specifically error rate. We would like to succinctly describe the known risks that this scheme could be wrong, which can only be assessed as research, mostly experimental research, progresses.

3.4.1 Risks that make quantum computers more reachable

1. We have assumed that cryptanalysis requires long skinny algorithms hence requiring error correction. Discovery of an algorithm that trades time for memory in a way that can be addressed with a small number of gates would make the target processor much smaller. This risk is medium, as more and more ideas are appearing, even though so far none shows a clear path to quantum advantage.
2. Discovery of physical qubits with extremely low intrinsic error rate. In principle, this is possible - control of qubits can be done with non-dissipative elements that do not produce errors. As the prime candidate, topological qubits, have recently suffered from a serious setback, and as quantum errors are for fundamental reasons more likely than classical errors, this risk is low.
3. Discovery of scalable qubits with long-distance interaction with the ability to implement high-dimensional connectivity: This would lead to very high error thresholds and at least logarithmic savings (cf. Section 8.2.4). Given the progress in neutral atoms, this risk is medium.
4. Discovery of accidental error avoidance in cryptographically relevant algorithms. This is related to the fact that error estimates following the diamond norm are usually very conservative and can in NISQ often be beaten by physics motivated error mitigation and co-design. However, current error mitigation is not efficiently scalable and the dense structure of QFT as the most crucial step of Shor's algorithm makes circumventing this quite unlikely.
5. Implementation of novel, ultra-fast quantum computing platforms in timescales of femtoseconds or attoseconds, the shortest directly accessible timescales in physics. This would speed up physical gate times by three orders of magnitude, making long algorithms more accessible. This has been tried, unsuccessfully, as the two-qubit gates do not benefit from these fast timescales as much as one-qubit gates, and as the classical periphery required to reach low errors is not developed yet. This is a low risk in short- and medium term and a medium risk in the long term. Algorithmic innovations and optimization of the logical encoding: the task of finding the optimal encoding (see [Jon13], or Section 0) and distillation structure (this is discussed in an older version of this study, see Section 7.2.4.3 in [WSL+20]) is not done in full detail in our analysis. While we take reasonable assumptions for required distance, distillation rounds or logical gate arrangement, an optimized version of a fault-tolerant algorithm found from simulations can be made much more efficient in terms of required qubits and error rates (see for example recent advances in [OC17], or different approaches to fault-tolerant Toffoli gate implementations [Jon13]). These optimizations will be done for sure when thinking about implementing large circuits, the correction will be a constant factor improvement (of maybe one or two orders of magnitude). So this is a more significant risk
6. Reaching extreme progress in error correction with transversal *T* gates: very unlikely.
7. Significantly improving scaling of the surface code when using lattice surgery, see [FG18] and our Section 15.4.

3.4.2 Risks that make quantum computers less reachable

1. Serious deviations in going from levels B to C: Even the best methods to measure operation fidelities on level B reveal an incomplete picture. While this risk was prominent in 2023, it has now been shown that it can be overcome. It is still understood that error probabilities measured at level B approximate the success prognosis of level C. This is risk is thus nearly cleared.
2. Discovery of new correlated error mechanisms: Error correction relies on multi-qubit errors being exponentially (in the number of qubits) less likely than single-qubit errors. This problem seemed to limit superconducting qubits but has now been mitigated by the new results at Google – but a nonvanishing noise floor of this errors remains. It remains an intermediate risk.
3. Discovery of persistent non-Markovianity: Similar to spatial correlations also temporal error correlations are difficult to catch. This is unlikely, as measurements usually destroy temporal correlations.
4. Insurmountable engineering problems: Assembling large processors cannot guarantee the same quality as the components. The same would hold for temporal stability when scaling operation time, e.g., spurious heating and drifts. Albeit analyzing these operational challenges is done based on what is known for the level C platforms, there can be challenges that only appear while it is attempted.
5. Dominance of coherent errors: Albeit coherent errors have the same error correction threshold as corresponding incoherent errors, the surface code scales less favorably below threshold, which may increase the overhead. Intermediate risk.
6. Loss of interest in quantum computing in the international community: For potential costumers quantum computation has to offer a real advantage, because of which there is need to attract more communication towards out of field people such as well-educated software application designers. Quantum computation is currently in a phase of steep rise in private and public funding - partially due to a certain media hype enhanced by uncurbed claims of many companies - which leads to the inclusion of a broader community. However, any economic uprising of new technologies brings with it the risk that investors lose interest, which in this case would accordingly slow down progress considerably.

PART II: Evaluation of algorithms

Subsequently we describe quantum algorithmic innovations that are relevant for judging the security of currently prevalent cryptographic solutions. We focus on algorithms that can be applied to classical implementations of cryptographic schemes, e.g., factoring a public RSA modulus or leveraging a collection of known plaintext-ciphertext pairs for a block cipher like AES. We also mention some attacks assuming a stronger attack model, in which an adversary has superposition access to a cryptographic implementation that involves an unknown secret key. While this stronger attack model enables insights about fundamental security limitations, assuming superposition access is not practical for cryptographic implementations commonly used today.

On the side of asymmetric cryptography, we focus on algorithmic innovations (i) to decompose integers into prime factors, which are especially relevant for RSA-based solutions, and (ii) to compute discrete logarithms in suitable finite groups, e.g., on elliptic curves over a finite prime field. The latter are, for instance, relevant for popular digital signatures and key establishment solutions building on the famous Diffie-Hellman design.

On the side of symmetric cryptography, our emphasis is on quantum cryptanalytic insights on popular block ciphers, especially AES, and cryptographic hash functions.

As noted in Section 3.2, quantum algorithms can be grouped into multiple categories. The perhaps most significant distinguishing feature for different kinds of algorithms is whether the expected termination of the algorithm is based on a mathematical proof or heuristics. Another important distinction, which is currently of public interest, is an algorithm's suitability for NISQ computers (see Section 3.1.2) and quantum annealers (see Section 9), as opposed to the need to employ error-corrected or fault-tolerant quantum computers. At the time being, these two qualitative features are not unrelated to one another. In the first place, the only realistic implementation of cryptanalytic algorithms with a known proof of termination requires the use of a fault tolerant quantum computer. Such algorithms are analyzed in the following Chapter 4.

4 Algorithms with proof of termination

Quantum attacks against symmetric and asymmetric primitives have quite different flavors. Based on our current understanding, the cryptanalytic impact of quantum computing on established public-key encryption schemes, digital signature solutions, and key-establishment protocols is much more severe than on popular block ciphers or cryptographic hash functions. We start by a look at the quantum cryptanalysis of important symmetric primitives.

4.1 Minimizing quantum circuits

When discussing quantum circuits, different elementary gate sets are possible, and it is common in the literature to start out with classical reversible circuits, which are then translated (without further low-level optimization) to a particular universal gate set. It is reasonable to assume that such "naïvely compiled" circuits can in general be optimized further. Minimizing quantum circuits at the lower level is an active research area, and much emphasis is currently placed on the Clifford+T gate set. The latter can be implemented in a fault-tolerant manner, e.g., by means of surface codes [FFSG09, FMMC12]. Using number-theoretic tools, Kliuchnikov showed how an arbitrary unitary transformation on n qubits can be approximated with precision ϵ using a Clifford+T circuit of size $O(4^n n(\log(1/\epsilon) + n))$ and two ancillas [Kli13]. This approach is optimal, if the number of qubits is fixed. For 4-bit circuits, the problem of finding optimal reversible decompositions has been solved [GFM10], and from a cryptanalytic angle this is rather useful. For instance, the S-boxes of the block cipher Serpent operate on four bits, and in an exhaustive key search with Grover's algorithm this result can be leveraged to derive efficient quantum implementations of Serpent's nonlinear part.

Heuristic techniques and manual optimization of quantum circuits have occurred regularly in the quantum-cryptanalytic literature. For instance, algorithmic tools from permutation group theory (cf. [GLRS16]) can be leveraged on the level of reversible circuits: modeling NOT, CNOT, and Toffoli gates as generators of a permutation group, expressing an AES S-box in these gates can be translated into a word problem. However, over the years, more powerful software tools have emerged, and they find broader use in the quantum cryptanalytic community, leading to improvements in the derivation of efficient quantum circuits. An interesting example is work on AES by Jaques et al. [JNRV20], which leverages Q# for circuit optimization and resource estimation. However, as discussed by Huang and Sun [HS22, Remark 3], such automated resource estimation still requires some care, and software errors occur. Still, in view of the complexity and size of quantum cryptanalytic circuits, it is reasonable to expect that automated tools will further gain popularity, leading to improved/more efficient circuits.

Measurement-based uncomputation has gained some popularity to implement pertinent arithmetic (e.g., an AES S-box [JNRV20] or computations on an elliptic curve [HJNRS20]). Instead of translating Toffoli gates in a classical reversible circuit directly into a Clifford+T circuit, AND gates are used. To realize such an AND gate (and thereby multiplication in GF(2)), an ancilla qubit is used, and uncomputation involves the execution of gates conditioned on the outcome of a measurement. Key feature of this approach is that – at the cost of a measurement and conditioned operations – T gates can be avoided. For instance, an AND gate implementation described by Gidney [Gid18, Figure 3] involves 4 T gates (along with some Clifford gates), and the uncomputation can be done without any T gates (but involves a measurement).

Because of the complex design space, developing suitable software tools to support the quantum circuit design process is a natural approach to take. Work by Paler et al. [POB22] evidences that intuitive design approaches may be misleading, e.g., reducing the number of T gates may end up being detrimental to the circuit depth. Interestingly, the (classical) cost to optimize large-scale quantum circuits can become non-trivial. Paler and Badmadjian [PB22] looked at the (energy) cost for optimizing multipliers as used in a large-scale quantum circuit for mounting an attack with Shor's algorithm. Their work suggests that, with the available techniques, the energy cost for optimizing a multiplier may already for 8192-bit numbers approach the magnitude of a Giga-Watt hour.

4.2 Algorithmic innovations with relevance for symmetric cryptography

Despite an increasing number of results on more sophisticated quantum attacks against symmetric building blocks, Grover's algorithm [Gro96] remains the most prominent quantum algorithm that is known to be applicable to the analysis of symmetric cryptographic primitives. So, we start by looking at this search procedure. After addressing its application to a key search for a block cipher, we discuss its use for preimage and collision attacks on prominent hash functions. In terms of the evaluation scheme from Section 3.2, Grover's algorithm is (A) provably correct, and (B) its hardware requirements are compatible with hardware that is currently developed. The algorithm assumes a fault tolerant implementation, and we address (C) available resource analyses for important cryptographic use cases below.

4.2.1 Grover's algorithm

Even though the running time improvement of this algorithm over a classical solution is only in the order of a square root—and therefore, an exponential time bound still remains exponential—the speed-up is relevant when quantifying security margins. In general, Grover's algorithm is a versatile tool for hybrid attack strategies: one tries to rephrase a(n exhaustive) search inside some classical cryptanalytic approach in such a way that the requirements of Grover's algorithm are met. Ideally, one can in this way expedite a time-critical component of the classical attack with a quantum subroutine, possibly even with an asymptotic gain. Arguably the two most prominent cryptanalytic applications of Grover's algorithm are

- Speeding up an exhaustive key search against a block cipher.
- Speeding up a preimage search against a hash function.

Loosely speaking, Grover's Algorithm can complete a search of a space of size 2^n in $2^{n/2}$ steps (with very high probability), therewith offering a substantial speed-up over a classical search that would take on average 2^{n-1} steps. To protect against a Grover-based key search, doubling the key length (n) is a natural strategy to consider, if this is feasible – Bhaumik et al. [BCFNP22] explore this in more detail.

At the core of Grover's algorithm is a Grover operator which encodes a predicate that decides if a candidate element meets our desired search criteria. If there are M elements satisfying this predicate in the search space of size N, the Grover operator needs to be applied $O((N/M)^{1/2})$ times. In the case of a uniquely characterized secret key of a block cipher (through a collection of plaintext-ciphertext pairs), the total number of times the Grover operation would need to be run can be calculated easily based on the key size. For a key of size n, this number is $\lfloor(\pi/4) \cdot 2^{n/2}\rfloor$, or approximately $2^{n/2}$, but this can only give a lower bound on the attack costs (qubits, gates, and depth), as the implementation cost for the encryption scheme itself plays an essential role—the details of the Grover operator depend on the targeted primitive. In a 2023 preprint [SW23], Stoudenmire and Waintal suggest that "that there is no a priori theoretical quantum speedup associated with Grover's algorithm." The preprint received significant criticism [Aar23], and the asymptotic speed-up of Grover's algorithm, in the appropriate theoretical model, is not in question in the research community.

While using a high-level description of Grover's algorithm to compute the cost of breaking symmetric cryptographic systems such as AES-k (k = 128,192, 256), MARS, SERPENT, SIMON, SPECK, etc. is the right approach, the details of the cost can vary greatly and rely heavily on the key size as well as the implementation complexity of the cryptographic system.

Note: Grover's search algorithm was proved optimal for quantum searching, and it allows no non-trivial parallelization [Zal99]; improvements would require an attack on the targeted cryptographic scheme itself. More specifically, Zalka's work implies that giving a quantum algorithm access to s identical oracles that uniquely characterize an n-bit key with plaintext-ciphertext pairs, we can obtain a speed-up of at most a factor $s^{1/2}$. This is no better than running s independent Grover searches, each on a size $2^n/s$ subset of the key space.

In cryptographic terms, suppose we have a symmetric encryption scheme F that takes a 128-bit key k as input to encrypt a plaintext P into a ciphertext $C = F_k(P)$. In order for Grover's Algorithm to work, we would

need a plaintext-ciphertext pair (P,C) and a quantum realization of the symmetric key encryption scheme F. The result of the algorithm will with high probability be the appropriate key k^*, which when used in the encryption scheme yields the correct ciphertext. To characterize the target key uniquely (or at least reduce the number of candidates to a small set) multiple plaintext-ciphertext pairs may be needed—a typical estimate being 2 or 3. This causes no fundamental difference for mounting the attack but impacts the amount of quantum resources needed.

Grover's algorithm creates a superposition of all candidate keys, so that each key has equal probability. The algorithm runs the superposition of keys through F^*, which is a Boolean function that returns 1 if and only if the key is the correct key and 0 otherwise. For instance, F^* can verify if a candidate key matches one or several plaintext-ciphertext pairs. A key k being correct translates into the condition $F_k(P) = C$. Owing to the superposition, each possible key is in effect tried simultaneously and the one correct key (here we are assuming there is only one correct key) will be "tagged." Once the correct key is "tagged," the second phase of the Grover algorithm, the diffusion operator, is run. This increases the likelihood of the correct key being produced when measured. These two phases represent one iteration of the Grover algorithm. Since each time the two phases are run, the probability of the correct key being measured increases, if measured after the correct number of iterations, the correct key would be produced with high probability.

Note that to evaluate the Boolean function F^*, the full encryption process must be implemented on the quantum hardware and then its result can be compared to the known ciphertext. While the final comparison is a simple and short quantum operation, the depth and cost of implementing the encryption scheme can vary drastically and is needed at least once in each iteration of the algorithm. This means not only will, say AES-256, take more iterations of Grover than AES-128, each iteration will probably require more quantum gates and qubits, increasing the overall cost further. This additional cost may or may not be negligible in comparison to the Grover operations, but for a system such as AES-128 which would take approximately 2^{64} iterations of Grover, it is a pertinent factor to consider in a quantitative analysis.

Case study: the AES family

The Advanced Encryption Standard (AES), designed in 1998 by Rijmen and Daemen and accepted by NIST in 2001 [NIS01] as the replacement for DES (Data Encryption Standard) [NIS99] is a subset of the Rijndael cipher [DR99]. AES encrypts with three different key sizes (128, 192, and 256 bit) and all three have been adopted world-wide and are of cryptographic interest. In [GLRS16] a first cost analysis – at the logical level – of implementing AES-128, AES-192, and AES-256 as a quantum circuit has been given. Since then, a series of works identified improvements and different designs. A key design parameter is the handling of the S-box, which is the only part of AES that requires the use of non-Clifford gates, and ignoring or using the algebraic structure of this specific S-box allows various design approaches. In addition, different design choices can be made, focusing on the circuit depth or the number of qubits.

Kim et al. [KHJ18] present a framework to explore time-space tradeoffs for quantum cryptanalytic attacks like a key search in AES, explore different design choices in parallelizing a Grover-based attack or ensuring uniqueness of the target key. In [JNRV20], Jaques et al. show how AND-gates and measurement-based uncomputation can be leveraged to reduce the T-depth and overall depth in a key search for AES – at the cost of increasing the number of qubits and introducing measurements. Recent work on efficient AES implementations as a quantum circuit include [ZWS+20, CLCL22, JBS+22, WWL22, LGQW23, LPZW23, SF24]. The values in the subsequent table are taken from Jang et al. [JBS+22]. These values are consistent with the parameters explored more recently in [DC24]. The latter work explores the overhead needed when passing from logical to physical qubits.

Table 4.1: (Logical) quantum resources for implementing AES according to [JBS+22, Table 9(a)] (product of depth and number-of-qubits optimizing design).

	#CNOT gates	***#1qCliff. gates***	***#T-gates***	***#qubits***	***overall depth***
AES-128	138,148	19,096	86,660	3,428	731
AES-192	156,008	21,272	98,000	3,748	874
AES-256	191,772	26,607	122,024	4,036	1,025

Table 4.2: (Logical) quantum resources for a Grover-based key search for AES according to [JBS+22, Table 10(a)] (product of depth and number-of-qubits optimizing design).

	#qubits	***#(Clifford + T) gates***	***overall depth***
AES-128	3,429	$1.473 \cdot 2^{82}$	$1.121 \cdot 2^{74}$
AES-192	7,305	$1.539 \cdot 2^{115}$	$1.34 \cdot 2^{106}$
AES-256	7,817	$1.859 \cdot 2^{147}$	$1.572 \cdot 2^{138}$

The parameters shown here refer to logical qubits; they reduce the product of the number of qubits and the overall circuit depth. To determine the overall depth, [JBS+22] relies on a depth-eight decomposition of Toffoli gates into eight Clifford and seven T gates from [AMMR13]. Considering a physical error rate as low as 10^{-6}, [DC24] offers physical resource estimates for a number of design choices to implement a Grover-based key search. With a circuit depth of 2^{64}, already for AES-128, the estimated number of physical qubits is as high as $2^{48.1}$. For AES-192, this number already reaches $2^{112.6}$, and for AES-256, the number of physical qubits is estimated to be as high as $2^{177.1}$. Jang et al. [JBS+22] offer several additional parameter choices, and while different optimization options are available and further improvements by small constant factors are plausible, the exponential scaling of Grover's algorithm remains a formidable hurdle for the number of gates and the circuit depth. Although the quantum security analysis of AES in [BNPS19] still builds on the gate counts in [GLRS16], the positive view of the authors of [BNPS19] on the post-quantum security of AES-256 still appears valid.

Referencing [CNPS17], Bonnetain et al. indicate in [BNPS19] that the 128-bit size of the internal AES state may offer an avenue for quantum cryptanalytic progress. The internal state size of AES does not enlarge when increasing the key size. So, building on classical results, e.g., on the CTR mode, it is conceivable that for certain modes of operation, a quantum speed-up might reduce the security level significantly below 128 bit. However, no feasible quantum attack against AES has been identified so far. Another line of work for which not many publications are available so far is to try to integrate Grover's algorithm with classical attacks to lower their cost. Wang et al. [WCJ22] explore such an option for a classical distinguisher, but again no feasible attack against AES appears to be known at this point.

4.2.2 Quantum attacks on cryptographic hash functions

A preimage search for a cryptographic hash function is another natural application for Grover's algorithm. Let H be a cryptographic hash function with an n-bit output, and restrict H's input to bitstrings of length n. Intuitively, restricting a cryptographic hash function H in this way, we should obtain something "close" to a one-way permutation on $\{0,1\}^n$. Using the search criteria whether applying H to a given n-bit string yields the desired image, one can expect that Grover's algorithm yields a preimage for a given image in time $O(2^{n/2})$. The precise cost for such an attack depends on the cost for implementing H (for restricted input) as a quantum circuit. Amy et al. [AMG+16a] offered an initial analysis for a Grover-based preimage attack on two specific variants of the SHA family of hash functions. The Secure Hash Algorithm (SHA) is a family of hash functions standardized by the National Institute of Standards and Technology (NIST) [NIS15a, NIS15b]. A number of authors explored efficient quantum circuits for members of these families since then, including, e.g., Preston [Pre22] and Song et al. [SJS23] The following table is based on a state-of-the art design in the latest available revision of an analysis by Jang et al. [JLO+24]:

Table 4.3: (Logical) quantum resources for implementing different members of the SHA family according to [JLO+24, Tables 6 and 10].

	#CNOT gates	***#1qCliff. gates***	***#T-gates***	***#qubits***	***overall depth***
SHA-2-256	693,832	84,086	495,089	5,715	12,791
SHA-2-384	1,847,124	225,008	1,335,511	13,773	17,257
SHA-2-512	1,864,872	226,533	1,346,011	13,901	17,303
SHA-3[5]	752,000	124,937	425,600	22,400	578

[5] valid for the 256-, 384-, and 512-bit case

Instead of trying to mount an (infeasible) preimage attack – with $(\pi/4) \cdot (2^{128})$ or more Grover iterations for a modern hash function – one may look at quantum speed-ups of different types of attacks. Banegas and Bernstein [BB17] consider a multi-preimage search with a quantum algorithm. They combine Grover's technique with a reversible parallel rho-algorithm and make a case that *quantum preimage search benefits asymptotically from having multiple targets.* At this point, their analysis focuses on asymptotic aspects, and gate-level resource counts are not available. Dunkelman et al. [DKRS23] show that, with the help of quantum-accessible classical memory, inverting a random function on one of d values can be done with a more attractive trade-off than in the classical setting: Dunkelman et al. establish an attack satisfying $t^{4/3}M^2d^2=N^2$, with t representing online (in contrast to precomputation) time and N being the size of the domain of the function to be inverted, e.g., $N=2^{256}$ for SHA-2-256. If the size M of available (quantum-accessible classical) memory exceeds $(N/d)^{2/3}$, this offers an opportunity to improve on the quadratic speed-up of a simple Grover-based approach.

Going beyond preimage attacks, one can also seek to leverage Grover's algorithm to accelerate a collision search, hoping for a stronger quantum cryptanalytic impact. Before proceeding, recall that Grover's Algorithm has two similar but different forms, depending on whether the number of solutions is known or not which is directly related to the number of expected collisions here. If the specific number of collisions is known, the simpler form of Grover can be applied while an unknown number of solutions requires the use of the more generic form of the algorithm found in [BBHT98].
Hash functions like SHA-256 [NIS15a] and FORK-256 [HCS+06] take an input of (for practical purposes) arbitrary size and map it to an output size of 256 bits, but it might be beneficial to explain the quantum collision algorithm assuming the number of collisions is known and finite.

Assuming the hash function is *r*-to-one.

As explained in [BHT98], assume there exists some random hash function H such that $H: X \rightarrow Y$ is an r-to-one function, meaning exactly r inputs produce each output where $r \geq 2$. Thus, if $|X| = N = 2^r$ then $|Y| = N/r$. If space is available, the best solution requires the computation of a random subset K of X of cardinality $k = (N/r)^{1/3}$ and each tuple stored in a table. This table can be computed on a classical computer and would take k evaluations of H. This list would then need to be sorted and if any collisions are found such that $H(x_i) = H(x_j)$ then $\{x_i,x_j\}$ can be output and the search is over, however this probability is quite low.

While this list can be computed on a classical computer, the table would need to be stored in qubits so Grover can reference this list of values in the table each iteration. Thus, if $O((N/r)^{1/3})$ storage qubits are unavailable or too costly, the list would need to be reduced which would increase the running time of the algorithm. The algorithm would compare the computed hash value with all the values in the second column of the table and return a '1' if the output value is found in the second column of the table and the input value is not found in the first column. The algorithm would return a '0' otherwise. After a specific number of iterations, a collision would be found with probability 1/2 and the result would be a plaintext $x \in X \backslash K$ such that $H(x)$ is a value in the stored table. To complete the process, $H(x)$ would need to be computed and found in the table. If $H(x) = H(x_0)$ for some $(x_0,H(x_0))$ tuple in the table, then $\{x,x_0\}$ is a collision which can be output.

Since k distinct input values are stored for comparison and each output value has r distinct input values that hash to it, the probability of a collision is $r \cdot k/N$. Thus, the expected number of Grover iterations would be about $(N/(rk))^{1/2} = (N/(rN^{1/3}))^{1/2} = (N/r)^{1/3}$. Since the number of classical computations of H is $k+1 = (N/r)^{1/3} + 1$ we get the expected run time of the algorithm to be $O((N/r)^{1/3})$ times the time it takes to compute the hash function. However, this expected run time comes at the cost of $O((N/r)^{1/3})$ quantum memory.

Generic hash functions

When less is known about the hash function or even when we just know it is not specifically r-to-one for any $r \geq 2$ the argument above must be slightly modified. Changes must be made to how $K \subseteq X$ is chosen, but the more general version of Grover can be used. Obviously, the smaller the chosen $K \subseteq X$ the longer it will take to find a collision and while a larger K will reduce the number of Grover iterations, the storage and classical computations of the hash will increase.

However, if the input size is known to be a specific finite number or at most some finite number, then $|K|$ can be determined based on the probability of each output being repeated [FHZ14], but it is still $O(N^{1/3})$ where N is the size of the hash space. When searching for a collision in SHA-256 or FORK-256 or other hash functions, this is all that is necessary since the searched input size can simply be fixed to be anything bigger than 256 bit to guarantee a collision.

Searching for a claw

Another result in [BHT98] is that of finding a claw. A claw is similar to a collision in a hash function but is a collision among two hash functions [OK91]. Specifically, if F and G are two distinct hash functions such that $F : X \to Z$ and $G : Y \to Z$ with $|X| = |Y| = |Z| = N$, then one can find a pair $x \in X$ and $y \in Y$ such that $F(x) = G(y)$ in an expected number of $O(N^{1/3})$ by applying the same algorithm as above expect picking the K subset from before from X and applying the Grover search to Y.

Even though these functions more closely resemble permutations, this algorithm can again be extended to more general r-to-one hash functions in the same way as before. And while it is not expressly stated in [BHT98], it would seem to still hold for hash functions that are not specifically r-to-one either. For Grover to run most efficiently when looking for a claw, any collisions completely in K should be removed and replaced before continuing. This is because the Grover search is most efficient when the exact number of solutions is known and a collision inside K reduces the probability of finding a collision outside of K. However, since we already assume this probability to be extremely low and are already sorting K, this is a minor additional step.

Therefore, for any generic hash function where $N = 2^m$ is the size of the hash space, picking a random $K \subseteq X$ such that $|K| = O(N^{1/3})$ yields an expected collision with probability greater than 1/2 after a run time of $O(N^{1/3})$. The exact run time depends on the size of K, the number of Grover iterations, the cost of computing the hash function and searching for a collision in K. Also, the assumption is that there are $O(N^{1/3})$ quantum bits of storage to run Grover's Algorithm which is non-trivial. Less than this would increase the overall search time which would max out at $O(N^{1/2})$ (the standard Grover run time).

4.2.3 Questions on quantum collision search and the case of SHA

Work by Bernstein [Ber09] questions the cost-effectiveness of the quantum collision search by Brassard, Høyer, and Tapp. Specific obstacles pointed out are the required cost for accessing the (large) quantum memory needed, and the cost needed to implement the Grover oracle, which goes well beyond a single application of the hash function. Following the reasoning in [Ber09], mounting a purely classical collision search is more cost-effective than implementing a quantum algorithm as described above. The significance of quantum collision attacks remains controversial. In [CNPS17], Chailloux et al. present a quantum collision search algorithm where, with S (up to $N^{1/4}$) processors, the amount of quantum memory scales linear in $S \cdot \log N$ and – ignoring logarithmic factors – the runtime is reported to scale with $N^{2/5} \cdot S^{-3/5}$. The choice $S = N^{1/5}$ is suggested to outperform the best classical algorithm in the time×(classical+quantum space) metric, but Bernstein [Ber17] questions the accuracy of Chailloux et al.'s analysis and suggests that a classical (parallel rho) collision search outperforms the proposed quantum algorithm. At this point, it remains questionable if quantum algorithms can offer a practical benefit for finding collisions in established hash functions. An up-to-date quantum resource estimate, for a quantum collision search, leveraging Chailloux et al.'s approach is given in the following table. This design allows in the order of $2^{n/6}$ parallel instances for output length n of the hash function, as well as measurement-based uncomputation. As can be seen, the attack complexities are considerable/impractical.

Table 4.4: (Logical) quantum resources for implementing a collision attack against different members of the SHA family according to [JLO+24, Table 13]., Table 13].

	#gates	***#qubits***	***overall depth***
SHA-2-256	$1.49 \cdot 2^{97}$	$1.13 \cdot 2^{55}$	$1.58 \cdot 2^{90}$
SHA-2-384	$1.32 \cdot 2^{137}$	$1.72 \cdot 2^{77}$	$1.45 \cdot 2^{129}$
SHA-2-512	$1.76 \cdot 2^{175}$	$1.09 \cdot 2^{99}$	$1.91 \cdot 2^{167}$
SHA-3-256	$1.31 \cdot 2^{97}$	$1.16 \cdot 2^{57}$	$1.39 \cdot 2^{86}$
SHA-3-384	$1.73 \cdot 2^{135}$	$1.46 \cdot 2^{78}$	$1.84 \cdot 2^{124}$
SHA-3-512	$1.14 \cdot 2^{174}$	$1.84 \cdot 2^{99}$	$1.21 \cdot 2^{163}$

Augmenting classical attacks

In [KLLNP16], the study of differential and linear cryptanalysis in connection with quantum attacks is initiated. On the one hand, a scenario with quantum queries to the attacked block cipher is considered, which for today's implementations on classical platforms may be considered an unrealistic model. On the other hand, the paper also makes the point that even when restricting to classical queries, a quantum algorithm in combination with differential and linear cryptanalysis can sometimes yield a more efficient attack than a key search with Grover. Such hybrid classical-quantum attacks against symmetric primitives turned out to be a fruitful research area. Hosoyamada and Sasaki argue in [HS20] that a differential trail that may not be exploitable classically, may still be exploitable for quantum cryptanalysis. For 7-round AES-MMO and 6-round Whirlpool, they show that a quantum computer can enhance the reach of the best-known classical attack. Dong et al. [DSS+20], expand on this line of work, reducing the quantum resource requirements of [HS20], and obtain improved attacks on AES-MMO and AES-MP. Further research in this area by Dong et al. [DZS+21], led to an improved attack on the compression function of Whirlpool, and it seems plausible that further improvements of dedicated quantum attacks on specific hash functions can be identified. Baek et al. [BCK22] show how to construct quantum free-start collision attacks on Hirose and NJH designs, instantiated with AES-256. Hosoyamada and Sasaki [HS21] showed that specifically for SHA-256 and SHA-512 the reach of classical attacks can be increased by seven and twelve steps, respectively. Overall, research on hash-function specific quantum cryptanalytic attacks continues to remain an active research area that deserves to be followed.

4.2.4 Leveraging other quantum algorithms

Grover's algorithm is by no means the only quantum cryptanalytic tool available to attack symmetric primitives—see, for instance, [RS15, KLNP16, KLLNP16, SS17, BNP18]. Notwithstanding this, it is fair to say that for attacking today's implementations, which are entirely classical, Grover's approach is currently the most relevant tool. Conceptually, *Simon's algorithm* enables an interesting and different type of attack, but from a practical point of view, it is important to pay close attention to how an application/oracle interface is accessed. What is Simon's algorithm? It is a quantum algorithm which can solve the following problem in expected polynomial time, provided that the involved function $f\colon \{0,1\}^k \to \{0,1\}^{k'}$ can be evaluated in polynomial time *on a superposition of inputs*. For the function f it is assumed that $k' \geq k$ and one of the following conditions holds:

1. f is injective, or
2. there is a bitstring s, not entirely zero, such that for every $x \neq x'$ we have $f(x) = f(x')$ if and only if $x = x' \oplus s$.

The task is to decide for a given f which of the two cases holds, and in the second case to determine the "hidden shift" s. In the evaluation scheme of Section 3.2, Simon's algorithm qualifies as (A) provably correct,

and from a cryptanalytic point of view, involving Simon's efficient solution to this problem is attractive, when the adversary can actually implement and evaluate f at a superposition. Bonnetain [Bon21Bon21] gives a thorough cost analysis of Simon's algorithm from a cryptanalytic angle. A common problematic assumption in attacks based on Simon's algorithm is that the function *f* depends on the attacked secret key, so that *quantum access to an implementation of the attacked cipher which stores the attacked secret key* becomes necessary. It is fair to say that for today's classical implementations this assumption is not met. So, while Simon's algorithm is in principle (B) compatible with quantum hardware as developed today, the cryptanalytic context – attacking a purely classical implementation of a symmetric cryptographic primitive like AES-128 – may impose an unrealistic hardware assumption, as a required superposition access is unavailable, leaving a more detailed (C) quantum resource analysis to be of very limited use.

Related-key attack

To illustrate this point, let us take a brief look at a quantum version of a related-key attack in [RS15], which relies on Simon's algorithm and in principle enables the recovery of the secret key of a large class of block ciphers in polynomial time (measured in the key length). So, if quantum access to the keyed primitive is/were indeed possible, the attack is highly potent against symmetric encryption schemes. The setting considered in [RS15] is a related-key attack, where the function *f* depends on the attacked block cipher (which can reasonably be assumed to be known), but also on the attacked secret key. Access to the latter is in a related-key attack in principle available—commonly modelled through a suitable encryption oracle. However, to bring Simon's algorithm to use, the oracle must accept a superposition of inputs, which for classical implementations is not the case. This is very different from (and less threatening than) Grover's algorithm, where the attacker needs only the specification of the block cipher (plus plaintext-ciphertext pairs) to mount an attack against the secret key. However, if quantum access were available, the resulting attack would be polynomial time—unlike a key search with Grover. Cid et al. [CHLS20] consider quantum attacks against Feistel structures and expand on [RS15]. The related-key attacks considered in [CHLS20] limit the adversary in that its control of the quantum superpositions that can be queried is restricted.

Modes of operation

Similar as in the case of the related-key attack just mentioned, in [KLNP16] Kaplan et al. show how Simon's algorithm can be leveraged to invalidate the security of popular modes of operation for achieving authenticated encryption or for constructing a MAC from a block cipher. The same paper uses Simon's algorithm—with the same limitation—to expedite a slide attack. More recently, Sun et al. [SCQWG23], expanded this line of work, proposing quantum attacks on a number of MAC designs where the classical security aims at guarantees beyond the birthday bound. Conceptually, these attacks are interesting, but from a pragmatic point of view they are not an imminent threat for today's implementations, as the assumptions of the attack model are not met.

Relating to Simon's algorithm, Bonnetain et al.'s work in [BHNP+19] deserves mentioning, as it shows that in specific cases, Simon's algorithm can be leveraged for a key recovery with fewer or no superposition queries to the attacked cipher than was reported before. In [BSS22], Bonnetain et al. demonstrate that in fact for a specific symmetric design, Simon's algorithm can enable a speed-up that goes beyond Grover's without requiring superposition access. While the attack scenario may still be restrictive, conceptually this improvement beyond a square root savings is interesting. Schrottenloher's work on quantum-linear key-recovery attacks using the quantum Fourier transform [Sch23https://sch23/] fits into this line of work, too. He shows how to adapt a classical technique to expedite linear key-recover attacks by leveraging superposition queries or quantum-accessible classical memory.

4.3 Algorithmic innovations with relevance for asymmetric cryptography

For cryptographic algorithms that rely on the computational hardness of factoring "large" integers or of computing discrete logarithms in a suitably chosen cyclic group, the impact of quantum algorithms appears at this point more fundamental than for symmetric cryptography. Leaving aside a possible performance

penalty, doubling the key length and ensuring a sufficiently large state size seems a viable approach to address the most impactful quantum attacks – Bhaumik et al. [BCFNP22] discuss a generic construction for such a "doubling up." Similarly, the available quantum speed-up in finding a collision for a hash function is only polynomial. For factoring and computing discrete logarithms, Shor's seminal work in [Sho94, Sho97] reveals a very different picture: He presented polynomial time solutions for factoring and for computing discrete logarithms, which is very different from the best known classical algorithms, which exhibit, at best, a subexponential run time. In the evaluation scheme from Section 3.2, Shor's algorithm qualifies as (A) provably correct, (B) compatible with currently developed hardware, and (C) the literature offers solid quantitative insights into the quantum resources needed. Before quantifying quantum resources for factoring and computing discrete logarithms for common cryptographic problem instances, it may be helpful to start out with an asymptotic perspective as presented, e.g., in [BBM17] and [RNSL17c].

Factoring integers

The predominant classical approach to factoring in cryptanalytic contexts is the Number Field Sieve (NFS). For factoring a composite n-bit number, the running time of this algorithm is estimated to be subexponential of the form $(\exp(n^{1/3} \cdot \log^{2/3} n))^{c+o(1)}$ with a constant c of about 1.902. Bernstein et al. in [BBM17] present a quantum algorithm with a better – but still subexponential – running time: They reduce the exponent c to about 1.387, and at the same time they ensure that the number of qubits needed by their method grows with $n^{2/3+o(1)}$ only, i.e., the growth is sublinear. This is conceptually different from Shor's algorithm, where the number of qubits needed is linear in n. However, the expected running time of Shor's algorithm is only cubic in n, i.e., polynomial in the bit length. There has been significant progress in optimizing the complexity of Shor's algorithm and improving on the original proposal. With Regev's factoring algorithm [Reg24], even an alternate technique for factoring integers has appeared. Still, so far achieving simultaneously a polynomial running time and using only a sublinear number of qubits remains a challenge.

Discrete logarithms

For discrete logarithms in the multiplicative group of a finite field, prime fields are arguably the cryptographically most interesting case. Again, an NFS-based technique is available in this scenario. Also in this case, [BBM17] offers a way to speed-up at least one of two phases of the classical algorithm—in the running time of $(\exp(n^{1/3} \cdot \log^{2/3} n))^{c+o(1)}$ (now n represents the bit size of the field), the constant c can again be reduced from about 1.902 to about 1.387, involving only a sublinear number of qubits. From what we know so far, for elliptic curves over prime fields, the techniques in [BBM17] do not apply, and for adequately chosen curves, the expected running time of the best available classical algorithm (a parallel version of Pollard's rho method) is exponential in the bit length n of the group size: $((p/2)^{1/2} + o(1)) \cdot N^{1/2}$, where N is the group size. Shor's algorithm offers here an exponential speed-up: it has an expected running time that is no more than cubic in the bit length of the group size, i.e., it is a polynomial time solution. For implementing this method, an—in the bit length of the group size—linear number of qubits is used, however.

Shor's algorithm is applicable to any finite cyclic group in common cryptographic use today. In contrast, a more recent approach by Ekerå and Gärtner [EG24], which builds on Regev's factoring algorithm [Reg24], is more restricted in its effectiveness. Somewhat reminiscent of traditional index calculus, group elements are not treated as structureless, and the approach of Ekerå and Gärtner is mostly of interest for discrete logarithm problems in the multiplicative group of a prime field where a natural notion of "small" elements is available. For Schnorr groups, the size of the ambient field impacts the cost, and for elliptic curves, the approach does not seem promising at this time. Similar to factoring, being able to restrict the number of qubits to a sublinear range while preserving polynomial running time remains a challenge for discrete logarithm computations.to factoring, being able to restrict the number of qubits to a sublinear range while preserving polynomial running time remains a challenge for discrete logarithm computations.

4.3.1 Factoring integers

Shor's solution can be expected to find a factor of a composite n-bit number in time $O(n^3)$—following Proos and Zalka [PZ03], we can estimate the constant to be about 4. Essentially, there are two phases to the algorithm, the second of which is entirely classical. This portion is not hard to implement, but it is worthwhile to put some thought into the implementation of this portion, so that unnecessary repetitions of the first phase, which relies on a quantum computer, can be avoided [Law15, Joh17, Eke21, Eke22]. In fact, Ekerå [Eke21, Eke22] shows that usually a single execution of the quantum part of Shor's algorithm suffices to recover the complete factorization of the target number through efficient classical post-processing. The first (quantum) phase of Shor's algorithm is also referred to as *order finding*: we must find the order of a randomly chosen $\alpha \in \mathbb{Z}/N\mathbb{Z}^*$, where N is the number to be factored. No efficient classical algorithm is known for this problem, but from Shor's work we know that the *Quantum Fourier Transformation* (QFT) can be invoked to solve this problem efficiently on a quantum computer. Unlike a classical Fast Fourier Transform (FFT), a QFT can be implemented in polylogarithmic time (namely $O(\log^2 N)$). Cleve and Watrous [CW00] offer a theorem which neatly separates a classical and a quantum portion of factoring an integer—they argue that a polynomial size classical pre-processing and a polynomial-size classical post-processing can be combined with an $O(\log n)$-depth quantum circuit of polynomial size.

The most expensive operation, and the bottleneck in running Shor's algorithm, is the computation of a modular exponentiation on a quantum computer: we must be able to compute $\alpha^k \bmod N$, where k is in superposition. There is ample classical work available on implementing this type of arithmetic, but we do need this arithmetic as a quantum circuit. There is a strong connection with Shor's algorithm for the discrete logarithm problem in a prime field, as in the latter case we also face an exponentiation task with a known modulus. So the question of implementing modular arithmetic efficiently as a quantum circuit is of key importance to actually use Shor's algorithm.

The number of qubits needed to factor with Shor's algorithm is quite modest—Beauregard [Bea03] showed that for an n-bit number a circuit with $2n + 3$ qubits and $O(n^3 \log(n))$ elementary quantum gates (and cubic depth) is available. Zalka [Zal08] argues that $1.5n$ logical qubits suffice. Work by Ekerå and Håstad [EH17] indicates that factoring might be feasible with more shallow circuits, offering roughly a reduction by a factor of 4. Having the number of qubits proportional to the bitlength n of the number to be factored appears essential with the current state-of-the-art, unless one is willing to sacrifice the polynomial running time (see the discussion of Bernstein et al.'s approach from [BBM17] below.) One of the most recent detailed cost analyses of factoring an RSA modulus is due to Gidney and Ekerå [GE21], and also here the number of logical qubits is essentially chosen to be linear (actually, slightly worse): $3n + 0.002n \cdot \log_2 n$ – using a slightly worse than cubic ($0.3n^3 + 0.0005n^3 \cdot \log_2 n$) number of Toffoli gates.

Kahanamoku-Meyer and Yao [KMY24] put forward a multiplication technique that combines ideas of Toom-Cook multiplication with Draper's quantum addition [Dra00] and makes heavy use of controlled phase rotations. The gate-level analysis for modular arithmetic as needed for Shor's algorithm is still in an early stage, and a detailed quantitative analysis for a full Shor implementation, e.g., for a 2048-bit factorization is still lacking. Kahanamoku-Meyer and Yao note in their discussion of 2048-bit multiplication that "the gate counts are very promising, although impossible to compare directly to alternate strategies without compiling to a common native gate set." Non-trivial savings in the gate cost seem plausible, and follow-up work on the preprint by Kahanamoku-Meyer and Yao can be expected. Asymptotically, it is already clear that with the number of logical qubits being in the order of $2n+O(\log n)$, an implementation with a sub-cubic (actually close to quadratic) logical gate count is now feasible.

Resource counts and adjusting Shor's algorithm

It has been fairly common for a while, that research papers did not elaborate on how to pass from a (correct) high-level algorithm to an actual quantum circuit. An interesting and elaborate design to factor an RSA modulus with Shor's algorithm is due to Pham and Svore [PS13]. They employ a 2D *nearest-neighbor* quantum architecture with the following resource counts: depth $O(\log^3 n)$, size $O(n^4 \log n)$, and $O(n^4)$ qubits. Pham and Svore offer explicit bounds, and the constants hidden are non-trivial. E. g., for the number of qubits in a modular exponentiation the multiplicative constant in front of the n^4 is about 95,000 and the number of gates hides a term in the magnitude of $3.5 \cdot 10^6 \cdot n^4$. Still, this result offers an exponential

improvement in circuit depth over prior *nearest-neighbor* solutions at the cost of a polynomial increase of gate count and number of qubits.

If we give up the nearest-neighbor restriction and would like to keep the number of qubits small, a design proposed by Häner et al. in 2016 can at the moment be seen as leading contender for a cryptographically relevant implementation of Shor's algorithm [HRS17]. This proposal has been analyzed at a quite detailed level, and the available algorithm analysis is backed by serious software simulation (with cryptographically relevant input sizes). In addition, the authors make a case that their Toffoli-network based arithmetic facilitates debugging when being implemented on a quantum hardware, which from an experimental point of view is indeed a valuable feature. With $2n + 2$ qubits, the width of Häner et al.'s solution is quite moderate, the depth is $O(n^3)$, and the number of gates calculates to $64n^3 \log_2(n) + O(n^3) = O(n^3 \log n)$. Going beyond an asymptotic characterization, [HRS17, RNSL17c] suggests that for factoring an n-bit RSA modulus, $2n + 2$ qubits and $n^3 \cdot (64 \cdot (\log_2(n)-2)+29.46)$ Toffoli gates suffice. From [HRS17, RNSL17c], taking into account [EH17], we obtain the resource estimates shown in Table 4.5, where n denotes the bit length of the number to be factored.RNSL17c] suggests that for factoring an n-bit RSA modulus, $2n + 2$ qubits and $n^3 \cdot (64 \cdot (\log_2(n)-2)+29.46)$ Toffoli gates suffice. From [HRS17, RNSL17c], taking into account [EH17], we obtain the resource estimates shown in Table 4.5, where n denotes the bit length of the number to be factored.

Table 4.5: Toffoli gate counts for factoring an n-bit number according to [HRS17], [RNSL17c, Table 2], taking into account work by Ekerå and Håstad [EH17] that reduces the Toffoli gate count by a small factor (4).

n	***Number of qubits***	***Number of Toffoli gates***
1024	2050	$1.45 \cdot 10^{11}$
2048	4098	$1.30 \cdot 10^{12}$
3072	6146	$4.65 \cdot 10^{12}$
7680	15362	$8.25 \cdot 10^{13}$
1530	30722	$7.18 \cdot 10^{14}$

If one is willing to leverage a larger number of logical qubits, Gidney and Ekerå's [GE21] design offers an attractive alternative. The paper uses a number of techniques to reduce the cost for arithmetic. In addition to reducing the circuit depth by factoring through reduction to a short discrete logarithm computation (see below), the arithmetic is optimized in several ways. For instance, instead of a traditional representation of a modular integer as a computational basis state, a so-called coset representation (cf. [Zal08]) is invoked and the exponentiation makes use of windowing. From the perspective of the evaluation scheme in Section 3.2, the (A) provable correctness and (B) compatibility with currently developed quantum hardware of the approach by Gidney and Ekerå is on par with Shor's algorithm, but the (C) detailed quantum resource analysis changes. While the number of logical qubits is larger than in Häner et al.'s approach, Gidney and Ekerå's approach offers savings in the number of non-Clifford gates (see [GE21, Table 1]). More specifically, going with Gidney and Ekerå's design, the number of logical qubits scales with $3n + 0.002n \times \log n$ instead of $2n + 2$, but the Toffoli count is lower – the dominating term is $0.0005n^3 \log n$ (see [GE21, Table 1). Including the overhead for fault tolerance, i.e., passing from logical to physical qubits, for a suitable superconducting qubit platform with nearest-neighbor connectivity in a planar grid, [GE21] establish a fairly thorough quantum resource analysis for the case of trying to factor a 2048-bit RSA modulus. They conclude that 20 million noisy qubits could enable such a factorization within 0.31 days. With a (more traditional) Toffoli-based arithmetic, we obtain an estimate of about one million qubits as being needed to factor 2048-bit RSA in 100 days, taking fault-tolerance into account.

Building on the same algorithmic idea as [GE21], Gouzien and Sangouard [GS21] suggest an implementation using only 13436 physical qubits, but invoking a quantum memory capable of storing 28 million spatial modes and 45 temporal modes. The experimental realization of such a configuration at the required scale is an open problem, but if the proposed type of quantum memory can be implemented, Gouzien and Sangouard's work suggests that a 2048-bit RSA modulus could be factored in less than half a year.

Several authors proposed modifications of Shor's algorithm with to reduce the requirements on the underlying quantum hardware. At the cost of a (more expensive) classical post-processing phase, the use of simpler quantum hardware becomes possible. The simpler quantum device may then have to be used

multiple times to collect sufficient data for a successful factorization – Regev's factoring algorithm [Reg24], discussed below, can be seen as a major contribution along this research trajectory. Ekerå and Håstad [EH17]'s earlier work fits in with this line of thinking as well. Building on Ekerå [Eke16]; they reduce the task of factoring an RSA modulus $N = pq$ to computing a short logarithm inside the multiplicative group modulo N. This reduction is entirely classical – a discrete logarithm problem is derived, where the discrete logarithm is known to be $p+q$ (with high probability) – which for practical choices of p and q is small compared to the order of the multiplicative group modulo N. The fact that the exponent is small can then be leveraged in the quantum portion of the algorithm to work with smaller exponents. The resulting setting is pretty much the same as for Shor's original approach, but one can reduce the number of T gates by approximately a factor 4 (cf. [RNSL17c, Remark 3]). When using a semi-classical implementation of the QFT, which is standard, there is not really a saving in the number of qubits, however.

Historically, Seifert's earlier work [Sei00] is similar in nature to Ekerå and Håstad's approach in that a more elaborate classical prost-processing is used, with the goal of having a simpler quantum hardware that is used multiple times to collect sufficient information to ensure a successful factorization. However, the key obstacle in implementing Shor's algorithm – implementing the modular arithmetic – remains. Overall, the techniques introduced by Seifert, Ekerå, and Håstad reduce the number of gates (and circuit depth) by roughly a factor 4, but do not have a relevant impact on the number of qubits needed. Still, Gidney and Ekerå's work [GS21] illustrates that for other resource counts, like the measurement depth (which is relevant when leveraging measurement-based uncomputation), these observations can be valuable.

Chevignard et al.'s recent preprint [CFS24] fits into the idea of simplifying the quantum hardware and using it multiple times as well: They show that (with a gate count no more than cubic) the number of logical qubits can be reduced to $(\log N)/2 + o(\log N)$. For a 2048-bit RSA modulus they estimate that a device with 1730 logical qubits is sufficient, and on average 40 runs would be needed.

Regev's factoring algorithm

This algorithm relies on a non-trivial classical post-processing, using lattice techniques, and it also relies on a quantum portion that is executed multiple times. For our discussion, we use Ekerå and Gärtner's [EG24b] work, which accounts for important improvements to the original version of Regev's proposal [Reg24].]. Specifically, work by Ragavan and Vaikuntanathan on more space-efficient arithmetic using Fibonacci numbers in the exponent [RV24] (building on work by Kaliski [Kal17b]) and the recent constant factor improvements by Ragavan [Rag24] are important from a cryptanalytic point of view. The analysis and optimization of Regev's alternative to Shor's factorization algorithm is an active area of research, with relevant results being available in a preprint format only. In particular, Ekerå and Gärtner's [EG24] extension of Regev's approach to factoring an integer completely with order finding deserves to be mentioned.

Before discussing the efficiency of this alternative to Shor's technique, we note that both Regev's original algorithm and Ekerå and Gärtner's extension are heuristic in the sense that each relies on a number-theoretic assumption. This is not a real concern, however: a result from April 2024 by Pilatte [Pil24] shows that the correctness can be proven unconditionally, possibly invoking a parameter choice one would not make from a purely pragmatic cryptanalytic perspective. Subject to this subtlety, in the evaluation scheme from Section 3.2, Regev's algorithm qualifies as (A) provably correct, (B) compatible with currently developed hardware, and the (C) the literature offers so far limited quantitative insights into the quantum resources needed; the focus so far was more on the asymptotic analysis.

In a nutshell, *Regev's* algorithm lifts an essential idea in Shor's algorithm to a higher dimension: If N is the number to be factored, Shor's algorithm finds the order r of a unit in the integers modulo N. Then, assuming r is even, taking this unit to the power $r/2$ we find a non-trivial square root of 1 modulo N, which enables us to factor N. Instead of working with a single unit modulo N, Regev's approach chooses several, in comparison to N, *small* base values $b_1,\ldots, b_d$ and constructs a (short) exponent vector $(e_1,\ldots,e_d)$ with integer entries such that $b_1^{e_1} \cdot \ldots \cdot b_d^{e_d}$ is a non-trivial square root of 1 modulo N. Here, d can be thought to be in the magnitude of $(\log N)^{1/2}$, and the size of b_i is in the order of $O(\log N)$.

Choosing the base values b_i small enables savings in the calculations that need to be implemented. Somewhat analogous to Shor's algorithm, the circuit complexity in Regev's algorithm crucially depends on

implementing a multi- exponentiation of the form $b_1^{x_1} \cdot \ldots \cdot b_d^{x_d}$ where the size of the exponents is bounded by $N^{O(1/d)}$. The quantum portion of Regev's algorithm is executed around d times, each run yielding a vector. Ultimately, a classical post-processing involving lattice reduction distills the desired exponent vector $(e_1,\ldots,e_d)$ from the set of these vectors. This leads immediately to questions about the robustness of Regev's approach to errors, as some of the individual runs could yield an incorrect result, e.g., due to a failure in the error correction, which potentially could impact the computation of the final output vector. It turns out that this is less of a problem than one might expect and that Regev's post-processing is quite robust against errors [EG24c, EG24, RV24].

With much of the work on Regev's algorithm being still very recent, further optimizations can still be expected and it is still soon for a comparison with Shor's algorithm and its improvements. Ragavan's work [Rag24], which also incorporates a (privately communicated) optimization attributed to Remaud, suggests that a single run of an optimized version of Regev's algorithm can be implemented with $10.43 \cdot \log N$ qubits and $45.7 \cdot (\log N)^{1/2}$ multiplications – with other trade-offs being possible. Regev's algorithm is compatible with the already mentioned multiplier design by Kahanamoku-Meyer and Yao [KY24], suggesting that an implementation with a linear (in $\log N$) number of qubits and $O((\log N)^{½+\varepsilon})$ gates is possible. Where does this leave us in terms of competitiveness with Shor's algorithm and its optimizations when trying to factor a cryptographically relevant number like a 2048-bit or 4096-bit RSA modulus? The most advanced available analysis is due to Ekerå and Gärtner [EG24b] and takes into account the extension of Regev's algorithm in [EG24]. Their analysis is based on a metric that favors Regev's approach, e.g., space usage and the overhead of quantum error correction are not accounted for – the latter is relevant for the success probability of individual runs. Ekerå and Gärtner conclude that even with applied optimizations neither Regev's algorithm nor its extension by Ekerå and Gärtner are preferable over state-of-the-art variations of Shor's factoring approach.

Having said this, it is important to note how little time has passed since Regev's algorithm was proposed, so this line of research deserves to be watched closely.

Additional quantum-algorithmic approaches to factoring

If we give up the nearest-neighbor restriction and accept some uncertainty about the asymptotic cross-over, a proposal by Bernstein et al. [BBM17] becomes interesting. This algorithm comes with a heuristic complexity analysis, emphasizes the saving of qubits and restricts to using $(\log N)^{2/3+o(1)}$ logical qubits to factor an RSA modulus N. The running time is about $\exp((\log N)^{1/3}(\log\log N)^{2/3})^{1.387+o(1)}$. Key contribution of this algorithm is that the number of qubits grows *sublinear* in the size of the number to be factored—this is different from Shor's algorithm. Bernstein et al.'s approach starts out with a fast classical factoring algorithm (the Number Field Sieve) and then leverages Grover's algorithm to speed-up the sieving step. Remarkably, the predicate used in Grover's algorithm relies on an implementation of Shor's algorithm—basically, Shor's algorithm is deployed as smoothness test. The exact cost of this elaborate algorithm for a fixed key size (like a 2048-bit modulus) is still unclear, even though asymptotically this new approach plausibly saves qubits over Shor's algorithm. In terms of the evaluation scheme in Section 3.2, (A) the correctness of [BBM17] is – within the limitation of a plausible heuristic analysis as is common for classical factoring algorithms – proven. Fundamentally, the approach is (B) compatible with currently developed hardware, but with the currently available asymptotic analysis, a (C) detailed quantum resource analysis remains an open issue.

In a similar line of work, Mosca et al. [MBV20], try to expedite the classical Number Field Sieve, using a quantum subroutine. Their approach uses a (quantum) SAT solver for smoothness testing based on a circuit that is derived from the classical Elliptic Curve Method. Under the assumption that a quantum computer can achieve a sufficient speed-up over classical SAT solvers, an asymptotic speed-up for the Number Field Sieve is obtained – in the case of a quadratic quantum speed-up, the asymptotic running-time of [BBM17] could be obtained. A key idea here is that implementing an efficient quantum SAT solver could potentially be feasible using annealing, potentially circumventing the need for a fault-tolerant implementation. However, it is unclear if such an efficient quantum SAT solver can be built. For cryptographic parameters of interest, classical special-purpose hardware that implements the Elliptic Curve Method (see, for instance, [GJKPS06]), may potentially be an interesting alternate route to (non-asymptotically) speed-up the Number Field Sieve. Thinking in terms of the evaluation scheme in Section

3.2, (A) the correctness of the approach in [MBV20] is non-controversial, but it is unclear that a speed-up over a classical solution can be achieved, as we (B) currently lack a plausible candidate hardware for the needed SAT solver implementation.

The idea of side-stepping the Number Field Sieve altogether and to capture integer factorization directly as a SAT problem can been considered, too, but this approach does not seem promising. Specifically, the authors of [MV22] note that they "are not aware of any evidence that any SAT-based quantum factoring results to date [...] are relevant milestones toward large-scale integer factorization or the demonstration of a speed-up over the best known classical algorithms for integer factorization."

In December 2022, Yan et al. proposed another hybrid approach [YTWJ+22], combining a factoring algorithm suggested by Schnorr with a quantum approximate optimization algorithm (QAOA). The paper suggests that this approach may be able to threaten a 1024-bit RSA modulus with only 205 *physical* qubits and a 2048-bit RSA modulus with only 372 *physical* qubits. More general, for factoring an n-bit number the number of physical qubits is estimated to be sublinear as $O(n/\log n)$. The paper discusses experimental results, including the factorization of a 48-bit number. However, significant doubts about the feasibility of this approach remain [GGRV+23]. From the perspective of the evaluation scheme in Section 3.2, (A) the scalability of the underlying classical factoring algorithm to cryptographically relevant numbers is not broadly accepted in the research community, and the potential for a speed-up with the proposed quantum subroutine is unclear. Yan et al. acknowledge uncertainty about their approach, stating *that the quantum speedup of the algorithm is unclear due to the ambiguous convergence of QAOA*. At this point, there is no clear evidence that Yan et al.'s approach yields a feasible attack against today's RSA parameters.

4.3.2 Computing discrete logarithms

Shor's solution to the discrete logarithm problem is remarkably generic and affects any finite cyclic group of cryptographic interest. Again, the algorithm includes a classical phase, which is easy to implement, and a phase which requires a quantum computer. The pertinent quantum circuit begins with a simple application of Hadamard gates, finishes with a QFT, and in between relies on the availability of efficient group arithmetic: to find the discrete logarithm of $h \in \langle g \rangle$ we need to be able to compute (in multiplicative notation) $g^k \cdot h^{k'}$ where the exponents k and k' are in superposition. The exact cost of this operation will depend on the complexity of the underlying group arithmetic. Just as in the case of factoring, this (double) exponentiation is the bottleneck of Shor's algorithm—for the QFT portion we can rely on the results of Cleve and Watrous again. As noted by Mosca and Zalka [MZ04], for the discrete logarithm setting, we could in principle even use an exact Quantum Fourier Transform instead of an approximate version (whose dimension is a power of two), but there appears no obvious practical gain in this approach.

If the target subgroup is embedded in a finite prime field, we face the task of implementing simple modular arithmetic, resulting in a situation very similar to the one for factoring. The fact that our modulus is now a prime number is, as far as the implementation complexity goes, without significance. We can (re-)use the modular exponentiation circuits from Shor's algorithm for factoring to implement the needed group arithmetic. Perhaps unsurprisingly, detailing circuits for this scenario has not been a topic of significant interest in the research literature so far. More recently, [GE21] gives some explicit cost estimates, taking into account, e.g., if a discrete logarithm is known to be small. Overall, the cost estimates provided by [GE21, Table 4] confirm the similarity in complexity for factoring and discrete logarithms in a prime field. Chevignard et al.'s approach [CFS24] can be applied to short discrete logarithms in a prime field. Moreover, Regev's algorithm for factoring [Reg24] can be adapted to discrete logarithms [EG24], but the cryptanalytic relevance of this adaptation appears limited at this point: just as in the case of factoring, a suitable notion of "small" elements is needed, and for elliptic curves such a notion is not known to be available. For Schnorr groups, the naturally available notion of "small" relies on the ambient prime field, i.e., it is not clear how to exploit the smaller size of the group of interest. The most interesting setting for the adaptation of Regev's approach to the discrete logarithm is over a finite prime field. As this is a fairly new line of research, further optimizations can be expected, but the available analysis by Ekerå and Gärtner [EG24b] in a metric that favors Regev's approach suggests that, in analogy to the case of factoring, a state-of-the-art variation of Shor's algorithm is still the preferable way to compute a cryptanalytically relevant discrete logarithm with a quantum computer.

As a specific example, for finding a discrete logarithm for a 2048-bit modulus (a safe prime) with Shor's algorithm, [GE21, Table 5] estimates the use of 26 million qubits for one (seven hour) run of the algorithm.

Elliptic curve discrete logarithms

At comparable classical security levels (cf. [Gir20], which includes the BSI recommendations) elliptic curves appear to require less resources than factoring an RSA modulus with Shor's approach. Applying Shor's algorithm against an elliptic curve requires in particular the implementation of arithmetic on this curve. According to Proos and Zalka [PZ03], it is not necessary to implement the complete addition law on the elliptic curve, and it suffices to restrict to implement a generic case of a point addition—doubling and adding the inverse can be ignored. Roetteler et al. [RNSL17c] adopt this saving technique. An alternative would be to consider complete addition laws, but for odd characteristic no quantum circuits for such an approach appear to be available in the literature at this point. To implement the pertinent prime field arithmetic, Roetteler et al. invoke Montgomery multiplication and the extended binary Euclidean algorithm as a quantum circuit—not surprisingly, the inversion operation requires particular care, as the running time of a straightforward Euclidean algorithm depends on the inputs. The elliptic curve arithmetic itself relies on the familiar affine representation with a short Weierstraß equation $y^2 = x^3 + ax + b$.

A completely exact resource count would have to take the bit structure of the underlying prime field (and the constants defining the curve) into account, but based on the discussion in [RNSL17c] it seems reasonable to assume that the variation caused by this is not really significant. Overall, [RNSL17c] obtain the circuit characteristics shown in Table 4.6 for an elliptic curve over a prime field GF(p) with $n = \lceil \log_2(p) \rceil$, which are backed by simulation results in software. The table given here already considers a correction from [Roe17] for the case $n = 160$. The approach in [HNRSJ20] leverages AND gates and measurement-based uncomputation, and various trade-offs are offered. The number of qubits in their low-width designs is comparable to the values in Table 4.6. Specifically, for a 256-bit modulus a design with 2124 qubits, for a 384-bit modulus a design with 3151 qubits, and for a 521-bit modulus a design with 4258 qubits is reported. However, as shown in [HNRSJ20, Table 1] other trade-offs are possible, which at the expense of additional qubits reduce the circuit depth. For a fair comparison, it should be pointed out that, unlike [RNSL17c], in [HNRSJ20] measurements are part of the algorithm – e.g., for a 256-bit curve with the above-mentioned 2124 qubit implementation, about 1.76×2^{26} measurements are involved.

Table 4.6: Toffoli gate counts for a dlog computation over an elliptic curve over a prime field GF(p) with n = $\lceil \log_2(p) \rceil$, according to [RNSL17c, Table 2], [Roe17], taking into account a possible resource savings by [Eke21b, Eke21c].

N	***Number of qubits***	***Number of Toffoli gates***	***Toffoli depth***
160	1466	$1.49 \cdot 10^{10}$	$1.37 \cdot 10^{10}$
224	2042	$4.22 \cdot 10^{10}$	$3.87 \cdot 10^{10}$
256	2330	$6.30 \cdot 10^{10}$	$5.80 \cdot 10^{10}$
384	3484	$2.26 \cdot 10^{11}$	$2.08 \cdot 10^{11}$
521	4719	$5.70 \cdot 10^{11}$	$5.25 \cdot 10^{11}$

In general, [RNSL17c] offers an upper bound of about $9n + 2\lceil \log_2(n) \rceil + 10$ qubits and $448n^3 \cdot (\log_2(n) + 4090)$ Toffoli gates to be sufficient to implement Shor's algorithm. Additionally, $8n^2$ T gates are required for small rotations, and at least $290n^3 \log_2(n)$ CNOT and $71n^3 \log_2(n)$ NOT gates [RNSL17c]. The results in [Eke21b, Eke21c] do not change the qualitative picture – the number of qubits is not affected, but the number of gates and depth can approximately be cut in half.

Using a circuit from [AMMR13, fig. 7a], each Toffoli gate translates into a circuit on three qubits comprised of seven T- (resp. $T^\dagger$) gates plus two Hadamard and six CNOT gates with a T-depth of 4. An alternative circuit [AMMR13, fig. 13] reduces the T-depth to 3, using one more CNOT and a slightly larger overall depth. When implementing in the surface code in a time-optimized manner, the latter is the preferable circuit since the computation time only depends on the T-depth, and an additional CNOT does not produce much overhead compared to the T gates (see Chapter 8). Based on [HNRSJ20, Table 1], an alternative approach with measurement-based uncomputation (rather than a direct decomposition of Toffolis) can reduce the gate count by two magnitudes, but this comes at the cost of introducing numerous measurements. For instance, Webb et al.'s quantum resource analysis for a 256-bit curve [WEWH22] uses Häner et al.'s

approach as a starting point, starting out with 2871 logical qubits, $5.76 \cdot 10^9$ *T* gates and a measurement depth of $1.88 \cdot 10^7$. Incorporating overhead for error handling, Webber et al. [WEWH22] establish a fairly thorough quantum resource analysis for an attack against ECDSA. They argue that $3.17 \cdot 10^8$ physical qubits could enable a successful attack against a 256-bit curve within an hour, and $1.3 \cdot 10^7$ physical qubits would suffice for completing the calculation within a day.

Remarks

Roetteler et al. exploit a qubit-saving technique that avoids a dedicated Quantum Fourier Transform step in the last part of Shor's algorithm. This is different from the "textbook description" of Shor's algorithm. Instead of the QFT step at the end of the algorithm, $2n$ (single qubit) measurements are conducted *during* the execution of Shor's algorithm, and phase shift gates that are to be implemented depend on the outcome of these measurements.

Earlier work by Proos and Zalka [PZ03] suggests that resource savings are possible compared to the above approach. No actual simulation results for the latter approach have been reported so far, neither have exact Clifford+*T* counts been documented. However, if implemented as predicted, the number of qubits could potentially be reduced to about $5n + 8n^{1/2} + 4 \log_2(n)$. Proos and Zalka's more optimistic estimate suggests that for a 256-bit curve, 1500 logical qubits and a Toffoli depth of about $1.8 \cdot 10^{10}$ suffice. For a 512-bit curve, Proos and Zalka's more optimistic estimate suggests 2800 logical qubits and a Toffoli depth of about $1.5 \cdot 10^{11}$ to be sufficient.

Additional approaches to implement the necessary elliptic curve arithmetic

It is tempting to invoke a carefully drafted curve representation to minimize the circuit cost for the (double) exponentiation in Shor's algorithm. This opens seemingly an interesting degree of design freedom, but an important technicality needs to be considered: For Shor's algorithm to work, a *unique representation of group elements* must be ensured before the QFT step—this implies that a naïve use of projective coordinates is not adequate. The problem is somewhat similar to the uniqueness requirement for distinguished points in parallel classical implementations of the Pollard-rho algorithm.

A popular algorithm layout to implement the double exponentiation is to juxtapose two sequential variants of a double-and-add procedure [PZ03, KZ04, MMCP09]. Each addition circuit adds a precomputed point, i. e., one operand can always be "hard-coded," to the current intermediate result if and only if the appropriate bit in the exponent k respectively k' is set. To reduce circuit complexity, this addition is commonly only synthesized for the "generic case" (doubling, addition of the inverse, and identity argument are ignored). High-level modifications can be applied to reduce the depth of such a circuit: Roetteler and Steinwandt [RS14] suggest parallelizing the double exponentiation $g^k \cdot h^{k'}$ with a tree structure that substantially reduces the circuit depth at the expense of additional qubits. The extreme parallelization considered in [RS14] to achieve low depth exploits a uniform addition law on the underlying elliptic curve. In principle this is not needed, but unlike the sequential solution, a full implementation of the addition law—including all "exceptional cases"—is assumed. So far, no gate-level analysis of this parallel approach has been published for the prime field case. For binary fields, a depth $O(\log^2 n)$ implementation of Shor's algorithm is possible, but this comes at the cost of investing many additional qubits, so that a tree structure can be realized. For the prime field case one would have to cope with the same issue—to implement the parallel tree structure, a large number of qubits would be needed, and implementing the general case of the addition law appears quite costly. It is fair to say that at this point the "obvious" sequential approach to implement a double-and-add is the most promising approach for realizing the scalar multiplications/exponentiations in Shor's algorithm for elliptic curves.

As far as the curve representation and ground field arithmetic are concerned, various papers looked at the case of binary fields, including [MMCP09, ARS13, BS15], and Banegas et al. [BBvHL20] offers a design with $7n + \lfloor \log_2(n) \rfloor + 9$ logical qubits.

Going beyond Shor's algorithm

In [Eke21b], Ekerå extends earlier work on trading more extensive classical post-processing for the (repeated) use of a simpler quantum device, and presents an algorithm that does not require the order of the underlying group to be known. In cryptanalytic applications with a group of hidden order, Ekerå's algorithm enables a reduction of the number of group operations that need to be executed on a quantum computer compared to an approach based on Shor. Arguably, the more prominent cryptanalytic setting is a discrete logarithm problem in a cyclic group of known order. For this case, [Eke21c] improves slightly over [GE21] – reducing the number of group operations in each run of the quantum computer from about $n+2n/s$ to about $n+n/s$ for a trade-off parameter s. Compared to Shor's original algorithm, optimistically, we may hope that Ekerå's approach approximately halves the number of gates and the circuit depth.

In [Kal17], Kaliski suggests a hybrid approach to the discrete logarithm problem, leveraging a classical result by Blum and Micali. The idea is that for solving the discrete logarithm problem efficiently with a classical algorithm, it is sufficient to be able to approximate the *half-bit* of the discrete logarithm – which indicates whether the secret exponent is less than half of the group order – non-negligibly better than guessing. Kaliski suggests a candidate quantum algorithm for finding such a half-bit approximation, but a detailed analysis of how to derive a quantum circuit for cryptographically interesting problem sizes is currently unavailable. In the evaluation scheme of Section 3.2, Kaliski's hybrid approach offers (A) a correct algorithm, and it is (B) compatible with currently developed quantum hardware, but (C) the exact quantum resource needs for relevant problem sizes are unclear.

Parallel computation of multiple discrete logarithms on a dedicated hardware architecture

In 2023, Litinski considered the task of computing multiple elliptic curve discrete logarithms in the same elliptic curve group [Lit23]. He proposes a number of algorithmic modifications to reduce the cost over simply running Shor's algorithm multiple times. The improvements include combining multiple modular inversions into a single one and incorporating a classical exhaustive search for a part of the targeted secret. Litinski suggests the use of a specialized hardware architecture consisting of M modules, each module being connected with $O(\log M)$ other modules, where within each module nearest-neighbor two-qubit gates can be implemented. Realizing such an architecture with non-local connections effectively is not obvious at this point, but [Lit23, Figure 1] suggests that such an architecture with M=24,000 modules, each having 1,152 physical qubits, could potentially reduce the time for computing 256-elliptic curve keys into the range of seconds. Monitoring this design approach for possible elaboration and more detailed hardware considerations is appropriate.

4.4 The quantum linear system algorithm (HHL)

In [HHL09], Harrow et al. proposed a quantum algorithm to efficiently solve a type of linear algebra problem. This quantum linear system algorithm is now commonly referred to as HHL – after the initials of its inventors Harrow, Hassidim, and Lloyd. The algorithm can provide an exponential speed-up over the best available classical algorithm (based on the conjugate gradient method). One aspect that makes the HHL algorithm potentially interesting from a cryptanalytic point of view is the possibility to use it to solve polynomial systems of equations over GF(2). We give a brief overview of key aspects of HHL, mostly following [SVMA+17,DHMS+18], and then look into a potential cryptanalytic use, mostly following [Pla19]. The details of the algorithm are fairly involved, and we refer to [SVMA+17,DHMS+18] for a more elaborate discussion.

Given a Hermitian $N \times N$ matrix A with unit determinant (through a suitable embedding, this condition on A can be relaxed) and a vector b, the HHL algorithm in essence finds a solution to the quantum linear systems problem $A|x\rangle = |b\rangle$, making use of a spectral decomposition. More specifically, the quantum linear systems problem asks that given (oracle access to) the matrix A and given the state $|b\rangle$, to find a state $|x'\rangle$ such that the distance between $|x\rangle$ and $|x'\rangle$ is below or equal some error e with probability greater than 0.5. The running time of HHL to solve this problem is given by $O(\log(N)s^2\kappa^2/e)$, where s is a parameter

characterizing the sparsity of A, and κ is the so-called condition number of A, i.e., the ratio between A's largest and A's smallest eigenvalue.

The original HHL algorithm has been improved by a number of authors. In [Amb10], the running time is reduced to $O(\log(N)s^2\kappa\text{polylog}(\kappa)/e)$, and Childs et al. [CKS17] achieve a running time of $O(s\kappa\ \text{polylog}(s\kappa/e))$; further improvements have been reported by Wossnig et al. [WZP18]. Regrettably, the literature does not offer much work on gate-level discussions of HHL and its successors. Work by Scherer et al. [SVMA+17] is somewhat of an exception – their paper offers a case study with a quantum resource analysis of HHL in the Clifford+T model. Using a problem size of N=332,020,680 – which was hoped to be near the cross-over point with the best classical algorithm for an accuracy of e=1/100, the resulting circuit depth has been found to be in the order of 10^{25} or more – not yet taking into account overhead for fault tolerance. Scherer et al. make use of an HHL generalization from [CJS13], which has two key components: (1) quantum phase estimation, involving the QFT and Hamiltonian simulation and (2) quantum amplitude estimation which involves Grover's algorithm. The first part extracts information about the eigenvalues of A, and according to Scherer et al.'s analysis, the Hamiltonian simulation in this part, which implements an operator of the form $\exp(iAr)$ with $r=O(\kappa/e)$, turns out to be very costly in terms of gate complexity. In fact, taking this cost into account changes the circuit depth by more than three orders of magnitude, and the estimate for the number of qubits by more than five orders of magnitude. With these high resource counts, the cryptanalytic value of HHL over classical linear algebra tools remains fairly unclear.

Building on HHL, Chen and Gao, [CG18, CG21] established an interesting result that a polynomial system of equations in n variables with a total of t non-zero terms over GF(2) can be solved with gate complexity $\tilde{O}((n^{3.5} + t^{3.5})\kappa^2 \log(1/e))$ and success probability at least 1-e, where $0<e<1$. The main idea is to translate a (sparse) Boolean system of polynomial equations into a (sparse) system of polynomial equations over the complex numbers, and then use a Macaulay matrix approach to solve this system with HHL. The κ-value in the cost estimate is the condition number of the involved Macaulay matrix, so the obvious question is to determine/estimate such condition numbers. Determining actual values for κ in systems of interest appears non-trivial. However, Ding et al. [DGGHL23] established a lower bound on the running time of Chen and Gao's algorithm, suggesting that for cryptanalytic settings this approach is not attractive. More specifically, in a cryptanalytic scenario, the solution of the Boolean system of polynomial equations is commonly a (unique) random vector, and Ding et al. argue that the running time can be expected to be lower-bounded by a function that is exponential in the Hamming weight of the solution. And as a consequence, relying on Grover's algorithm seems actually preferable over HHL to find a solution of the Boolean system of equations. Ding et al. consider alternative approaches to Chen and Gao's, but it seems fair to say that at this point there is no indication of HHL having practical cryptanalytic impact. In the evaluation scheme of Section 3.2, HHL qualifies as (A) algorithm with provable correctness, and it is (B) compatible with currently developed hardware. However, with a relevant cryptanalytic impact being unlikely, (C) there is currently little cryptographic motivation to develop a detailed quantum resource analysis of HHL. The exponential lower bound on the condition number that Ding et al. [DGGHL23] establish for the cryptanalytically arguably most interesting scenario is a fairly impactful result. It suggests that several other quantum approaches to solving linear systems of equations [SSO19, LT20, CAS+21, AL22] are very limited in their cryptanalytic reach, too, as their efficiency depends on the condition number being not large.

5 Cryptanalysis on NISQ computers including adiabatic quantum computers

Below we assess a number of works that describe advances of quantum cryptanalysis for the NISQ era. To do this, we evaluate the algorithms along the evaluation scheme for quantum algorithms introduced in Section 3.2, ranging from Level A through C. In principle, it is conceivable that NISQ computers, whose gate set is not restricted to Clifford+T and which can execute roughly p^{-1} two-qubit gates with small error probability, can attack realistic cryptographic codes. As noted in Section 3.1.2, the reasonable assumption of two-qubit gate errors of no less than $p \simeq 10^{-5}$, which is below the error correction threshold, results in the possible execution of up to $p^{-1} \simeq 10^5$ quantum gates per run. As we show in this chapter, for cryptanalytic applications the literature does at this point not offer quantum circuits that have been shown to meet these criteria. This is reflected by the fact that no algorithm evaluated below has reached level C.

With regards to the discrete logarithm, low-depth solutions have been considered for solving the discrete logarithm problem on particular elliptic curves [RS14], but this comes at the cost of a large number of gates and qubits. On the side of symmetric key encryption, the potential improvement over a Grover-based exhaustive search suggested in the discussion of the Tiny Encryption Algorithm in [SS10] deserves mentioning. However, there is no clear statement about the expected running time available, and for established block ciphers (including AES) no non-trivial resource analysis of the adiabatic approach is available in the literature. Despite the polynomial equivalence with the circuit model, one could hope for an improvement in the exponent, but the current literature does not offer a sufficient foundation to make reliable quantitative estimates.

As a consequence, below we first describe and evaluate several proposed NISQ algorithms for prime factorization, and afterwards discuss subroutines of algorithms that a priori cannot be run on NISQ devices. We also include adiabatic quantum computation in this chapter. For completeness, it should be said that there are also approaches for quantum error correction in the adiabatic scheme (see, for example, [JFS+06]), which is meaningful if there is a proof of speedup with the energy gap of the adiabatic quantum computer being bounded as needed. However, this has not been established to adiabatic algorithms for quantum cryptanalysis.

5.1 Adiabatic quantum computation model

The quantum cryptanalytic literature focuses on the quantum circuit model and on minimizing the number of qubits, quantum gates, and the circuit depth as critical parameters. Such circuits are designed to be implemented on a fault-tolerant quantum computer; depth and gate counts for *T*-gates are often considered separately, to facilitate accounting for the implementation cost of this non-Clifford gate. *Adiabatic quantum computation* [AL18b] offers an alternative approach, but at this point, the cryptanalytic significance of the adiabatic approach for realistic cryptographic parameters remains unclear. Some interesting experimental work on toy parameters is available, but a reliable way to extrapolate from these results to genuine cryptographic parameters is lacking. Below we document some of the results achieved in the literature but note that – differing from the literature on quantum circuits – there is at the moment no obvious roadmap or implementation strategy on how to apply adiabatic quantum computation for computing a discrete logarithm or for factoring an RSA modulus as used in cryptographic applications.

5.2 Prime factorization

In 2002, Christopher Burges formulated the task of integer factorization as an optimization problem [Bur02]. Since optimization is an application of quantum computation, it is perhaps not surprising that in the meantime a number of different NISQ approaches for such factorization via optimization have been put forward, including [JBM+18,AOGC19,HPAA+21,KSK+21].

Suppose we are given an input biprime number N, which is the product of two prime factors p and q, i.e., $N = pq$. A key step in the setup of adiabatic quantum computation is to encode the prime factors of N into the

ground state of a Hamiltonian acting on a collection of qubits. To arrive at such a Hamiltonian, one introduces a cost function defined for integers x,y>2

$$f(x,y)=(N-xy)^2,$$

which clearly is zero only when x and y are the prime factors of N. The resulting Hamiltonian can then be obtained by replacing x and y with their bitwise operator representation. Alternatively, in a classical preprocessing step one can compute the bitwise multiplication table of the product of the variables xy, which lowers the number of required qubits for the following optimization. Details for these methods are given in Appendix 14.

For example, Dattani and Bryans' work on factoring 56,153 with only 4 qubits [DB14] in the adiabatic regime shows interesting potential for the operand size that can be considered when translating the integer factorization problem to an optimization problem, but it is not clear how their finding can be leveraged to factor a realistic RSA modulus. In terms of the evaluation scheme in Section 3.2, the underlying approach is plausible, but with the currently available data, the scalability and asymptotics are unclear (level *B*). Similarly, Schaller and Schützhold's work [SS10] evidences that one can solve the factoring problem for an RSA modulus more efficiently than a generic NP problem with the adiabatic approach, but a quantifiable impact for realistic RSA parameters is unclear. In the absence of more experimental data, the scalability and asymptotics remain open questions (level *B*). Small-scale recent examples of explicit prime decompositions include the factorization of 200,099 = 401×499 [DA17] (using Gröbner bases techniques for pre-processing), 249,919 = 491×509 [JBM+18], and 1,028,171 = 1009×1019 [WHYW20], but extrapolating the effectiveness of these methods when scaling to cryptographically relevant inputs, e.g., a 2048-bit RSA modulus, remains an open issue (level *B*).

Several different quantum computing methods for finding the ground state of H_1 have been applied. Below we describe and assess approaches of using digitized adiabatic quantum computation, quantum annealing and variational quantum eigensolvers.

5.2.1 Digitized adiabatic quantum computation

In [HPAA+21], Hegade et al. introduce the application of digitized adiabatic quantum computation to the prime factorization problem. This means that the adiabatic evolution is realized by a sequence of quantum gates rather than a continuous change of the instantaneous Hamiltonian's parameters. Details of this scheme are discussed in Appendix 14.

The time evolution is approximated by carrying out so-called *Trotter steps* (which are related to the Trotter formula). Such a Trotter step is used for carrying out quantum gates based on a particular type of Hamiltonians, which are sums of non-commuting and natively realizable quantum operators. The Trotter formula is a direct consequence of the Lie Product formula [Hal13], and its use in quantum computation is detailed in Nielsen and Chuang [NC00]. The number of Trotter steps constitutes a hardware-agnostic cost function associated with the quantum algorithm of Ref. [HPAA+21]. This number is agnostic to hardware, because it is a property of the algorithm and thus independent of the quantum device. In contrast, the duration of the realization of each Trotter step depends on the used hardware.

Reference [HPAA+21] implements two different approaches, one with and one without a classical preprocessing step. For each approach, two different driving techniques are discussed, one of which is the straightforward application of digitized adiabatic quantum computation, and the other using an additional ingredient called "shortcuts to adiabaticity". These in total four different variations of the algorithm are compared using both numerical simulation and experimental realization. The largest number thus factorized is 2497 using numerical simulation [HPAA+21].

For the evaluation within the algorithmic scheme in Section 3.2, first consider level *A*. The concept of adiabatic quantum computation is a paradigm that has been proven to be equivalent to gate-based quantum computing, and all the procedures that are part of the algorithm are well established.

Now consider level *B*. The algorithm has been tested both numerically and experimentally. However, [HPAA+21] does not provide sufficient data to predict asymptotic scaling behavior of the proposed implementations of the algorithm. While the authors do report numerical data of factoring six integers, an evaluation of the cost function is done only for three of these. Since, furthermore, those three data points

belong to two different variations of the algorithm, we have only at most two data points for the proposed analysis.

Another complication is the realization of the Trotter steps mentioned above. Each Trotter step is realized by several quantum gates, labeled *K* in [HPAA+21]. Hegade et al. do not disclose this number *K*, so we know neither the total number of steps for any of the calculations, nor can we discern the growth of *K* when increasing the input size.

The algorithm of [HPAA+21] is to be sorted in level *B* of our evaluation scheme since it fulfills the bare minimum requirement of level *B* ("tested on hardware") and parameters for evaluation of the cost function have been provided. However, the amount of data is insufficient to draw any conclusions towards the algorithm's asymptotic complexity. As noted in our description of the evaluation scheme at the end of Section 3.2, the cost function scaling of this algorithm would have to be a polynomial with low degree to be critical for cryptanalytic purposes.

5.2.2 Quantum annealing

In Reference [JBM+18], Jiang et al. show a method to perform prime factorization on a quantum annealer. Like the case of variational quantum eigensolvers described in Section 5.2.3, the cost function for the quantum annealing problem is cast into an Ising Hamiltonian. Many quantum annealing devices, such as those manufactured and operated by the company D-Wave Systems, are limited to pairwise couplings, i.e., in this case the Hamiltonian needs to have at most 2-local terms. The reduction to such Hamiltonians can be realized by introducing additional Hamiltonian terms [JBM+18].

The main challenge in investigating claims based on adiabatic quantum computing / quantum annealing is the careful benchmarking of speedup. The paper [JBM+18] explicitly refrains from any statement to this end, see second paragraph of its conclusion. We describe this challenge along this paper in two ways:

First, orthodox adiabatic quantum computing requires the quantum computer to always remain in the ground state thus mandating a duration of the annealing schedule proportional to the inverse minimal spectral gap of the problem. This is a sufficient condition at zero temperature. An annealing schedule thus has polynomial time scaling if that minimal gap drops polynomially in system size. For general constrained optimization problems, this gap is at least conjectured to drop exponentially. Again, an analysis of scaling of the gap is not given in the paper. Also note that while previous work of Aharonov et al. [AvDK+07] states that any gate-based algorithm can be mapped onto an adiabatic algorithm without changing time complexity, this construction is not used in Jiang et al.

While this is a zero-temperature argument, one needs to observe that for a large problem, the spectral gap even if only polynomial in problem size will dive below the experimental temperature. This requires either error correction or genuine quantum annealing, i.e., quantum-assisted relaxation from the low-lying excited states to the ground states. The latter describes the approach in D-Wave machines.

Quantifying complexity and speedup in quantum annealing in a reliable mathematical way has not been achieved in the literature. No state-of-the-art analysis has been presented in [JBM+18]. In summary, while this paper shows an approach to factoring on an annealer, it does not give any indication of quantum speedup. While not impossible, speedup is unlikely. A full investigation of speedup would require a full research project with major access to hardware.

While the D-Wave quantum annealers have grown comparatively rapidly over the last decade to hosting up to 5000 qubits per machine, an indisputable proof of a computational advantage for an algorithm running on a D-Wave machine has not been put forward. Nevertheless, the basic theory of quantum annealing, which is a limited form of adiabatic quantum computation, is founded on a widely accepted theory rooted in statistical physics [KN98].

This algorithm has been tested on hardware, and in [JBM+18] four different biprimes ranging between 15 and 376289 have been factored. This work provides detailed experimental data (such as the run time and figures related to the success probability) for two of these calculations (see Fig. 1 in [JBM+18]). We thus do not have access to sufficient data that would allow for estimating the asymptotic complexity of the algorithm (level *B*).

5.2.3 Variational quantum factoring

A work by Anschuetz et al. on variational quantum factoring (VQF) [AOGC19] offers an alternative to Shor's algorithm for finding an integer's prime factorization using a hybrid quantum-classical algorithm. These hybrid algorithms like the Quantum Approximate Optimization Algorithm (QAOA) [FGG14] allow in some cases to benefit from quantum advantage with short segments of algorithms hence compatible with a rather large logical error rate. Pertaining to the class of variational quantum algorithms [CAB+21], they employ the variational principle to find approximate solutions to a given problem by encoding the problem in a Hamiltonian whose ground state corresponds to the approximate answer one is seeking. They depend on a heuristically chosen ansatz to probe the Hilbert space around an initial guess for the ground state.

Similar to works described above, in [AOGC19] Anschuetz et al. map the problem of finding the prime factors to an Ising Hamiltonian, whose ground state is given by the prime factors. The ground state is searched for using QAOA [FGG14]. By using efficient classical preprocessing, the authors can greatly reduce the number of qubits needed. They provide empirical data claiming that using their preprocessing methods require only about 50 qubits to factorize a number of size 10^5, a threefold improvement compared to the qubit requirements without their pre-processing method. They simulate their algorithm under the assumption of noise by a Pauli error channel. They check their algorithm for integers 35, 77, 1207, 33667, 56153, and 291311, and find that VQF can in principle find the prime factors, even though in some cases it performs rather poorly if certain symmetries are violated.

An experimental application of this variational quantum factoring algorithm is reported in [KSK+21]. In that work, three numbers (3127, 6557, and 1099551473989) are factored on a superconducting quantum processor. To understand their work better, the results are compared to a simulation that incorporates a nontrivial noise model that takes certain dominant two-qubit noise terms into account. For the two smallest of the three factored numbers, 3127 and 6557, the success rate reaches roughly 25%, which the authors attribute to the dominant two-qubit noise. For the third number, 1099551473989, a success rate of 80% is achieved.

As noted above, the variational quantum factoring algorithm introduced in [AOGC19] is based on QAOA [FGG14], which is a broadly accepted and commonly used algorithm for quantum optimization. The only data that is currently available in [AOGC19] stems from numerical simulations, which are based on a noise model that features only a simple Pauli error channel. Whether experimental data will yield results that are like the simulation data remains to be seen. This is not certain since the accessible numerical data from Ref. [KSK+21] gives rather unfavorable results. Also note that [KSK+21] only presents data for the factorization of three numbers, which is insufficient for a complexity estimate.

In conclusion, the algorithm described in [AOGC19] and experimentally applied more recently in [KSK+21] is to be sorted into level *B* since it is built on a sound framework and has been tested on quantum hardware. These hardware test results seem to be not very promising. We note, however, that follow-up work on this algorithm should be watched closely for two reasons. (i) the depth of QAOA is low, which is a major advantage for NISQ applicability. Furthermore, (ii) in the discussion of [AOGC19], the authors express their intention to collaborate with their partners to implement their algorithm on current NISQ devices to obtain detailed experimental data with the goal of drawing conclusions regarding the algorithm's scalability.

5.3 Discrete logarithm computation

Wroński demonstrated that the feasibility of a discrete logarithm computation in the prime fields GF(11), GF(23), and GF(59) on a D-Wave architecture [Wro22]. However, the approach is not expected to scale well, and the author points out that "the presented methods should not outperform Shor's polynomial-time algorithm for large prime fields." In the same line of work, Mahasinghe and Jayasinghe [MJ22], show how a discrete logarithm problem in a finite field can be mapped on a D-Wave architecture. Reported implementation examples include computations in GF(3) and GF(5), and the scalability to cryptographically relevant instances is unclear (level *B*). Mahasinghe and Jayasinghe specifically point out the challenge of scaling the classical precomputation used in their approach.

For the elliptic curve discrete logarithm problem over prime fields, Wroński showed that a D-Wave architecture can handle a cyclic group of order 271, using the elliptic curve $y^2=x^3+x+4$ defined over GF(251) [Wro21] with the curve point (128, 44) as generator. However, the scalability of the proposed approach remains an open question (level *B*).

On the side of symmetric cryptography, the potential improvement over a Grover-based exhaustive search suggested in the discussion of the Tiny Encryption Algorithm in [SS10] deserves mentioning. However, also in this case there is no clear statement about the expected running time available, and for established block ciphers (including AES) no non-trivial resource analysis of the adiabatic approach is available in the literature. Despite the polynomial equivalence with the circuit model, one could hope for an improvement in the exponent, but the current literature does not offer a sufficient foundation to make reliable quantitative estimates. Similarly, Burek et al. [BWMM22] present a setup for an algebraic attack that in principle can be mounted using quantum annealing, but the running time of this attack is an open question (level *B*). Consequently, in our discussion we focus on the quantum circuit model.

5.4 Quantum computing for the shortest vector problem

A promising modern cryptosystem, lattice-based cryptography, is currently viewed as secure against quantum attacks. In that scheme, the security relies on hardness of the shortest vector problem (SVP) in both exact and approximate form.

SVP is conjectured to be hard even when employing quantum computers, but there is no proof that quantum computers cannot solve it in polynomial time. Despite the fact that the time complexity of AQC algorithms is in general hard to estimate, AQC is a valid candidate for the attack on lattice-based cryptography for two reasons: (1) SVP can be formulated as an optimization problem, and (2) while AQC in general has a prohibitive time cost of achieving adiabaticity, for approximate SVP up to a threshold, approximate solutions are also admissible.

SVP is defined as finding a shortest nonzero vector in a lattice given a particular basis, in the approximate version of the same problem the task is to find a vector whose length is upper bounded by a multiple of the length of the shortest vectors.

5.4.1 Approach via quantum annealing

The paper [JGLM19] proposes an embedding into an adiabatic quantum computer achieving that result. This method could be used to attack lattice-based cryptography. The embedding proceeds in multiple steps. It utilizes the Bose Hubbard model. This is a model of quantum particles embedded in a lattice that can move in the lattice and that can repel each other both on the same lattice site as well as across the lattice. Tayloring these interactions defines the lattice for the lattice-based algorithms and minimizing the interaction energy corresponds to solving the SVP problem. Quantum annealing is proposed to solve this model. The quantum tunneling term that is used to initialize the state is in this case the kinetic energy of particles hopping in the lattice. It is adiabatically switched off to settle the particles in a state that minimizes the interaction to solve the problem.

This being based on the Bose (not the Fermi) Hubbard model means that more than two states are allowed per lattice site, i.e., more than one qubit. This overhead does not change the observation that the embedding is efficient in the number of qubits. As an important technicality, rather than the ground state (which is the zero vector), one is looking for the first excited state. This complication is elegantly circumvented by using a separate state to represent the zero vector.

The analogy to the Bose Hubbard model is noteworthy. This model can be directly simulated in the sense of analogue, single-purpose quantum simulation, specifically cold atoms in optical lattices, see Section 13.2. Design of appropriate programmable interactions as it is, e.g., done in the EU Flagship project PASQuanS [PAS18] would allow to scale rather quickly. In fact, verification of quantum supremacy in these systems is an active field of research [EHWR+19, HKEG19]. The Bose-Hubbard model can also be studied in superconducting circuits [FZ01, LH10], combining the ease of programming and design of these systems (boosted by the tools developed around the quantum supremacy experiment) with a compact native application of this model. An aggressive scaling project of those simulators is not known.

As described above, a clear proof of quantum speed-up would require extracting the energy gap across the sweep, which is not achieved in [JGLM19]. Rather, they rely on numerical simulations on classical computers covering small examples (dimensions 2,3, and 4). These experiments confirm the value of adiabaticity, i.e., that if sweeps get slower, the distribution of output values clearly clusters at low energies. This is not made quantitative into a scaling analysis with, proven or extrapolated, speedup. It is pointed on new discussions of continuous but not fully adiabatic algorithms with no clear conclusion given.

In conclusion, the algorithm described and tested in [JGLM19] belongs to level *B* of our evaluation scheme.

The proposed faster sweeps are an interesting metaheuristic whose potential is not fully understood. Given the hardness of gap extraction, to evaluate these heuristics in interesting size, benchmarking on actual hardware would be the most important way forward and should be closely monitored. There is some indication that (repeated) fast sweeps reduce the time to solution [CFLLS14] but those have been done for generic cases and not for this specific model.

5.4.2 Quantum variational approaches

An approach to solving SVP on NISQ computers is described in [ASPW23]. The underlying approach is the use of a variational quantum algorithm, which is similar to the factoring algorithm discussed above in Section 5.2.3.

The authors of [ASPW23] state that at most a polynomial speedup (similar to Grover's algorithm) is expected from this approach. The objective aim of the study is to find the required qubit overhead as a function of the size of the problem, i.e., the dimensionality of the lattice. Because of this, the authors assume perfect qubits, and perform experiments on quantum simulators alone rather than on noisy hardware.

The solution to SVP is encoded into the ground state of a Hamiltonian. The calculation then proceeds by repeatedly using classical and quantum computers in turn. Besides this usual approach of the variational quantum algorithm, [ASPW23] first estimates bounds for lattice enumeration, through which new bounds on the number of required qubits are obtained. Furthermore, a difficulty with this approach is the exclusion of the zero vector from the quantum calculation, which is solved by that study in two different ways – one by altering the classical computation, and the other by modifying the used Hamiltonian.

The main result of the paper is that at most $O(n \log(n))$ qubits are needed for solving SVP for a lattice of dimension n. The experimental results include lattices with dimensions up to $n = 28$, which is the largest number realized so far in a quantum emulation. While further the number of calculation steps grows linearly with the size of the lattice, n, the authors state that an extrapolation to cryptographically relevant lattices (with dimensions larger than 400) cannot be extrapolated "with confidence" [ASPW23].

In conclusion, this algorithm seems to work rather well, though only rather small problem instances have been considered. Besides, the effects of noise have not been taken into account (level B).

5.5 Other linear algebra problems

In the field of linear algebra, consider the problem of solving a system of linear equations, or find x in the equation $Ax = b$, where A is square matrix with N many rows, and where x and b are column vectors with N many entries. The computational complexity of this problem when run on a classical computer is polynomial in the number of calculation steps. On a quantum computer, this problem may be solved using an algorithm due to Harrow, Hassidim and Lloyd [HHL09], which – together with its cryptanalytic relevance – is discussed in Section 4.4. In this way an exponential speed-up over known classical algorithms is conceivable.

[XSE+21] attempts to solve the same linear algebra problem using a NISQ computer. In that study a variational algorithm has been employed, which means that it is the same type of algorithm as that discussed above in Section 5.2.3. Most quantitative results presented in the paper stem from numerical simulation, while data for a minimal problem instance (in which the dimension of the problem is $N = 2$) have been obtained on a physical quantum device. The simulation data covers problem instances between $N = 2$ and $N = 64$. However, a decrease in complexity is not evident.

While most data have been obtained by simulations on classical hardware, the range of input values is significant. Nonetheless, the results of [XSE+21] suggest no significant speed-up in computation time for problem instances of up to $N = 64$ (level *B*).

5.6 Focus on algorithmic elements

An alternative to running quantum algorithms whose termination is unknown on NISQ devices is to consider a single subroutine of a quantum algorithm whose asymptotic complexity is known, and which is currently expected not to run on NISQ computers for relevant input. For example, Cleve and Watrous [CW00] showed that the Quantum Fourier Transform (QFT)—which is at the heart of Shor's algorithms—can be realized in logarithmic depth, but for the number of gates needed, only a polynomial bound is available.

In view of the overhead incurred by error correction, researchers have explored the possibility that errors at the gate level may be tolerated without significantly impeding the logical correctness of a cryptanalytic algorithm. Indeed, Nam and Blümel (see [Nam17, NB15b, NB15a]) make the case that a QFT implementation can perform very well even in the presence of noise and gate defects—thus suggesting that if the QFT is performed at the end of Shor's algorithm, one could try to be lenient with error correction. One may also hope to simplify the QFT by passing to an approximate QFT (see [Cop94,NSM20]), but for state-of-the-art implementations of Shor's algorithms the logical gate cost is dominated by the arithmetic portion. State-of-the-art implementations of Shor's algorithm such as [RNSL17c] save qubits by using a semi-classical QFT variant, with repeated (single qubit) measurements, where the required rotations are chosen adaptively (in dependence on preceding measurement outcomes), and savings/avoidance of error correction in the arithmetic would be particularly valuable.

A common approach for the arithmetic tasks is to start with a reversible circuit which is then further decomposed into Clifford and *T* gates—resulting in various options, e.g., to decompose a Toffoli gate (see [AMMR13,Jon13]). However, there is very limited literature on error tolerance of arithmetic in Shor's algorithm. Notably, in [Nam17], Nam considers an implementation of Shor's algorithm for factoring in the presence of errors in the angles occurring in elementary gates. Due to resource constraints the reported simulations are restricted to very small examples (Chapter 9 in [Nam17] discusses factoring of 21), which does not allow to meaningfully extrapolate gate counts for the arithmetic for cryptographically relevant factorization problems. In recent work [NB17] on working with imperfect gates, the question to what extent errors can be tolerated in a large-scale (cryptanalytic) computation remains open. In [NB15a], one particular adder design is considered and identified as quite robust against gate errors, but it remains open to what extent this can simplify a full-scale implementation of Shor's algorithm. Taking into account debugging considerations, implementing a Toffoli-based arithmetic (cf. [HRS17, RNSL17c]) may in fact be considered as preferable over a (QFT-based) adder design as considered in [NB15a].

Work predating Nam and Blümel's on the robustness of Shor's algorithm in the presence of errors is due to Devitt et al. [SJD06]. They consider specifically the quantum period finding (QPF) subroutine of Shor's algorithm and explore if a more lax error bound than imposing a precision of about $1/(\text{depth} \times \#\text{qubits})$ can be achieved. To test this, they apply three different discrete errors (bit flip, phase flip, both) randomly to the QPF portion of Shor's algorithm. Each number of errors was simulated 50 times for specific factorable numbers with a binary length L ranging from 5 to 10 (invoking $2L + 4$ qubits) to determine how many errors were allowable until the result was no longer useful. Their results suggest that for larger L, more errors were acceptable. For example, when $L = 5$, at most 15 errors were acceptable before the result was unrecognizable from random, but with $L = 8$, up to 40 errors could be allowed. However, even a single error for $L = 5$ reduces the probability of success to 0.34. These results suggest that the precision of $1/(\text{depth} \times \#\text{qubits})$ can be reduced to $p(L)/(\text{depth} \times \#\text{qubits})$ where $p(L)$ is monotonically increasing and at least linear in L. Devitt et al. note that the greatest benefit of these results is for small simulations of QPF where observing the quantum process is the goal and extensive quantum error correction may not be feasible. However, for large factoring problems (such as attacking cryptographically relevant RSA parameters) extensive error correction will still be required since the overall size of the quantum algorithm grows much faster ($O(L^4)$) than this error rate.

All work described in the several paragraphs above is about the cancellation of systematic errors due to a specific arrangement or symmetry of quantum gates. It is, of course, to be expected that any such

“accidental error tolerance” of arithmetic operations will depend on specific algorithmic choices (e.g., how exactly is a modular multiplication implemented, or how exactly is a point addition on an elliptic curve realized?).

Another promising direction to watch is the direct implementation of Toffoli gates in hardware. These have been demonstrated in ion traps [FML+17]. The observed error rates are not disruptive and not affecting our conclusion but deserve further attention.

PART III: Quantitative description of hardware evaluation scheme

This is the core connection between algorithms and the resulting gate counts and the evaluation of hardware. Given that the algorithms of proven cryptanalytic relevance require quantum error correction, it is primarily driven by the needs of this rather well-formulated framework. More background and its connection to the evaluation system at large is given in Section 3.2.

The five levels of this scheme define a coarse evaluation also in the type of research and development that takes place in these levels – level A describes physics experiment, levels D onwards large integrated efforts. They also need to be mounted consecutively with only little overlap: For example, does level B require that all basic functionalities of level A are met. They typically contain multiple sub steps whose order is not critical. In this vein, Chapter 7 describes level A, where basic component functionalities are verified that allow to run small protocols. Chapter 8 describes level B, where small protocols that can quantitatively evaluate device errors are described and the main quantitative indicators are introduced. Chapter 9 describes the mainstream of error correction that allows to understand levels C through E. It focuses on level C, while the subtleties of level D are moved to an appendix. Chapter 10 describes more specialized topics in error correction that are making a mark in the literature right now.

While focused on fault tolerant quantum computing, the ingredients to the scheme also apply to NISQ, but here one would focus on levels A and B and then test algorithmic performance right away.

6 Low-level analysis of qubit systems

6.1 Initial remarks

6.1.1 Scope and motivation

The present analysis is the lowest (in the sense of being closest to hardware) level of a cascaded evaluation system for quantum computing candidates. It talks about physical qubits and operations only. It contains parameters that are easily characterized experimentally and serve as a stepping-stone for level B evaluation schemes (see Chapter 8) that are in turn the basis for analyzing fault tolerance requirements (see Chapter 8).

Such a low-level scheme has been published a long time ago in the form of the DiVincenzo criteria [DiV00]. These criteria were giving a succinct summary of what it takes for a qubit candidate to be serious, mostly to help new and then-emerging (condensed matter) platforms to evaluate themselves and ask the right questions. Notably, these criteria are not quantitative (which they do not have to be, only the next level should) but they do not even give suitable numbers to use. As the field has matured since then, this part of our survey explores these numbers as they are typically given in experimental papers. It also compares different quantifiers used in different experimental traditions and develops relations between them. We review the DiVincenzo criteria and the modern ways to clarify and quantify them.

For a large-scale analysis of quantum computing candidates, this serves as an entry ticket. If these criteria and parameters cannot be verified and measured satisfactorily, development of architectures and measurement of performance parameters that are relevant for fault tolerance are usually futile—they require a functional qubit to at least have some understanding of which design operates under which condition. This is thus the lowest-level performance check for quantum computing platforms.

Notable special cases are adiabatic quantum computing/quantum annealing and cluster state quantum computing, which, although not fundamentally different, put different priorities on hardware and are thus not easily connected to these criteria and therefore need to be treated differently. We will describe how to evaluate them in a separate Section 9.1. We would also like to note that, albeit driven by the DiVincenzo criteria as well, photonic quantum computing is often described by more domain-specific indicators, which we will describe within the photonic platform Section 13.4.

6.1.2 Limitations

The next level beyond these low-level analyses is centered around randomized benchmarking (RB) [KLR+08, RLL09, MGE12, ECMG14, MLS+15, XLM+15, TB16] as covered below in Chapter 7. It plays a connecting role as it is relatively easy to use experimentally given basic qubit functionality. It consists of preparing a convenient initial state, running a sequence of random Clifford gates, invert it by a single further Clifford gate (relying on the fact that these gates form a group that can be efficiently simulated classically) and measure the survival probability of this initial state. It can be shown that this maps out the average fidelity of the sequence and can hence be a reliable estimator for the error per gate. Usually, the survival probability when fitted with an exponential does not extrapolate to unity at the initial time. The gap, i.e., the errors that even occur at zero gates, capture state preparation and measurement (SPAM) errors. Low-level performance indicators covered in this section are discussed up to the point where performing RB would be the more adequate choice. A detailed description of RB as well as its limitations is given later.

6.2 Review of DiVincenzo criteria

The 5+2 criteria [DiV00] for quantum computation are:

1. a scalable physical system with well characterized qubits
2. the ability to initialize the state of the qubits to a simple fiducial state

3. long relevant decoherence times, much longer than the gate operation time
4. a universal set of quantum gates
5. a qubit-specific measurement capability
6. the ability to interconvert stationary and flying qubits
7. the ability to faithfully transmit flying qubits between specified locations.

A few initial remarks are in order.

Well-characterized qubit array

The requirements that the qubits are *well characterized* means that the physical parameters should be accurately known, including the internal Hamiltonian, couplings to other qubit states, interactions with other qubits and coupling with external fields. Higher qubits states should be avoided (leakage) so the physical qubits represent mathematical qubits—abstract two-level systems. The proper identification of the qubit needs to be done carefully. Remedies to imprecise characterization can be found in robust control, which are however generally less efficient than controls for precisely characterized systems.

Initialization

The need for initialization arises from the straightforward computing requirement of known initialized registers. The evolution of a closed quantum system is unitary, hence invertible, whereas initialization is not invertible. Thus, initialization requires opening the quantum system operation to achieve a non-invertible action, e.g., cooling or measurement. Initialization is also important for quantum error correction, where a continuous supply of fresh qubits for re-encoding is a real headache for many implementations. The speed of initialization is an important issue in experiments.

The main approaches for initialization are projective measurements with feed-forward correction and cooling to the ground state of the Hamiltonian. For the former, we measure the state and apply an additional gate depending on the measurement outcome [RvLK+12]. The latter, cooling, works if the energy gap between the ground and first excited states of the quantum computer is much smaller than the temperature in appropriate units. In practice, it is hard to define that temperature in some cases—e.g., the effective temperature of a Josephson circuit is usually higher than the temperature of the surrounding Helium bath—which can be mitigated by making temperature margins wide enough. Unfortunately, natural cooling is on the same timescale as energy relaxation, which is just the bit flip error rate described below, posing a conundrum when using this method within error correction. This is mitigated if the relaxation rate can be switched or otherwise manipulated. In some optical approaches (ions and neutral atoms), where qubits are encoded in hyperfine states, relaxation is so slow that it needs to be manipulated by optical pumping: selective excitation of one of the qubit states to a metastable excited state.

Coherence

Coherence times characterize how long a quantum system maintains its information. This is important for the functioning of quantum algorithms which rely on the quantum properties of the system. The loss of coherence, decoherence, can arise, e.g., due to interactions of the quantum state with the environment, or due to leakage into other quantum states. To avoid errors in quantum computation, the coherence time must be long enough, where “long enough does not mean necessarily the whole duration of the process, but can be reduced with error correction. This is discussed in Section 3.2.1 and Section 8.3.

Coherent errors

Note that also errors other than those due to decoherence enter that threshold, e.g., systematic errors such as gate axis misalignment or over- and under-rotation. The latter two errors are unitary errors where in the first case the rotation axis n' is tilted compared to the ideal axis n, and in the second case the rotation angle $\theta' = \theta \pm \epsilon$ is too large or too small. The former occurs, for example, in gates driven by resonant radiation if

the resonance condition is not met perfectly, the latter occurs based on errors of amplitude of the drive field or timing. A more detailed description of those is given in the Appendix (Chapter 15).

Universal set of gates

The universal set of gates is the heart of quantum computing. In principle, the desired Hamiltonians to perform quantum gates are turned on and off via external controls, with somewhat smooth pulse shapes. These have to address all the interactions that cannot be turned off, e.g. in NMR, i.e., in the presence of spurious coupling, there is some control required to simply keep qubits or registers idle, typically in the form of refocusing operations. Refocusing consists of designing control sequences such that the impact of undesired term averages out in the end. Its simplest example is Hahn spin echo [Lev01,VC05]. It has been invented in original NMR and can be interpreted in quantum computing to protect quantum memory from inhomogeneity. Turning off all couplings between the spins is known as decoupling, and turning on specific couplings is called refocusing, and the latter can be done efficiently [LCYY00,VC05]. The drawback of these techniques is that they make gate sequences longer thus making operations more susceptible to unitary error. Refocusing is compatible with error correction, see Appendix 24 in an older version of this study [WSL+20]. In the context of our evaluation scheme, experimentalists will decide whether to use refocusing for their operations and benchmark them accordingly on level B.

Also, auxiliary systems are used for gate implementations, e.g., in ion traps, where direct interactions between qubits cannot be turned on. Also, fully parallel operations are needed for quantum error correction, which can be a problem when a single bus is used to mediate the interaction between arbitrary qubits, while nearest neighbor interactions allow for sufficient parallelism. Systematic errors due to imperfect gates should be below the error correction threshold [Pre97b, DiV00]—see measures for error rates described for level B in Section 8.4, and thresholds described for level C in Section 9.2.1.3. Note that we are talking about physical gates here that are meant to execute the operations underlying fault tolerance—logical error-corrected gates are treated later, in Chapter 8. Coding the qubit can reduce the number of required gates. A standard universal gate set choice for physical qubits are single qubit rotations and a perfect two-qubit entangler [Mak02,ZVSW03] (often a CNOT). For *logical* qubits one typically relies on the minimal set of Clifford gates and the *T* gate, a $\pi/8$ phase shift with opposite signs for its basis states.

Measurement

The qubit specific measurement capability is at least needed to read out the result of the computation. If the measurement is an ideal quantum measurement (restrictions to this are described below), it can be used for fast state preparation, e.g., for recycling qubits in quantum error correction—but this is not necessary as quantum error correction can be done only with final measurements but other overhead. In threshold calculations, a single quantum-efficiency parameter is often used to summarize the fidelity of a quantum measurement, whereas the reality is more complex. Improving the efficiency can be done by a "copy" of the single qubit to three, which is done by initializing two qubits to $|0\rangle$, applying CNOTs and measuring all of them [DiV00]. Also, perfect initialization of maximally entangled states in the form of cluster states leads to a protocol that only requires single qubit gates for computation, making measurement a resource for actual computation.

Communication-related criteria

The last two criteria play a role for communication, i.e., transmission of qubits. Requirement (7) is important for cryptography. Proposal for flying qubits usually assume photons as flying qubits, but also electrons traveling through solids. Potential candidates are described in Chapter 9 discussing nonstandard architectures. They are important if quantum processors are used as or in quantum repeaters (which are not part of this study) or in distributed quantum computing (see Section 9.2.3).

6.3 Coherence time scales

Decoherence describes the process of the loss of quantum information through interaction with an environment. Its nomenclature is not unique throughout literature. In this review, we are going to describe both decoherence and energy relaxation in a unified language and do not discriminate that the former governs the quantum-to-classical transition whereas the latter can also occur in a purely classical system—after all, both are contributing to errors of the quantum algorithm so they both are of relevance for reaching the threshold for error correction (see Section 2.4). As a first characterization of qubits that implement the circuit model in time, any of these time scales should be much longer than a typical gate time.

We assume a qubit with some capability for single qubit gates. If that does not exist yet, coherence time scales are also related to spectroscopic line widths. The latter is proportional to the decay rate of the state through spontaneous emission.

6.3.1 Single-qubit level

The nomenclature of coherence times in quantum computing has largely been adapted from nuclear magnetic resonance (NMR), where they were introduced with the Bloch equation [Lev01,VC05]. This nomenclature assumes a preferred basis set by some static energy splitting that is larger than any time-dependent controls. In most quantum computing architecture, this is also the basis in which the qubit states are encoded. A further assumption behind the Bloch equation is that errors are Markovian, i.e., the noise process does not have any temporal memory. The Markov assumption implies that terms decay exponentially, hence an error occurring over a time T_e and within a gate time T_g leads to an error $1\text{-}\exp(-T_g/T_e) = T_g/T_e + O((T_g/T_e)^2)$. Exceptions to this assumption are discussed later. Most of these rates can be estimated from the noise of the qubit environment, if known, using Fermi's golden rule [MKT+00,SW03,SHKW05].

In this framework, we identify the following time scales as being relevant:

Energy relaxation time T_1

The time T_1 describes the time of energy relaxation, i.e., bit flip errors. It is dominated by noise at the transition frequency of the qubit. Note that long T_1 can always be reached by inhibiting transitions of the qubit between its logical states (including coherent gates), hence on its own it alone is not a clear performance indicator. The standard experiments to get T_1 are inversion or saturation recovery [VC05], e.g., one prepares a non-stationary mixture of energy eigenstates and measures their decay time.

Phase coherence time T_2 and pure dephasing time T_ϕ

The time T_2 describes the time of phase randomization, i.e., the time it takes to transfer a superposition of the qubit states into a statistical mixture. This is not independent of T_1 errors and in fact it can be shown that $T_2 \leq 2T_1$ based on the constraint that the qubit density matrix remains positive. The difference as a rate (inverse time) can be identified as the pure dephasing time T_ϕ as $T_2^{-1} = (2T_1)^{-1} + T_\phi^{-1}$. The rate T_ϕ^{-1} is proportional to the low-frequency energy fluctuations of the qubit. Formally, the relevant frequency is zero, however, practically this is set by one over the duration of the experiment. Applying this argument to $1/f$-noise produces a short T_ϕ that formally diverges in a long experiment. While this formal divergence shows the limitations of this simple argument [MS04], see also our discussion in Subsection 6.3.3.2, this motivates that the impact of $1/f$ noise needs to be avoided. This can be achieved if the fluctuations do not impact qubit energy – which can be arranged, e.g., in Josephson qubits, by choosing an optimum working point [VAC+02,CW08]. T_2 can be measured by Ramsey interferometry that is corrected for homogeneous effects (see below) by some type of echo. Ramsey interferometry consists of preparing the qubit in an energy eigenstate, then performing a $\pi/2$ rotation into an equal superposition of eigenstates, waiting for a time t_r and repeat the $\pi/2$ rotation. The decay of the resulting signal shows the decay of a superposition hence directly gives T_2.

Note that while it is intuitive that T_1 limits T_2 (energy relaxation through an environment breaks the phase), the factor 2 arising above has been subject to much argument. Its existence is well established, and many experiments reach $T_2 \simeq 2T_1$ one should keep in mind that in the Bloch equations, T_2 appears twice and T_1 appears once—and that T_2 describes the decay of a probability *amplitude* whereas T_1 describes the decay of a probability.

Ensemble phase coherence time T_2^*

Measurements of T_2 for example by Ramsey interferometry require collecting data from an ensemble as they are based on expectation values. This type of ensemble averages is collected on single quantum systems by repeating the experiment in time. Now in principle, the parameters of the experiment can be slightly different between these ensemble members due to slow noise. This randomizes the phase of the average even further, hence creating the impression of a short T_2 as an artefact of the ensemble measurement. In some realizations (in spin ensembles in NMR) the ensemble is built in one temporal run but inhomogeneity between ensemble members arises because of variations of the magnetic field across the test tube. This phenomenon is also called inhomogeneous broadening (from the broadening of the Fourier transform, i.e., the spectral line below saturation).

Inhomogeneous effects can be suppressed by the spin echo technique (the NMR Hartmann-Hahn echo can be viewed as stabilization of quantum memory). Logical operations need to incorporate echo in the form of composite pulses or robust controls, which are typically longer than uncompensated pulses. Experimental designs thus decide whether the savings of going from T_2* to T_2 are overcompensated or not by the echo technique. Basic notions are described in Ref. [VC05] and its application to quantum computing is outlined in Appendix 24 in an older version of this study [WSL+20].

Rotating frame decay time $T_{1\rho}$

In many case it is useful to visualize qubits in three-dimensional affine space by plotting the expectation values of the three Pauli matrices $\sigma_{x/y/z}$ on the respective coordinate axis—the Bloch sphere. Pure qubit states are represented by points on the Bloch sphere, mixed states by points in its interior, the Bloch ball. In this representation, a basis change to a time dependent with continuously evolving phase factors can be visualized as a changing into a co-rotating frame, which is often very useful to understand and describe qubit dynamics. Specifically, most quantum computing platforms realize off-diagonal single-qubit gates by resonant external fields that are easily described by quasi-static terms in a frame rotating with that resonant field, and that drive Rabi oscillations. Moreover, based on a phenomenon called spin-locking, the relevant decoherence time for these gates is not T_2 but $T_{1\rho}$ which probes the environment at the Rabi frequency scale rather that at very low frequencies as T_ϕ would do. In particular, in systems with strong $1/f$ or other low-frequency noise this time can be much longer than T_2, hence leading to more optimistic performance estimates for these gates [VC05].

6.3.2 Properties unique to multi-qubit noise

Qubit noise metrology becomes much more complex on the multi-qubit level. The commonly used mathematical structure to describe this is the Lindblad equation (of which the Bloch equation is a special case)—a master equation that describes general strictly memoryless (Markovian) and completely positive quantum dynamics. We will describe limitations to this method below. A novel component that needs to be considered is the question whether noises are correlated across quantum bits, whether they are separate and uncorrelated between qubits, or whether they are correlated. On an operational level, correlated noise is less harmful and, in some cases, allows for decoherence-free subspaces [LW03] see also Appendix 24 in an older version of this study [WSL+20]. These are in fact a guiding principle behind the design of single-triplet and triple-dot qubits in semiconductors. On the other hand, it is known that the increase of sensitivity to uncorrelated noise is a measure of entanglement, so the effective dephasing rate of a maximally entangled N-qubit state is N-times faster than the individual dephasing rates, making uncorrelated noise a worst-case scenario. This is taken into account in fault tolerance.

Discussion of noise correlations is mostly driven by noise modeling—when the primary source of noise is known one can assess their spatial correlations. This includes knowledge that the long-range of nuclear magnetic fields makes noise in GaAs mostly correlated, the same is true for anomalous heating in ion traps—it also includes knowledge that materials-induced noise in superconducting qubits is mostly uncorrelated.

Measurements of noise correlations are rare (example given for ultra cold atoms in [Föl14]) as they would require partial process tomography, see process tomography in Section 7.4.2. Rather, given that multi-qubit operations rest on the shoulders of coherent single qubits, they are obtained by an intermediate-level characterization method, specifically can be inferred from error budgets gleaned from RB. Randomized benchmarking methods have been realized in ion traps [GMT+12, HAB+14, MKC+15], at IBM [MGJ+12], in NMR [RLL09] and in semiconductors [MLS+15]. However, it is often assumed that the correlation in noise between qubits either is small or can be ignored in fault-tolerant estimates [MGE12]. The information contained in RB will be discussed in Section 7.4.3 and the precise nature of multi-qubit errors is described in Section 7.3.2.

6.3.3 Non-Markovian effects and other caveats

6.3.3.1 General observations

As discussed above, characterization of coherence decay in terms of exponential decay and single time scales relies on a number of assumptions. The most crucial of those is the Markov assumption—the assumption that temporal correlations of the environment are short-lived. This is a central assumption behind the description of decoherence in terms of the Lindblad equation [Lin76,BP02]. At first, this appears very unreasonable, given the low temperature most qubits operate at. Low-temperature operation is not an experimental accident, it is often needed to avoid thermal noise, it is also needed to allow initialization into the ground state by thermalization. However, if done properly [WSHG06] it turns out that the environmental correlation time needs to be shorter only than the typical coherence decay time. This implies that for serious qubit candidates, where the latter is long, naturally can be described with Markovian decay pictures.

A few exceptions to this general equation observations need to be noted.

6.3.3.2 1/f noise and nuclear spin noise

Pink noise with a frequency spectrum that diverges roughly as $1/f$ at low frequency f are ubiquitous in condensed phases [VC76, DH81, Wei88, SMS02] leading to very slow correlation decay in the time domain. It turns out [ICJ+05,SMSS06] that coherence decay here is Gaussian $\propto \exp(-T^2/T_2^2)$ and still a time scale T_2 can be defined. Now note that this bounds a short-term error rate by $1 - \exp(-T^2/T_2^2) = T^2/T_2^2 + O(T^4/T_2^4)$ seeming lower. While this is established in single experimental runs, it is theoretically understood that this assumes starting from non-entangled qubit and environment and thus only applies to the first operation applied to a freshly initialized qubit.

Similarly, but with a much richer set of details, decoherence due to a nuclear spin bath in electron spin qubits (typically in GaAs) can be described. Nuclear spin baths are also intrinsically slow owing to the large nuclear mass compared to the electron mass. They cannot be described by their correlation function alone due to their localized nature and restricted spectrum. Still, their impact can be put into a time scale that can be gauged similar to T_2 [FTCL09].

6.3.3.3 Slippage and other non-Markovian effects

Another assumption of Markovian decoherence is that the initial conditions between qubit and heat bath are uncorrelated, which is rather artificial. It is known [SSO92,Wil08] that this mostly leads to short-time effects or even loss of initial visibility. These phenomena contribute to state preparation and measurement (SPAM) errors on the next higher level (see Chapter 7).

In general, the notion of non-Markovianity is lacking a standard model comparable to the Lindblad equations. Criteria to quantify it have been introduced [BLPV16] and are currently actively researched. Generally, these effects are subtle and occur only if they are not masked by Markovian effects, hence, systems that are affected by this type of non-Markovian decoherence can be analyzed with RB, the key tool on the next level.

6.3.4 Catastrophic events and noise of the noise

In the context of fault tolerant quantum computing, “catastrophic events” consist of highly correlated errors across a whole quantum processor, that quantum error correction cannot catch (and rather reinforces), even though this can be possible if the events are sharply localized in time [TPM+24]. For any system that has met the criteria of level B, i.e., shows generally low error rates and can execute small quantum algorithms, these catastrophic events are rare and not taken into account in the initial engineering of the system, i.e., they are hard to predict. This means that there is a risk that newly discovered catastrophic events may slow down the development of scalable quantum computers or even present showstoppers.

In the well-documented error budget of superconducting qubits, it seemed for a long time [AAA+22] that these catastrophic events (bursts of ionizing radiation) were a showstopper to even reach break-even in quantum error correction, i.e., complete level C. The new experiment [AAA+22Goo+24] has shown that this can be overcome by careful device engineering, leading to the detection of a much rarer and weaker new catastrophic error mechanism of so far unknown origin.

6.4 Qubit definition indicators

So far, we have assumed that the noise parameters themselves are constant over time as the operation of a quantum computer persists. In the most mature settings, this is not necessarily the case. Specifically, in superconducting qubits, the noise timescales themselves are not stable [BBS+19] and there are rare catastrophic events that affect the processor as a whole. For the former, one is advised to quote a conservative estimate of coherence time while the latter is only uncovered in higher levels of our classification scheme.
An example of such catastrophic event would be the incidence of cosmic rays onto a superconducting qubit, which allows the generation of quasiparticles in superconductors [SSD08]. Quasiparticle tunneling through Josephson junctions can then cause correlated errors due to the stimulated decay of the qubit’s quantum state [LGL05].
Error mitigation of rare environmental events is both important for long time coherence, as well as to prevent stochastic errors which are ill-treated by usual noise reduction procedures.

6.4.1 Qubit longevity

For some platforms, the qubits themselves may be short-lived, primarily in neutral atoms where trapping forces are weak, even though this problem has recently been reduced [SSN+21].

6.4.2 Leakage

Mathematical qubits—systems that can be completely described as two-state quantum systems, do not exist in nature, not even as elementary particles [WL02]. Typically, the computational states are either one degree of freedom of an elementary particle (e.g. the spin-1/2 of a proton in NMR, which also possesses motional degrees of freedom) or they are taken as low-energy states of a more complex energy spectrum (e.g. in ions or Josephson circuits). In order to still operate these devices as qubits, one needs to guarantee that the state returns to the computational subspace (CSS) after operations (whereas non-computational states can in fact be useful in gate operations or for readout). Deviations from this are referred to as leakage. Leakage errors are particularly difficult to correct. In some platforms, leakage is not a problem—specifically when non-computational states are far separated in energy from computational states. Nuclear motion in molecules, for example, has frequencies in the infrared range whereas spin dynamics is between radio frequency and the low end of the microwave spectrum. In some platforms, most notably Josephson

qubits, leakage is an ever-present challenge as the energy splitting between qubit states differs from that to the leakage levels by typically only 10–20% in the transmon.

A first indicator for leakage resistance is the difference between such energy splittings. If they are critical, one can rely on a sophisticated array of detection techniques: Leakage measurement by IBM [WG17] introduces two new criteria, the leakage rate L_1 describing leakage from the computational states to other states, and the seepage rate L_2, population transfer from other states to computational subspace. The latter rate introduces memory effects to the system.

6.5 Qubit initialization indicators

If qubit initialization is done by cooling in the ground state, one can upper-bound its population by 1 – exp(-$\Delta E/k_B T$) where ΔE is the energy gap to the first excited state and k_B is the Boltzmann constant. In initialization by measurement, the maximum initialization fidelity is limited by the projection fidelity of the measurement and the fidelity of the gate that needs to be applied to correct the measurement if necessary [RvLK+12, RBLD12]. In initialization via optical pumping [Saf16] a high contrast of rates is required for good initialization.

A posteriori, initialization can be measured by measuring right after initialization. As measurement is typically more restricted than initialization, this is not often done.

6.6 Readout indicators

Readout is a crucial part of quantum computers (and of quantum physics). It does not only serve the final analysis of the outcomes of the algorithms but is pivotal in syndrome extraction for quantum error correction and thus an important ingredient of threshold calculations. Also, readout can influence architecture decisions, e.g., when readout is slow, one would like to avoid mid-circuit measurements

Quantum measurement is probably one of the most intriguing parts of quantum physics leading to a lot of foundational arguments. Also, quantum measurement science is related to precision quantum-limited measurement—a lot of modern quantum measurement science and engineering has for example been originally driven by the application of gravitational wave detection[CDG+10, BSV01, DK12, BBV+16]. We will only touch upon these two related tangents in a minimal way, to the extent that they are relevant to qubit measurement—for example because of some critical element in the overall measurement chain.

The key parameters of readout within a quantum processor architecture are:

- Readout contrast – i.e., the difference of detecting 1 when then qubit is in state |1> minus the probability of detecting 1 when the qubit is in state |0>. This characterizes misdetections which more completely can be put into the aptly-named *confusion matrix* . Low contrast can hinder quantum error correction
- Quantum-Nondestructiveness – measures by the probability that after the measurement the qubit is found in the state that it has been detected in, i.e., the proximity of the measurement process to an ideal, textbook quantum measurement. This is in particular important, if the post-measurement state is re-used in the algorithm as it the case, e.g., in quantum error correction
- Measurement crosstalk – the dependence of the measurement result on the state of neighboring qubits. This is again crucial for quantum error detection, where during syndrome readout it is crucial to not detect the data qubits
- Measurement time – detectors are typically made from a technology different from that of the qubits and operate on a different timescale. An exceedingly slow measurement, much longer than the time for gates, slows down NISQ calculations but, more crucially, is inefficient for mid-circuit measurements in quantum error correction

While the problem of characterizing a binary outcome detector has been completely described in [KOR08], as was outlined in earlier versions of this study, we identified that the current version focuses on the relevant information and takes scalability into account.

6.7 Final remarks

This low-key application of DiVincenzo's criteria is the first qualifier for quantum computing platforms. Passing them with structures containing at least a few qubits will enable a more quantitative performance discussion as that done in the next section, which essentially proposes small quantum algorithms that allow to extract quantitative performance indicators.

7 Benchmarking qubits

7.1 Introduction

When we have qubits that show basic functionality in the sense of the DiVincenzo criteria, we would like to know if they have the potential to be scalable, i.e., if they meet the threshold for quantum error correction. The question is if a device is given to us how to know if the threshold has been surpassed. This is nontrivial because one needs to know which measure returns the threshold. While the low-level criteria can give bounds on achievable errors, they crucially depend on very complex models to be accurate and complete – models that address human-made systems and hence would need to be re-evaluated over and over. Thus, to validate qubits and refine these models, it is important to have a way to measure the error of quantum operations on a real qubit. Next to evaluating the distance to the error correction threshold, this type of characterization also helps to improve quantum processor elements and assists in calibration of operations.

7.2 Benchmarking and error mitigation techniques

Benchmarking can be used to evaluate low-level gate design and error mitigation techniques. Specifically, dynamical decoupling and spin echo as described in Chapter 9 and Chapter 6 can be used to remove systematic errors and inhomogeneities, but they add complexity and in general longer gate times. On the other hand, decoherence-free subspaces (DFS, see Appendix 24 in an older version of this study [WSL+20]) use symmetries of the noise mechanism to protect qubit states and their effectiveness influences gate fidelities that can be benchmarked.

7.3 Qualitative criteria beyond DiVincenzo

A lot of the background on error correction has already been covered in Section 8.2.2, which discusses the surface code.

7.3.1 Connectivity

Error correction codes need the right connectivity of physical qubits to carry out operations, e.g., a nearest-neighbor lattice for the 2D surface code. A 1D-architecture with nearest neighbor-connectivity needs to face extremely low thresholds—full connectivity such as, e.g., in ion traps [LMR+17] allows to implement surface codes of high dimension with high thresholds.

7.3.2 Parallel operations

Error correction is envisaged to be done in parallel or with at most constant overhead on all qubits. Sequential error correction cycles would render error correction ineffective. An example of a non-parallelizable architecture is coupling all qubits to a single bus, which can typically only mediate a single two-qubit operation.

7.3.3 Supply of fresh qubits

Fresh initialized ancillae in error correction are needed in all cycles, requiring either a large supply or fast reset. Time for this needs to be factored into the determination of time constants for error correction.

7.4 Benchmarking operations

7.4.1 Gate fidelities

There exist a wealth of fidelity functions allowing to estimate the proximity of two quantum operations. In its simplest form, the fidelity can be written as a state overlap $\langle\psi_F|\psi_T\rangle$ between a desired state $|\psi_F\rangle$ and the final state $|\psi_T\rangle$. The final state is obtained by applying some operation on the prepared input state $|\psi_0\rangle$, and the desired state is the one we would get if the operation on the input state would be ideal. This state overlap basically defines the fidelity of the quantum process, but it depends on the given input state, leading to a large range of obtainable fidelities.

There are two natural routes to lift this input state-dependence: One is to average over all input states $|\psi_0\rangle$. Such an average can be reduced to the Hilbert-Schmidt scalar product of the two corresponding operators, like the trace fidelity $|\mathrm{tr}(U_F^\dagger U_T)|^2/N^2$ for a unitary process with the desired evolution U_F and the implemented evolution U_T. This can be extended for general maps, to a trace fidelity $|\mathrm{tr}(\Phi_F^{-1} \circ \Phi_T)|/N^2$, where $\Phi(\rho_0) = \rho$ maps density matrices onto density matrices, and the indices stand for desired (F) and actual (T) gates. The average gate fidelity is yet another way to measure the fidelity of a process and is defined through

$$F_g = \int \langle\psi|U_F^\dagger \Phi_T(|\psi\rangle\langle\psi|) U_F|\psi\rangle \, d\psi.$$

The integration is done over all possible input states $|\psi\rangle$ in the computational subspace. We will see in the end of this section that the average gate fidelity can be estimated efficiently through RB. However, for high dimensional gates, like an n-qubit controlled-phase gate $C\ldots CZ$, i.e., a lot of control qubits to perform a Z gate, leads to a high fidelity even for the identity operation. The other way is to look at the worst input state—the one producing the largest error. That combined with the possibility to augment the operation with a unit operation (hence finding the worst input state over a large set) defines the diamond norm. This measure depends on an input state that is defined through the norm itself. The diamond distance of two quantum channels Φ_1 and Φ_2 is defined as the trace distance of the channels for the worst-case input state ρ

$$\|\Phi_1 - \Phi_2\|_D = \sup_\rho \|(\Phi_1 \otimes 1)(\rho) - (\Phi_2 \otimes 1)(\rho)\|_1.$$

Then the diamond norm is 1 minus the diamond distance. The diamond norm measures the fidelity of the worst case possible, which maximizes the diamond distance. The diamond norm returns a significant error for this wrong implementation of the n-qubit controlled-phase gate $C\ldots CZ$.

It is the diamond norm that enters the threshold theorem of fault tolerance [AB099]. We will see that it is cumbersome and inefficient to measure, so one needs to rely on bounding it by feasible measurements. This statement will be made more formal later.

7.4.2 Process tomography—idea and pitfalls

The historic first benchmarking procedure proposed has been quantum process tomography (QPT), which is based on quantum state tomography (QST) [NC00]. QPT aims at reconstructing the full quantum process, from which operation errors and fidelities can be computed (for a caveat see next subsection). The goal of QST is to reconstruct the full density matrix of a state through measurement. For a system of qubits, it consists of measuring the expectation values of all combinations of Pauli matrices, including the identity, in a given state. Quantum state tomography is a procedure to measure the complete density matrix. For a system of qubits, it consists of measuring the expectation values of all combinations of Pauli matrices (including the identity) in a given state. It thus requires a number of measurement operators that is exponential in the number of qubits. Practically, in most cases with the possible exception of photon polarization, physical detectors are set up to measure only one specific observable. Measuring any other Pauli operator requires additional operations between the operation of interest and measurement, introducing an additional error source. Practically, measurement imperfections can easily lead to non-physical density matrices (e.g., with negative eigenvalues), which can be mitigated by advanced data analysis, need to be determined through many repeated experiments for each generalized Pauli operator,

then the Pauli decomposition of the state ρ can approximately be reconstructed. Although it is conceptually easy, it needs accurate state preparation and measurement (SPAM), during which it is prone to errors. These errors are called SPAM errors.

Quantum process tomography (QPT) consists of preparing a complete set of pure initial states spanning the space of input density matrices, which is of size d^2. Applying the process $\epsilon(\rho)$ for each initial states and performing full QST on the output [NC00] determines the full quantum process. This increases the needed resources by a factor of d^2 Given that in quantum processors there is usually a single fiducial initial state, QPT is as well prone to SPAM errors. One should note that for small systems, it can still be practical to implement QPT in efficient versions [MGS+13].

7.4.3 Randomized benchmarking and interleaved randomized benchmarking

QST and QPT need a lot of resources to characterize even small quantum systems. Additionally, they require accurate state preparation and measurement (SPAM), and are vulnerable to errors in these. An efficient way to estimate quantum gates is RB [KLR+08]. It does not need that many measurements and is stable under SPAM errors. Therefore, it is good candidate for characterization of large systems and the de facto standard tool for such a task.

The basic RB protocol works as follows: First, one chooses a fixed sequence length m, where a sequence contains m+1 Clifford gates. The Clifford gates form the Clifford group and are the normalizers of the Pauli group: They map Pauli operators onto Pauli operators. The generators of the Clifford group are the phase gate, the Hadamard gate and the CNOT gate. The last gate in a sequence is set as the inverse of the concatenated preceding m gates, which is feasible given the group structure. For the chosen m, one builds K_m random sequences, each with an error Λ, and calculates the average of the K_m fidelities, which are the measured survival probabilities of the initial state. This is repeated for each m and fitted to an exponential decay curve. Its offset is interpreted as the total SPAM error and from its base p we can infer 1-p as the error per gate. The average error rate is then given by $r = (d- 1)(1 -p)/d$ with the dimension d. RB approximates the average fidelity function. Various initial assumptions have been relaxed [MGE11, MGE12]. Note that this technique allows to measure even small errors by making the sequence very long in order to bring the sequence error into a range that can be conveniently detected. Its convergence is rather fast, which has later been quantified [CW15].

As described, RB measures the average error of the whole Clifford group. Interleaved randomized benchmarking (IRB) [MGJ+12] allows characterization of a specific Clifford gate by comparing a regular RB sequence with one where the gate in question is interleaved between two sequential Clifford gates. RB has been implemented in many systems, and typically requires a modest number of measurements mostly controlled by the sheer size of the two-qubit Clifford group. It is also possible to characterize leakage errors with RB separately and several protocols have been proposed [ECMG14, CW15, WG17] to do it. However, T gates cannot be benchmarked efficiently, which is a consequence of the Gottesman-Knill theorem [Got98], that states that non-Clifford gates are computationally hard to simulate classically. There are some attempts to include non-Clifford gates, or at least trying to reduce complexity by forgoing the last inverting Clifford gate and performing optimized state tomography instead [CMB+16, CRKW17]. Another proposed idea is Randomized Benchmarking Tomography (RBT) [JdSR+15]. The protocol is compared to IRB, where non-Clifford gates for RB are written as linear decomposition of Cliffords [KdSR+14], and the latter are benchmarked with IRB. For characterization at the logical level the idea of logical RB [CGFF17] has been proposed recently.

It needs to be noted that the difficulty of characterizing non-Clifford gates with RB is not considered to be a major problem. The physical T gate is not more difficult than the Z gate, which is a Clifford gate and one should not expect these errors to be vastly different. This is in sharp contrast to their difference in complexity as *logical* gates.
For larger systems, a variation called cycle benchmarking gets some more reliable information as it can clarify error sources on the level of Pauli errors, including crosstalk [EWP+19].

7.4.4 Gate set tomography

A complementary tomography tools to characterize qubits is gate set tomography (GST) [BKGN+13, MGS+13]. It is designed as a black-box characterization tool, such that the quantum device is accessible only through classical controls and measurement outcomes. In contrast to QST and QPT, it does not rely on accurate state preparation and measurement. Compared to RB, it needs much more resources: about 10^3 sequences for a single-qubit and 10^5 sequences for two-qubits. But it returns full tomography of gates, state preparation and measurement simultaneously, and an estimate of the diamond norm. GST has been successfully tested, for example in ion traps [BKGN+13, BKGN+17] and semiconductors [DMBK+16]. A Python implementation of GST (pyGSTi) can be found on GitHub [NER16].

In the black-box description the device contains some buttons to apply quantum gates, including an initialization button to prepare the (probably unknown) state ρ, a measurement button that returns a binary outcome, and K gates G_i. GST then works as follows: The state ρ is initialized, followed by a sequence of gates $s = \{G_{s1},...,G_{sL}\}$ with length L, and a final positive-operator valued measurement (POVM) E. Each such experiment is repeated N times to gather sufficient statistics of the recorded outcome, and this is done for M different sequences. The number M scales with Kd^4, where d is the Hilbert space dimension and K the number of gates one can apply directly (i.e., the number of gate buttons). Then linear inversion provides rough estimates of the gates, state preparation and measurement (simultaneous state and process tomography)[Gre15], and is used as a starting point for maximum likelihood estimation (MLE). Each sequence consists of three parts: an initial fiducial sequence, a short germ sequence which is repeated several times, and a final fiducial sequence [BKGN+17]. The fiducial sequences effectively change the initial state and the measurement basis. Repeating the germs allows to enhance specific errors, such as over-rotation, tilt or dephasing. GST is therefore more sensitive to coherent errors compared to RB, which randomizes over gates. GST assumes that the gates are Markovian and non-Markovianity is obtained from deviations in the fitting model, where short sequences are less prone to non-Markovianity. Up to the choice of basis (gauge) the gate set $\{\rho,E,G_i\}$ is self-consistently determined. A consequence of the gauge invariance is that the gates do not have to be completely positive and trace preserving (CPTP) maps in an arbitrary basis. Therefore, GST does not enforce the CPTP condition, and the gauge is usually chosen such that the estimated gates are as close as possible to the target gates.

7.4.5 Cross-entropy benchmarking (XEB)

Cross-entropy benchmarking has been introduced by the Google group [AAM+19] as a means to benchmark large quantum processors as a whole rather than individual components or gates, and to be able to naturally include non-Clifford gates. Such an undertaking needs to make sure that the benchmarking operations are representative for hard tasks given to the quantum hardware as they scale, and that classical simulation of a large quantum computer is not required or at least kept to a minimum.

These constraints are implemented by using a sampling problem as a synthetic benchmark, i.e., by running a quantum algorithm that does not have a unique result but rather a distribution from which measurements are sampled. If those distributions have both a quantum and a classical limit, then comparing the output distribution of the circuit to both these distributions through their cross-entropy, a well-known model testing method, allows to determine if the device is still a quantum processor.

In the case of the work [AAM+19], the implemented algorithm is a random set of gates. It is shown that the output distribution of that set of gates is described by the Porter-Thomas distribution, a notion from the field of quantum chaos (i.e., the quantum physics of classically chaotic systems). Its classical counterpart would be a uniform distribution of output values and it is argued that simulating the system on a classical computer with a polynomial-time algorithm needs to take shortcuts equivalent to reaching only that distribution. It is in fact shown that simulating quantum chaos of this type is computationally equivalent to problems in NP.

In this sense, cross-entropy benchmarking is suitable to its mission in that it allows to benchmark large quantum processors by certifying that they are quantum. It certainly also gives insights into error rates even though these are currently under debate. It is not a (societally motivated) application of a quantum

computer – in this sense XEB is a purely synthetic benchmark –, nor is it a replacement for the benchmarking methods (RB, IRB, GST).

7.4.6 Risks at mid-level

The average gate fidelity measures how well a channel Φ performs a desired unitary gate U, averaged over all pure input states $|\psi\rangle$ in the computational subspace. But as we have already seen, there exist gates with bad implementation but high average fidelity. The average error per Clifford gate, defined as $r = 1-F_g$ [MGE12], is not a measure for scalability [SWS16]. For example, the average gate fidelity underestimates unitary errors compared to the diamond norm. The proper threshold is defined through the diamond norm, but the latter lacks an efficient estimation like RB gives for the average error per gate. The question arises how useful the concept of the average error is. In [SWS16], an upper bound η^{ub} is given derived from r and the Hilbert space dimension d, such that the following condition holds if errors can be efficiently corrected,

$$\eta \leq \eta^{ub} < \eta^{lb} \leq \eta_0 ,$$

with the threshold η_0 for FTQC, the error rate of the device η, and η^{lb} the lower bound error rate. Furthermore, it is not completely clear if RB really estimates the average gate fidelity, since there are some problems with the gauge invariance [PRY+17]. It is currently debated whether cases where diamond norm and average fidelity vastly differ are practically relevant or pathological. While no example of the former has been found, it turns out that fidelities measured by GST are typically slightly lower than those obtained by RB.

Another point of concern is the Pauli twirling approximation (PTA) [GZ13] of arbitrary channels Λ. Given a map which reads $\Lambda(\rho) = \sum_i E_i \rho E_i^\dagger$, Pauli twirling (also full Clifford) takes the input state ρ, rotates it by a Pauli operator σ_i, applies the map Λ, and finally counter rotates the final state. The approximation is then performed by taking the average over all Pauli (Clifford) matrices, which can be cast into the form $\tilde{\Lambda}(\rho) = \sum_{\sigma i} p_{\sigma i} \sigma_i \rho \sigma_i$. The Pauli-twirl of any channel is mapped onto a Pauli channel, Pauli channels are mapped onto themselves, and the channel Λ and its Pauli twirl $\tilde{\Lambda}$ have the same average gate fidelity. Since Clifford twirling of a quantum operation leads to a depolarizing channel [MGE12], RB can effectively use a fit model for the depolarization parameter p to estimate the average error per gate. However, for coherent errors the Pauli twirling is in general not sufficient [GSVB13] and one has to take into account the difference between a coherent error and its Pauli twirl for threshold calculations (Pauli distance) [SWS16].

A currently investigated error in RB is the role of errors that error correction does not catch [WF14a], such as extreme non-Markovian or highly correlated errors. These will all affect the RB result but are difficult to treat with error correction, hence the impact of error correction may be lower than the estimates of the next chapter predict if the physical error rate is estimated with RB.

7.4.7 Recommendation

This intermediate state is where most of the work of building scalable quantum processors is currently performed. It allows for predicting what a fault tolerance implementation would do. It should be applied as follows:

1. Verify if one- and two-qubit RB experiments have been done. Do they find error rates that are below the fault tolerance threshold for the envisaged error correction code?
2. If the first step has been met, verify whether the error rates have been at least in a sample verified by another method—modern process tomography or gate set tomography and whether the results from these methods still allow for fault tolerance. Monitor the impact of a subsequent error correction experiment (for first implementations, see [WL17, SBM+11, KBF+15,ARL+17]). If it is not as effective as expected, this points to temporally or spatially correlated errors.

7.5 Quantum supremacy experiments as indicators of component benchmarking

The Google group [AAM+19] has published a highly celebrated experiment claiming quantum supremacy, i.e., the execution of a computational problem that would be impractically long on a classical computer given its restrictions. Other groups [WBC+21, ZWD+20, MLA+22] have followed. In the context of this study, these should be interpreted as system-wide technical benchmarks as they study artificial benchmarking problems that test the whole system, including but not restricted to its components. They allow conclusions for the more advanced benchmarking levels but do not replace them. In a way, they are precursors to testing NISQ algorithms.

For Google and the quantitative improved experiment [WBC+21] the problem studied as laid out in [BIS+16] is the creation of a Porter-Thomas output distribution from a random quantum circuit, which is characteristic of quantum chaos, and then sampling from it. The classical simulation of this problem is claimed to take around 10000 years on the currently largest supercomputers in the world largely because of a memory wall. It has been argued [PGMG19] that by more compact memory use that time could be brought down significantly. Yet, it has not been disputed that enlarging the processor would double the classical memory per added qubit. The algorithm was executed without error correction and the quantumness of the output was verified with cross-entropy benchmarking (XEB), i.e., it was verified that the error rate was low enough so this is a bona fide quantum computation.

This experiment defines a best-in-class benchmark on processor size, gate fidelity and speed. Its architecture is a square two-dimensional array as required by fault tolerance using the surface code. One may still ponder whether executing a purely synthetic benchmark such as XEB is a valid milestone for quantum supremacy. On the one hand, this is a freely programmable, universal quantum processor, so it could execute other tasks that follow a purpose other than pure benchmarking within the NISQ domain. As we argue in Chapter 2, there is no clear NISQ roadmap in cryptanalysis, so we cannot draw further conclusions, but need to continue to watch.

Quantum supremacy demonstrations based on Gaussian boson sampling [MLA+22, ZWD+20] should be seen in the same way – they are a valid benchmark of component and above that system performance, with the main caveat that the translation into cryptanalytic performance is even less clear.

8 Quantum error correction

This chapter gives an overview of the criteria that need to be fulfilled to perform quantum error correction to a set of qubits, and on the improvement of logical error rates that can be reached this way. While there are many different error correction codes, we largely focus on the well-known surface code [BK98]. We discuss the promising investigation of error correction codes with qualitatively better properties (see Section 8.2.5), however, those codes are currently in a premature state, so that the surface code still counts as one of the best codes known to date. This is due to its high error threshold and, in general, low operational demands, such as assuming only nearest neighbor connectivity on a two-dimensional array of qubits (which makes it applicable to virtually all quantum computing systems), and a small required gate set.

In the proposal by Kitaev [Kit97a,Kit97c,Kit03] the physical qubits are arranged on the surface of a torus, which corresponds to a surface with periodic boundaries. This is for many quantum computing platforms a nontrivial arrangement. However, it was realized that the surface code works efficiently with nearest-neighbor interactions on a two-dimensional square lattice with also non-periodic boundaries. Several other quantum error correcting schemes of interest, such as the color code or topological cluster states, are discussed briefly in Section 8.2.4. Some of these codes provide additional correcting possibilities, but often come with higher requirements to the physical implementation.

A previous version of this study contains a formalism for estimating the total space-time volume that is required for carrying out fault-tolerant quantum computations depending on the quantum computer's error rate [WSL+20] (Section 7.5 therein). This formalism is based on the surface code, and it was used to compare the resources (number of qubits and time) required for computing two cryptographically relevant functions, the discrete logarithm and prime factorization. While the results of this calculation still portray the large gap between current physical devices and the necessary capabilities for carrying out certain meaningful computations (as illustrated, for example, in Fig. 21.1 of [WSL+20]), we note that in the meantime various error-correction improvements have been put forth, which render that formalism obsolete in parts and thus not suitable for further inclusion.

With the aim to assist understanding the rather specialized language of quantum error correction, we have added a glossary of terms at the end of this chapter, Section 8.7.

8.1 General observations on the role of fault tolerance

Albeit accepting and producing regular binary output, quantum computers store intermediate information in the probability amplitudes of complex quantum states, which are analogue quantities. While these analogue quantities are not read out in a running quantum computer, which, as in Shor’s algorithm, only has binary input and output, they do matter as they provide probabilities for algorithmic errors. It thus appears imperative to correct potential output errors which, in practice, means reducing the probability of a wrong output to a fixed, acceptable value. The number of distinct probability amplitudes is exponential in the number of qubits, which by itself opens a multitude of possibilities for errors in computation.

One way to prevent these errors would be to completely isolate the qubits, which, however, would not allow for carrying out computations. One therefore necessarily opens the quantum processor to error channels. As described earlier, achievable error rates are generally expected to be vastly overcome by the demands of cryptographically relevant algorithms. Potential cryptanalytic applications of quantum computers discussed under the heading of the noisy intermediate scale quantum (NISQ) era [Pre18] are discussed above in Chapter 5. For those algorithms it is, at this stage, difficult to make predictions with high certainty regarding the required resources for the solution of relevant problem instances.

For computations beyond the NISQ era, quantum error correction allows to use error-prone hardware to efficiently simulate a perfect quantum computer with a predefined precision, i.e., its goal is to reduce the error of the result to a predefined value. Hence, generally not all errors are corrected, and fault tolerantly implemented algorithms are to some degree stochastic.

Before describing the current gold standard of quantum error correction and its applications as an evaluation tool for quantum computers, we start with a few basic clarifying observations and terminology.

8.1.1 Redundancy and measurement

Similar to classical error correction, quantum error correction is based on redundant information encoding: A single logical qubit (a qubit in which the fault-tolerant algorithms on higher levels are expressed) is encoded into multiple *physical* qubits. Information about errors is extracted by *syndrome measurements.* Given the intrinsic invasiveness of quantum measurements, this cannot be done by reading out all qubits first and then classically comparing the outcomes, rather, the syndrome information needs to be mapped by a small piece of algorithm onto an ancillary degree of freedom, which is then read out, revealing only syndrome information but not the logical state. The projective nature of the quantum measurement turns analog error amplitudes into probabilities for digital errors and given that the ancilla is entangled with the data qubits also guarantees that their state is projected into a state described by these syndromes. In other words, it is syndrome detection that translates analog errors into digital errors with a probability given by the analog amplitudes, allowing to handle the errors digitally – the projective nature of the measurement performs a test and replaces probability by certainty. It turns out that these resulting digital errors can be completely described by bit-flips and phase flips and arbitrary combinations thereof (Pauli errors). This also applies to over- and under-rotation errors (see Section 6.2) where the error probabilities can be calculated from the imprecise rotations according to Born's rule, with a number of caveats described in Section 7.4.1 in an older version of this study [WSL+20]. This is often stated but not exemplified in literature, hence we provided a simple example and contrast in [WSL+20], see Appendix 22 therein.

This is referred to as a *parity measurement* and the operators being measured are products of an even number (the *weight*) of single-qubit operators which have (degenerate) eigenvalues ±1 . In fact, in effectively characterizing quantum error correction one tends to describe quantum states not by their state vector, but by their set of *stabilizers*: A set of commuting operators that uniquely define the state up to a global phase by requiring it to be a +1 eigenstate of all of them.

8.1.2 Error detection, matching, and correction

An error correcting code is characterized by the number and type of (physical) errors it can handle, with larger codes being in general more powerful. After measurement of the (physical) syndrome operators, it is important to link the syndrome pattern to the errors that have happened. In simple majority-voting this is straightforward, but in complex codes this is difficult and requires complex minimum-weight matching algorithms [Edm65](see Section 15.1.4). Research on these *decoders*, pieces of software that extract error syndromes and evaluate the most likely error pattern and corrective action to these patterns. We are not detailing the process of error decoders per se but of general error correction methods and their stacks, i.e., subsystems of an error corrected quantum computing system, not its components.

Once errors are identified, conventional wisdom suggests that corrective action needs to be applied—i.e., gates that correct the error. Experimentally, this requires feed-forward, i.e., conditional application of gates within the time scale of the algorithm. This is enormously challenging—but not always necessary. As all the errors, after syndrome detection, are all Pauli gates[6] (hence form a subgroup of the Clifford group), their effect can be simulated classically with polynomial computational effort, so it is sufficient [Got98] to implement corrections on the final results of the quantum computation. This can be done completely after the quantum computation, as a correction to the classical output bit-string.

What this procedure still requires are initialized ancilla states after each round of error detection, placing a stringent requirement on speed and fidelity measurement.

8.1.3 Concatenated codes and the threshold theorem

There are various ways to enlarge the error correction code and correct more errors. A standard and illustrative way is that of *concatenated codes:* Build first-level logical qubits out of physical qubits and repeat this construction iteratively, so that qubits of level *n* are built from qubits of level *n*-1.

[6]In principle, any error can happen to the qubits, but the syndrome measurements are always chosen such that errors are mapped to Pauli (or identity) operators. This can be done by measuring only in Pauli-eigenbases.

Note that implementing error correction in such a way introduces more qubits as well as extra operations, both increasing the number of entry points for physical errors. This gives rise to the question whether error correction is beneficial, or whether the additional operations negate the improvement from error correction. This question is answered by the *threshold theorem* [ABO99], which exists in various versions. It states that there is a threshold error rate for the physical error of a real quantum computer, below which an ideal quantum computer can be realized with arbitrary precision using error correction. Practically, this means that below threshold the logical error rate (measured by the diamond norm, see Section 7.4.1) can be arbitrarily reduced (hence the size of an executable algorithm can be arbitrarily prolonged at fixed final logical error rate) by adding more and more error correction (e.g., in the form of more concatenation).

To compute thresholds, one needs to analyze each step of an error correction procedure on a given architecture. One designates analytically proven and numerically simulated thresholds, the latter being more generous. Architectural features that need to be discussed include, for example, the connectivity (expressed by range of interactions and the dimensionality of the processor), which determines swapping overheads.. Proofs of the threshold theorem assume errors that are uncorrelated between qubits. This is a crucial ingredient – a logical qubit will be exposed to errors when all its components experience errors at the same time, thus it is only affected if these simultaneous errors are less likely than individual errors. The precise definition of multi-qubit errors and the likelihood of them to occur are studied in Appendix 22 of [WSL+20]. The numerical value of the threshold contains the trade-off between the extra operations required for fault tolerance—which are all in themselves assumed to be imperfect—and the protection offered by error correction. Existence of a threshold thus requires code to be efficient enough for the extra operations to not eat up the protection.

8.1.4 Fault tolerant computation

Error correction narrowly defined talks about stabilizing quantum memory. In order to perform an effective fault-tolerant quantum computation, one needs to be able to implement a complete set of gates between *logical* qubits. The simplest way to do that—decode the logical qubits, operate on the vulnerable physical qubits—recode into logical qubits, would undo most of the benefit of error correction, eliminate the threshold, and is hence not viable. Rather, one would like to perform logic operations on the encoded qubits, so called transversal gates. These gates are usually performed by modifying the syndrome measurement cycles. This does not necessarily need the application of any additional gates in between the measurement cycle and therefore does not increase the time between two cycles. If additional gates are needed, the number of gates between two syndrome measurement rounds is kept very low in order to not increase the possibility for errors before the next round too much. For an optimal two-dimensional quantum error correction code, the set of transversal gates is the full Clifford group. Now given the Gottesman-Knill theorem, Clifford-only quantum algorithms can be efficiently simulated classically, so this is not sufficient. The most popular non-Clifford gate is the T gate or $\pi/8$ gate, a phase shift of the $|1\rangle$ state by $\pi/4$ relative to the $|0\rangle$ state. The Solovay-Kitaev theorem [Sol00, Kit97b] along with its practical constructions [HRC02] guarantees that with Clifford+T one can efficiently approximate any unitary gate, including small rotations needed in phase estimations. Implementing this efficiently is a major practical challenge in fault tolerance [BK13], as it is not always possible to perform it on logical qubits without turning off the protection. Note that these statements all apply to *logical* gates and would not be true for *physical* gates. Usually, additional resource-demanding codes like magic state distillation (see Section 15.3.3) and classical feed-forward are necessary on top of the surface code to perform logical T gates with the same accuracy as Clifford gates.

8.1.5 Conclusions for the evaluation system

The requirement of fault tolerance makes this a crucial connecting point between algorithmic research and hardware implementations in quantum computing:

1. Given that all cryptographically relevant algorithms are too long to be executed in a non-fault-tolerant way, gate counts in quantum algorithms need to be understood as fault-tolerant gates. They should be given in Clifford+T counts. Consequently, gate times and number of qubits required correspond to logical gate times and number of logical qubits.

2. Hardware needs to meet the requirements of fault tolerance. It requires a precise method to evaluate the error rate to establish a relation to the threshold. Also, for a threshold calculation to be viable, the architecture needs to meet all the requirements of the threshold calculation, specifically the required connectivity of qubits and fast ancilla initialization. As one needs to accept that most of the quantum computer's effort goes into error correction, this is thus a driver for architecture.
3. Careful investigation of the efficiency of error correction below threshold provides an efficient and effective scheme to translate logical qubit requirements into physical qubit requirements. We provided concrete formulae in Section 7.4 in an earlier version of this study [WSL+20].

The fault tolerance landscape is currently dominated by the surface code, which is the first code that makes full machine-level extrapolations possible. We will thus detail fault tolerance along this example and make it quantitative. We will remark on other codes in the end. In the Appendix, Chapter 15 gives a pedagogical and rather extensive introduction to the surface code and its underlying mechanisms. The parts directly relevant for the assessment of a physical platform are the basic requirements stated in Section 8.3 and the operational conclusions in Section 7.4 in [WSL+20]. Section 8.4 discusses the performance of the surface code in more detail concerning the underlying error model, trade-offs, and different experimental conditions.

Quantum error correction is a large and forward-looking theoretical and mathematical activity that necessarily makes assumptions about the physical world. Also, implementing the far-reaching ideas of this chapter is beyond the current status of experimentation. Still, small instances of error correction have been experimentally verified. These experimental implementations [WL17, SBM+11, KBF+15,ARL+17] confirm some basic assumptions yet call for refinement of error correction models. Two very specific experiments are described in Appendix 22 of the old version of this study [WSL+20].

8.2 Quantum error correction codes

In classical computing, errors occur much more rarely than in a quantum computer. Yet, many kinds of classical error correcting codes have been developed and are in use. Similarly, there are many different quantum error correcting codes, whose applicability depends on various factors, such as the code's ability to save data efficiently and to protect against errors, or the specifications of the used hardware. In this section, we list several well-established quantum error correction codes. Further error correction codes for another type of computation, quantum computation with continuous variables, are discussed in Sec. 9.3.

8.2.1 Notation

Before we start our description of error correction codes, we introduce a type of regularly used notation for describing codes. A generic quantum error correcting code, like its classical counterpart, can be characterized by three central parameters: the number n of used physical qubits, the number k of encoded logical qubits, and the code distance d. As noted above, for a given distance d a total of $(d-1)/2$ errors can be detected and corrected in a single error correction cycle. Similar to classical codes, whose default notation is $[n, k, d]$, we use the equivalent notation

$$[[n, k, d]]$$

for a quantum code.

8.2.2 Surface code

The surface code is currently the leading error correction code due to its high threshold and reliance on nearest-neighbor measurements only. It is therefore the backbone of our hardware evaluation, in which we compute the resource overhead for carrying out a given quantum algorithm fault-tolerantly assuming a realization of the surface code. In Section 8.2.2.1 we describe the basic notion of the surface code, while we provide the code's technical details – which allow the determination of the resource overhead – of this code in Appendix 15.

The surface code allows a trade-off between used space and used time, which is explained in Section 0. Finally, in Section 0 we comment on the assumed error model and the resulting performance characteristics of this error correction code.

8.2.2.1 Introduction to the surface code

The basic idea that errors are corrected (unless they are massively correlated) is implemented in a topological sense—only error patterns that change the topological genus of the state can go undetected, and this is unlikely to happen. The computational subspace of the surface code is stabilized by a set of operators (e.g., a +1 eigenstate of each), which are called stabilizers. Errors, such as unwanted bit flips or phase flips of single physical qubits, generally lead to changes of the measurement outcome of some of these stabilizers. The stabilizers mutually commute so they can be simultaneously measured, and they need to be complete, so their eigenvalues specify the state.

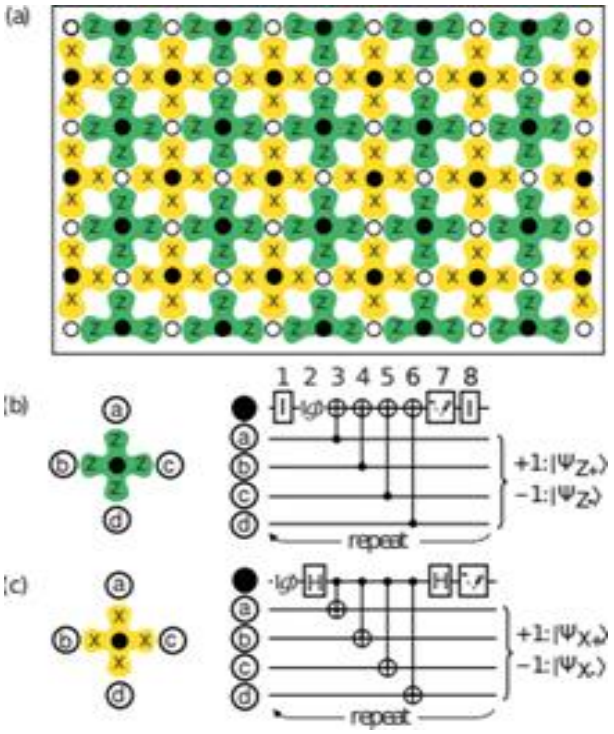

Figure 8.1: (a) Arrangement of physical qubits for the surface code. Data qubits are shown as open circles, measurement qubits as solid circles. The green and yellow crosses denote Z and X stabilizer measurements of the data qubits at the ends of the cross, respectively. At the boundaries, the stabilizer measurements include only three data qubits, represented by truncated crosses. (b) Circuit diagram for the Z stabilizer measurement. Identities are included to compensate for the Hadamards in the (c) X stabilizer measurement. Each step is performed simultaneously for all stabilizers. One round of such circuits for all Z and X stabilizers along the array corresponds to one syndrome measurement box. Reprinted figure with permission from [FMMC12] Copyright (2012) by the American Physical Society.

The qubits are arranged in two groups—data qubits and measurement (or syndrome) qubits—as shown in Figure 8.1. The measurement qubits are only used to indirectly measure the operator product $Z_aZ_bZ_cZ_d$ ("measure-Z") or $X_aX_bX_cX_d$ ("measure-X") of the four surrounding data qubits (at the boundaries, the operator products only include three qubits). Each data qubit is surrounded by two measure-Z and two measure-X qubits, the boundaries are chosen such that two opposite sides end with measure-Z qubits and the other two with measure-X qubits. The actual measurement of the operator product is performed by initializing the measurement qubit in an eigenstate of either *X* or *Z*, successive entangling all surrounding qubits with the measurement qubit using CNOT operations and then measuring it in the corresponding basis, *X* or *Z*. One such iteration, including all processes to measure the larger operator product indirectly, is referred as syndrome/stabilizer measurement or surface code cycle. For efficient performance, all steps of the stabilizer measurement (initialization, gates and measurement) need to be done *in parallel* along the whole array. For the CNOT, this means all qubits are arranged in pairs (in each of the four CNOT steps, a

measurement qubit is paired with another of its four adjacent data qubits) and a CNOT must be performed to every pair of qubits simultaneously.

The computational subspace is the set of states that are stabilized by all the operator products, which could be chosen to be their simultaneous +1 eigenstate. For practical reasons, however, one will use the state on which the system is projected after an initial measurement of all stabilizers. This state is random, but sufficiently characterized by the measurement outcomes. This way, initialization of every single data qubit is not necessary.

This stabilizer measurement will be executed consecutively (logical operations are done mostly by adjusting the structure of stabilizer measurements rather than performing additional gates between the stabilizer measurement); whenever an error occurs this can be detected from changes in the measurement outcomes as shown in Section 15.1. Nonetheless, these error detections are a crucial part of the error correction, because the stabilizer measurement projects the state into a stabilizer eigenstate, hence digitizing all continuous errors. The syndromes can be understood as changes in the stabilizer eigenvalues. Detected errors are not directly corrected on the quantum state, they can be tracked through the classical control and corrected all together in the end of the computation process [FMMC12].

In Appendix 15 we give details about central characteristics such as the interpretation of error syndromes and the implementation of logical operators. We further discuss an alternate type of surface code computation known as lattice surgery.

Volume compression and time-optimal computation

We can draw the defect structure (i.e., the positions of deactivated syndrome measurements, see Appendix 25.2 in [WSL+20] for schematic representation) for any logical gate sequence, including initializations and measurements in a three-dimensional diagram, where the third dimension represents time. A logical qubit is then represented by a pair of tubes of width $d/4$ separated by d, corresponding to the physical qubits needed to encode one logical qubit of distance d (the actual number is 4 times higher due to the syndrome measurement structure). Moving holes to other positions is represented by a tube of length d (i.e., during $d/4$ time-steps, d additional qubits are turned off) in a spatial direction, after which one needs to wait again d steps to prevent measurement errors, i.e., a connection of length d in temporal direction. The basic building block thus has an edge length of $d + d/4 = 5d/4$: d for a waiting or moving tube and $d/4$ for merging them. In such a diagram, topological equivalent structures perform the same operations. Thus, by deforming the structure, it is possible to significantly reduce the space-time overhead of a Clifford gate sequence. A CNOT or Hadamard gate requires an overall space-time volume of $12(5d/4)^3$ in a highly compressed form [FD12]. By increasing the number of qubits, it is also possible to deform any Clifford gate sequence such that increasing the number of gates does not increase the time required for execution (but only the number of qubits). Non-Clifford gates need classical feedback and therefore require a certain time-ordering which must be protected, so they cannot be performed in constant time.

To reduce the computation time for performing a large quantum algorithm to realistic and useful values, it is most important to optimize a quantum circuit to have lowest possible execution time. It has been shown [Fow12] that arbitrary large Clifford circuits can be performed in constant time by making the 3D structure flat and effectively performing operations in parallel. Furthermore, since the only time-step of a T gate that cannot be eliminated is the measurement with classical feedback, a circuit consisting of n T gates can be executed in asymptotic time nt_M with t_M being the physical measurement time + (negligible) classical feedback. Measurements are not necessarily limited to be done during the measurement step of a surface code cycle, so multiple T gates can be performed during one cycle. A typical approximation is $t_M = 0.1t_{SC}$ for a surface-code cycle time t_{SC}.

Performance

It is possible to reach arbitrarily low logical error rates by increasing the code distance, as long as all physical error rates per step (*physical* initialization, gates and measurements) are below a certain threshold. The underlying error model assumes [FMMC12, Section VII]

- the probability to initialize a qubit in a state orthogonal to the desired one to be p

- the probability to perform a single-qubit Pauli operator X, Y or Z on a data qubit when intended to do the identity (waiting) to be $p/3$ each
- the probability to perform an additional single-qubit Pauli operator X, Y or Z on a measurement qubit when intended to do a Hadamard to be $p/3$ each
- the probability for performing a tensor product of two Pauli operators, of which maximally one is the identity when intending to perform a CNOT between data and measurement qubit to be $p/15$ each
- the probability for reporting and projecting into the wrong eigenstate after measurement to be p.

Hence, p describes the probability for a Pauli error per step (of the error correction circuit) and per physical qubit, so the overall error probability in one complete error correction round is $\lesssim 8p$. Appendix 23 of [WSL+20] gives an analysis on how multiple errors add up during one cycle.

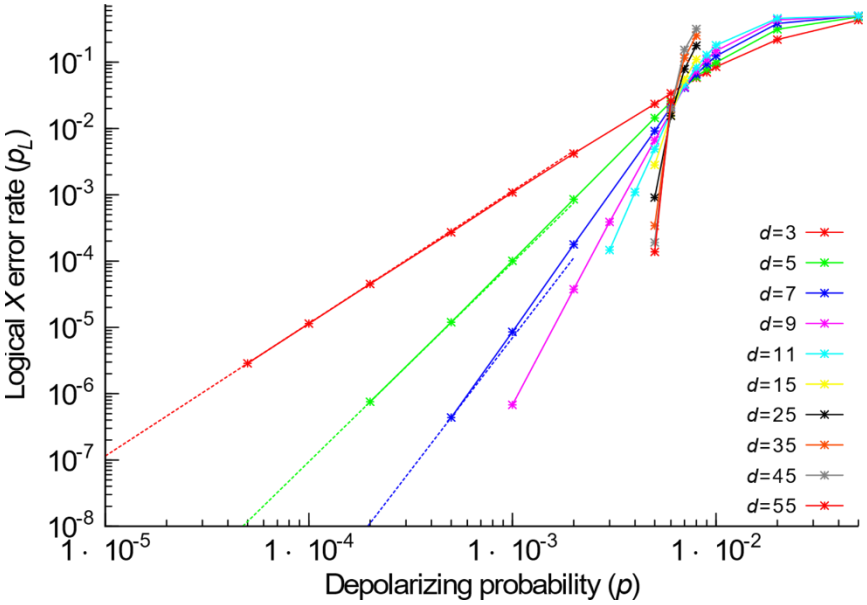

Figure 8.2: Performance below threshold for the surface code for distances 3, 5, 7, 9, 11, 15, 25, 35, 45, and 55. For distances 3, ,5 and 7, quadratic, cubic and quartic fit curves are shown as dashed lines. They only approximate the actual curves for low physical error rates p [FDJ13]. Reprinted by permission from Macmillan Publishers Ltd: Scientific Reports (A. G. Fowler, S. J. Devitt, and C. Jones, Sci. Rep., 3(1), 2013.), copyright (2013).

The threshold was found to be $p_{\text{th}} \approx 0.57\%$ for this error model [FMMC12], in the original publication of the surface code it was given as $p_{\text{th}} \approx 0.75\%$ [RH07], the actual value depends on the error model and underlying assumptions. The lower the physical error rate, the less qubit overhead is required to reach the same logical error rate. For physical error rates p much below the threshold and odd distances, the logical error rate was approximated by the empirical formula $P_l \approx 0.1(p/p_{\text{th}})^{(d+1)/2}$ [FDJ13]. Note that in this formula, p_{th} is not necessarily the actual threshold, since for error rates close to the threshold the approximation breaks down and p_{th} is the value where the fit lines (and not the actual curves) for different distances cross, see Figure 8.3. In literature, this value is sometimes referred as threshold under ideal syndrome extraction. Furthermore, the parameters for p_{th} and the prefactor might vary with the error model and the strength of syndrome extraction. [Fow13a] presents a way to find an analytic expression for the asymptotic performance of a code without the need for computational time-consuming simulations.

The important point that we learn here is that the logical error rate scales quadratic with the physical error rate for a distance 3 code, cubic for a distance 5 code, quartic for distance 7 and so on. This dependency can be intuitively understood by associating the logical error rate with the probability of an uncorrectable error chain (which has minimum length $(d+1)/2$). If we ignore non-Clifford gates for now, then the distance scales quadratic with the number of physical qubits: The simplest implementation of a logical qubit needs $(2d-1)^2$ physical qubits [Mar15][7]. It is important to keep in mind that this is the performance for a surface

[7]For an implementation of multiple double-cut qubits in a lattice it is a bit more, but still quadratic.

code only doing Clifford gates. The performance of the S and T gates depends on the distillation process, which has to be matched to the desired error rate (i.e., the error rate that the surface code can reach), requiring more overhead than the logical qubits for the rest of the calculation, see Section 15.3.3.

8.2.3 Color code

The color code is defined on a three-valent, three-colorable lattice with qubits on its vertices and stabilizers as operator chains around plaquettes. The two-dimensional color code can be mapped to a slight variation of the surface code by folding it along its diagonal [KYP15]. When compared to the surface code, the main advantage of the color code is the ability to carry out many quantum gates with less overhead. The disadvantages include a higher connectivity and a lower error threshold. For a comparison of the two and a discussion of different kinds of codes, see Ref. [CTV17].

Recently, color codes have received increased attention in the field of trapped ion quantum computing. This is mainly because at least within a single ion trap the required high connectivity – a main obstacle for many quantum computing platforms – can be realized straightforwardly using the Mølmer-Sørensen gate (see Section 13.1.2). Notably, the first experimental realization of a complete fault-tolerant gate set reported in Ref. [PHP+22] (albeit without reducing gate errors) is based on the color code.

Current literature does not suggest that the color code's essential advantage – simpler quantum gates – will make a decisive difference in fundamental gate count when compared to the usage of the surface code. This may be since the disadvantages – higher connectivity and lower error threshold – are still considerable obstacles, for example because in ion-based quantum computing the high-connectivity requirement is solved readily only within a single trap.

The gauge color code [BNB16] is a three-dimensional variation of the color code, which uses gauge-fixing to perform non-Clifford gates in constant time, but since the code itself needs more physical qubits the overall space-time overhead can only be reduced by a constant fraction at most. A rather promising approach is the doubled [BC15] or stacked [JOB16] color code, which can be mapped to a two-dimensional implementation. Computational universality is reached by switching between two encodings: one 2D code that can implement transversal Clifford gates on a 2D lattice, and one 3D code in which the T gate is transversal. Although the three-dimensional part can be mapped to a two-dimensional lattice, it requires some non-local interactions (but in a very limited way with only a small set of qubits involved).

The bottom line is that while the color code has important detailed consequences, in a large scale-extrapolation no major improvements are expected by current literature. Hence, we do not carry out a separate estimation of fault tolerance for the case of the color code, but rather concentrate our quantitative analysis on the surface code.

8.2.4 Other error correction codes

Another possibility for finding trade-offs is using other implementations or code variants. These often have special requirements on the physical system, but therefore come with additional benefits in terms of fault-tolerance or overhead. Hence, for some specific quantum computing platforms, they might still be a potential alternative. A short discussion of several code variants is given in [CTV17]. This section is restricted to qubit-based codes.

Bacon-Shor code

The first quantum error correction code that can be used to correct arbitrary qubit errors, i.e. bit-flip and phase-flip errors, was discovered by Peter Shor in 1995 [Sho95]. This code was later found to be a particular realization of a larger family of codes: Dave Bacon described two quantum error correction code families in [Bac06], one which consists of $[[n^2, n, 1]]$ codes and the other of $[[n^3, n, 1]]$ for integers n. Shor's code from 1995 is the n=3 example of the latter code family, because of which it is often called the Bacon-Shor code.

Toric code

The toric code, discovered by Alexei Kitaev [Kit97a,Kit97c,Kit03], is the first quantum error correction code that is based on topological properties. The toric code can be considered the precursor of the surface code, for this connection see the introduction of [FMMC121]. Due to the need of non-local interactions or nontrivial qubit layouts, the toric code has been considered impractical. However, non-local interactions are possible for certain quantum computing platforms (in particular, those based on atomic and ionic qubits), because of which the toric code has received increased attention in recent years.

Multi-level system codes

Implementations using multi-level systems, qudits, have been shown to be capable of reaching threshold error rates of more than 8% for high enough qudit dimensions [WAB15]. However, handling of such high-dimension multilevel systems is complicated and in most physical implementations not even possible. A possible platform would be molecules [TdVR02].

Long-range and high-dimensional interactions

Error correction codes using interactions of qubits that lie arbitrary far away can have much better threshold and performance than 2D nearest-neighbor codes like the 2D surface code. Often, they attract only little interest because in the leading platforms they are more than hard to implement. However, in distributed implementations using photonic interconnects (or any other flying qubit), like NV centers, quantum dots or trapped ions [MK13, MRR+14], arbitrary qubit interactions are not a big problem.

A rather old proposal of Knill [Kni05] reports a threshold of 3% for a code using non-local interactions and post-selection. Besides a change of threshold, codes using more than two dimensions are also capable of implementing transversal non-Clifford gates [BMD07], which significantly reduces the qubit overhead due to magic state distillation. However, one needs to be careful here: The ability to perform T gates often comes with a reduction of the set of easily realizable Clifford gates. The Hadamard gate for example cannot be performed in the three-dimensional color code without an extra logical ancilla.

Tailored codes

If the error model of the underlying is known, e.g., if it is dominated by phase errors but has negligible bit flip, the error correction code can be tailored to that mechanism. [TBF18] details a slight modification to the well-known surface code that leads to significant improvement in the error threshold for precisely that code. The modification consists of changing the plaque stabilizers from Z to Y operators and using a specific decoder [BSV14]. The results of this alteration to the surface code are made explicit in the error threshold values of 43.7% for pure dephasing noise, and 28.2% for a bias 10 (bias is the fraction of Z noise over X and Y noise).

While these results are promising, a full fault-tolerant analysis has not been included, i.e., the code behavior is only studied for ideal measurement and gate operations, so the threshold should not be compared to the results used in this study. It is unclear whether the positive results listed above will remain relevant after the code is adapted to provide fault-tolerance and, even if the code adjustments will show an improvement, it most probably will not be as substantial as the one in the paper.

Topological cluster states

There are physical systems, for which an initial collective interaction of the qubits is easier to implement than specific multi-qubit gates along the computation process. One-way quantum computation using topological cluster states is a possible alternative for these systems, also accounting for qubit loss, for which a fault-tolerant protocol similar to the surface code has been proposed [RHG06, WF14b]. However, this scheme requires a three-dimensional cluster state. Even if implemented on a 2D lattice, this needs more connectivity than the usual square lattice used for the surface code and usually also fast entangling

gates on the fly (which is in contradiction to the cluster state idea). Besides, this approach also does not allow transversal non-Clifford gates.

8.2.5 Current research goals

Perhaps the biggest disadvantage of both surface codes and color codes is the large resource overhead. Accordingly, on the theory side a lot of effort is directed towards finding novel types of error correction codes. Perhaps the most promising research area is that of low-density parity check codes (LDPC codes).

We note that the surface code in its original perception encodes a single logical qubit into n physical qubits, and the code distance scales as $n^{1/2}$. For example, [CSA+21] reports the experimental realization of a [[7, 1, 2]] surface code, i.e., a code that consists of 7 physical qubits – 4 data qubits and 3 ancilla qubits – with distance d=2. Note that with this distance one cannot correct even a single error [since (d-1)/2<10 for d=2*]*. More recently, [KLR+22] realized a [[17, 1, 3]] surface code, which uses 9 data qubits and 8 ancilla qubits, and which *can* correct a single physical error [(d-1)/2=1 for d=3].

The quest of finding "good" LDPC codes is to realize asymptotic constant resource overhead. That is, for large numbers of used physical qubits in a single code, n, both the number of encoded qubits and the number of correctable errors should scale linearly in n. In other words, good LDPC codes are those for which both k/n, the encoding density, and d/n converge to a finite value in the limit of large physical qubit numbers n.

We note that the surface and color codes are LDPC codes, but since they only encode one logical qubit (k=1) independent of the number of physical qubits, n, they are not high-density codes. While good classical codes are simple to find, the existence of such quantum codes has yet to be established. A theorem proved in [Got14] states that such quantum codes could indeed exist, and it is formulated under assumptions not unlike those of the error correction threshold discussed in Section 8.1.3. An overview of the most important progress in this area of LDPC codes can be found in the recent review article [BE21].

8.2.5.1 Good LDPC codes

In 2024, Bravyi et al. reported the finding of a family of good, or high-density LDPC error correction codes [BCG+24]. That work includes a numerical performance analysis using an error decoder yielding a code threshold of 0.7%, a value comparable to the surface code threshold. The new code is of great importance, because it constitutes a step toward significantly more efficient error correction, with shown qubit overhead reductions by an order of magnitude for logical qubits encoded into up to 288 physical qubits (see also Sec. 9.3.3.1 for a comparison to error corrections schemes with cat qubits that appeared around the same time). Reference [BCG+24] however, does not provide protocols for carrying out unitary quantum operations, so that this code can currently only be used as a quantum memory. We also note that the high encoding rate of this code is not mathematically proven for arbitrary code sizes, and so its usefulness for large qubit numbers is not guaranteed.

The impact of this code is particularly high for superconducting qubits, for which good LDPC codes are generally difficult to find, because their usually two-dimensional chip layout strongly limits qubit connectivity. Indeed, also this new LDPC code is not local, which means certain non-nearest-neighbor qubits must be directly coupled. To solve the problem of the resulting intersecting microwave lines on the chip, several technological advances need to be accomplished. As is laid out in the paper, quantum processors must be operated using bilayer chips, with superconducting circuits on the top and bottom surface layers. The operation of such devices is based on the usage of high-fidelity through substrate vias (TSVs) which connect the two surfaces. Development of TSVs for multi-layer chips has already been ongoing for many years, see, e.g., [RWC+20]. Further, the number of qubit connections needs to increase from currently (often) four to seven. Some of these connections will connect qubits separated by large distances, which requires a type of frequency engineering. According to [BCG+24], this last technological advancement of long-distance connections is the most difficult.

8.3 Basic requirements

In [FMMC12], an exemplary analysis of the quantitative requirements for running a factoring algorithm was done: Assuming the physical error rate to be 10% of the threshold error rate, factoring a 2000 bit number requires $2 \cdot 10^7$ physical qubits for the logical qubits, and $2 \cdot 10^8$ additional physical qubits for the distillation ancillae, i.e., a total number of $2.2 \cdot 10^8$ qubits. With measurement times of 100 ns, the computation will run around 27 h. In Section 7.4 of [WSL+20] we turned this into a general conversion formula for fault-tolerant execution of algorithms, resembling the concept of quantum volume brought forward by IBM [BBC+17].

The qualitative requirements for the surface code to be implementable can be classified in three levels: the physical qubit level, the experimental setup and the classical control. For the **physical qubits**, the requirements are:

- The ability to initialize and frequently reinitialize the qubit in at least one basis
- The ability to perform single qubit gates, at least Pauli, Hadamard and T gates
- The ability to measure in at least one basis
- The ability to perform two-qubit SWAP and CNOT gates, at least for nearest-neighbors on a two-dimensional square lattice
- Error rates for all possible operations (gate, waiting, initialization and measurement) significantly lower than the threshold of approximately 1% that do not increase with the qubit number / array size. This does not mean that the coherence time of the qubit needs to exceed the whole computation process, but it must be long enough to ensure sufficient low error rates after the time required for one operation. Trade-offs are possible (see Section 8.4.2)
- No qubit losses occurring at all (i.e., photons or atoms disappearing)[8]

Further desirable properties are a low probability of parallel, correlated errors and leakage errors. However, these errors only lead to slightly worse performance or can be corrected with some additional effort (see Section 1.4.1 in [WSL+20]). Requirements on the experimental setup are:

- Many qubits arranged in a 2D square lattice existing simultaneous and long enough, all fully controllable and all fulfilling the above requirements. This implicates
  - large space at sufficiently low temperature available
  - long timescales to be reached: Even though the coherence time of the qubit can be lower, the qubits must at least exist through the whole computation process (see for example trapping times of ions / neutral atoms as described in 13.2.2), also cooling and isolation must be available long enough
- Simultaneous measurement, initialization and gates (Hadamard, SWAP, CNOT)[9]:
  - For a lattice of $2n$ physical qubits (n data and n measurement qubits), n operations at the same time, being either initialization, measurement or CNOT are required. Note that if only one basis is experimentally accessible, measurement and initialization include Hadamard gates.
  - Simultaneous SWAP gates are limited to the region of the logical qubits on which a logical Hadamard shall be performed (which can be several at the same time, though).

The basic requirements on the **classical control** are pretty much met already, using Edmonds' minimum-weight perfect matching algorithm [Edm65] and optimization tools[FWMR12]. It has been shown [Fow15] that, given a 2D array of (parallel) processing elements with communication between nearest neighbors and an external memory, parallel decoding can be performed in constant $O(1)$ time for the surface code, independent of the number of qubits. Thus, the main challenges are large parallel computation, enough

[8] Quantum error correction with topological cluster states can deal with qubit losses [WF14b].

[9] This requirement might be softened if gates are fast enough to make partially sequential runs (not scaling with the lattice size) acceptable.

memory and most important processors fast enough to preserve the low error rates of the qubits (i.e., significant faster than coherence and gate times) and to retain reasonable computation times.

8.4 Performance discussion

The effect of errors on the outcome of quantum algorithms depends on the type of considered error. Here we focus on stochastic errors. Coherent and non-Pauli errors also probabilistically affect the output of quantum algorithms, resulting in a slightly different error propagation. This is discussed in detail in an older version of this study [WSL+20].

8.4.1 Simplifications within stochastic errors

The error model on which the standard performance discussions and syndrome extraction algorithms are based on is a rather simple and unrealistic one: Every possible kind of error, faulty single-qubit gate, two-qubit gate, initialization, measurement and waiting period (identity gate), is assumed to happen with equal probability. In this section, we discuss more realistic models that are still based on stochastic error models whereas in the next section we discuss the impact of coherent errors. Given the sometimes-huge difference already between single-qubit and multi-qubit gate fidelities, this is far from reality and cannot reflect a realistic quantum system. Also, as described in Section 6.3, incoherent errors are not always depolarizing. More generally, the transversal decay time T_2 is different, often shorter, than the energy decay time T_1. Also, at low temperature, energy relaxation is asymmetric and the final state the system decays into is not fully mixed. This is not a problem for syndrome extraction per se – if 7.4.3. But if one understands the error processes better, we see that it is unnecessary to restrict all errors to the same threshold, since some trade-offs are possible here. It also enhances the syndrome extraction significantly if the exact error rates are known, Autotune makes use of this fact [FWMR12] and reaches highly improved logical error rates. Figure 8.3 shows two plots for the performance of the surface code on a realistic error model, one with the usual syndrome extraction, and one with the help of Autotune. The enhancement comes from the fact that with realistic error models, the shortest path is not always the most probable one, but the unoptimized algorithms can only find the shortest paths.Figure 8.3 shows two plots for the performance of the surface code on a realistic error model, one with the usual syndrome extraction, and one with the help of Autotune. The enhancement comes from the fact that with realistic error models, the shortest path is not always the most probable one, but the unoptimized algorithms can only find the shortest paths.

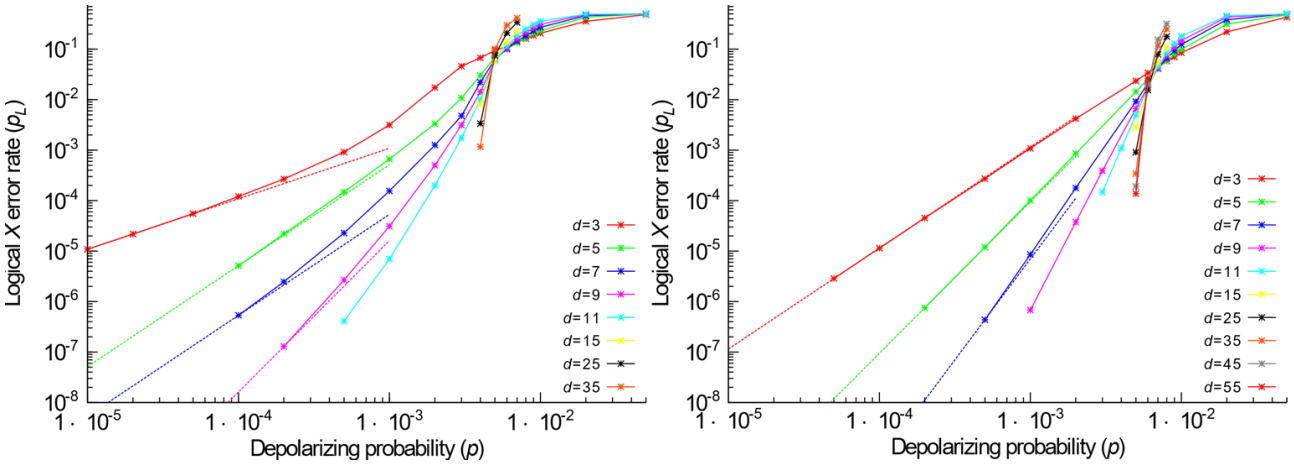

Figure 8.3: Another two threshold plots indicating the threshold at the crossing of the different lines.

With the Autotune library, available on the website of the Topological Quantum Error Correction Group in Melbourne, it is also possible to calculate the actual performance for any given implementation with given error rates. According to [Mar15], measurement errors can be the highest ones, single and two-qubit errors can be around the same range, therefor it is most important to optimize two-qubit errors: With that, the required single-qubit error rates will usually be automatically met. An extreme example of the use of error asymmetries is the result [TBF18], described below under “other error correcting codes”.

Furthermore, error and overhead calculations are often done for implementations of only one logical qubit along the whole array, therefore not requiring any double-cuts and needing less qubit overhead. This does not drastically change the performance but should at least be kept in mind. All experimental implementations of surface codes so far do the same and only demonstrate single logical qubits. Showing a fault-tolerant two qubit gate is a major program goal. This is a step in the right direction but does not show the ability to perform logical operations on multiple (or even single) qubits. Furthermore, there has never been any implementation shown that can cope with the huge number of qubits needed for relevant calculations. Thus, we do not know how the fidelities and coherence times of each physical qubit change when embedded in such a huge cluster. Interaction effects, cooling or addressing problems might occur.

Of course, these simulations (and implementations) also do usually not include the ability for non-Clifford gates: The distillation error rates need to be matched to the respective error rate the surface code can perform. Most of the qubit overhead during a calculation is caused by the ancillae needed for state distillation, so the overall qubit overhead does not only depend on the code distance but also strongly on the number of distillation rounds – which has a different dependency on the error rates than the distance (see Section 15.3.3).

A further problem consists of errors that are not at all included in the error model, such as leakage, qubit loss, or correlated errors.

Qubit loss cannot be treated in the surface code, but with a variant, the topological cluster states [WF14b].

Leakage errors, which for example appear in superconducting qubits with more than two energy levels, cannot be corrected with the standard setup of the surface code but after slightly adjusting it as described in [GF15]. By using SWAP operations between data and measurement qubits after each round of error correction, each qubit is a measurement qubit every other round and therefore is reset from time to time (during the initialization for the stabilizer measurement). So, even if a qubit leaks out of the computational subspace, it will be brought back during its next round as measurement qubit. This adjustment needs only $2d$-1 additional physical qubits for a distance d code, and additional time cost independent of d. For benchmarking protocols accounting for leakage, see Section 7.4.3.

Correlated and multi-qubit errors were analyzed by Fowler and Martinis in 2014 [FM14]. They found that the surface code is rather robust to such kinds of errors. For local errors, and exponential suppression of large-area errors it is sufficient, typical experimental errors can be compensated for with negligible qubit overhead. Long-range two-qubit errors can be corrected with even less overhead, although there is not always a threshold[10] depending on how strong correlations are suppressed. However, error rates low enough for reasonable computation can be reached. Experimentally, the important thing is to observe the error rates when a maximum number of qubits is manipulated in parallel, to see whether an implementation can reach reasonable logical error rates or not. Further discussion on correlated errors can be found in Appendix 22.4 of [WSL+20].

8.4.2 Possible Trade-offs

There are several trade-offs between physical error rates, qubit overhead and computation time, making different approaches possible.

For both the bare surface code and the distillation, the relations between qubit overhead and error rate improvement are exponential. The exact relations differ, but both processes can be done with less overhead if lower initial error rates are available; but also with higher initial error rates allowed for the cost of more qubit overhead, depending on the underlying physical conditions.

A significant effect on the threshold can be reached with particularizing the error model to realistic values. Already early calculations [WFH11] have shown that using a model with error rates typical for ion trap implementations, i.e., $p_2 = p$, $p_1 = p/1000$ and $p_M = p/100$ for two-qubit, single-qubit and measurement errors, respectively, the threshold condition could be raised to $p < 1.4\%$. Using Autotune [FWMR12],

[10] No threshold does not mean that no improvement is possible at all. But for a given physical error rate—no matter how low—it is not possible to reach arbitrary low logical error rates.

acceptable measurement errors of up to 10% were reported, provided that two-qubit gates can be performed with a rate of $p_2 = 0.1\%$.

Knowing that logical T gates are the most demanding elements of fault tolerant computation, it also makes sense to think of algorithms that, even if requiring more qubits or computation steps, need less total T gates. This is a problem of finding trade-offs on the code side. It has been shown [BK13] that in general, 2D codes cannot implement non-Clifford gates without turning off the topological protection at some points and thereby reducing the fault-tolerance. For 3D geometries, however, some gates, including the T gate, can be implemented without the large overhead caused by state distillation. Although some of these three-dimensional codes can be mapped onto a two-dimensional lattice [JOB16, BC15], they do not reach the same high level of error threshold as the surface code and thus can only be realized with physical error rates that are one magnitude lower.

A trade-off between space and time can be reached by deforming the topological space-time structure of defects (see Appendix 14), but also in the production of the magic state ancillae. When created in ancilla-factories in an independent part of the circuit, they can be directly used in the actual computation circuit whenever they are needed (without waiting for them to be created), so the actual T gate can be performed in the time required for the CNOT, measurement and feed-forward. Further time-optimization [Fow12] proposes that the only relevant time scale is the time needed for the classical feed-forward of non-deterministic gates—one measurement time per T gate—as long as enough additional qubits are introduced (as further explained in Appendix 15.4). Even in time-optimized models, typical times for relevant factoring algorithms are still in the order of days or hours. For this reason, as long as no faster algorithms (in terms of T gate rounds) or faster measurements are available, a qubit-optimized but time-consuming run is not worth consideration.

In general, determining the effort for a given task consists of determining its logical volume—number of qubits and gates and translate it into physical volume.

8.5 Experimental status of error correction

8.5.1 Resolution of evaluation levels C and D

In defining the evaluation levels, we have grouped achievements that need to be achieved before transitioning into the next level and which also define different ways of developing quantum computers. Within these levels, still, multiple milestones need to be achieved to complete the level, however, they have usually no definite order or dependency. With the aim of categorizing and evaluating the cutting edge of experiments in quantum error correction and fault tolerant quantum computation, we would like to outline the points inside the key levels C and D.

As described above, level C is concerned with performing an error correction experiment on quantum memory. Within this, there is a list of actions to take in order:

1) Perform error correction against a single type of error for
   i) one or ii) multiple rounds and showing improvement of the error rate a) with increasing the number of rounds and b) below the physical error,
2) Perform the same experiment as in 1) but for two independent single qubit errors, usually bit flip X and phase Z,
3) Perform the same experiment as in 2) but now with code distances larger 3 (recall that distance 3 allows the correction of errors occurring on 1 qubit per cycle) and show improvement with code distance.

Evaluation level D is concerned with actually performing fault tolerant gates on error corrected qubits and has been attempted only very recently. It has to sit on the foundation of level C and one key question is, whether the performance of level C is preserved while performing these operations, i.e., if error correction is still beneficial. Another difference is whether transversal gates that are performed within the main error correction code (usually Clifford gates) are demonstrated, or a complete universal set (usually Clifford+T).

We thus can define the categories

1) Demonstration of single logical qubit Clifford gates I) basic functionality and ii) performance with full level C reduction of the error rate
2) Same as 1) but for two logical qubit Clifford gates
3) Same as 1) but for single logical qubit universal gates
4) Same as 2) but for two logical qubit universal gates

8.5.2 Evaluation of the Google paper on 105-qubit QEC beyond break-even point

Google AI has released a preprint that demonstrates quantum error correction beyond the break-even point. [Goo+24].

Its main achievement is exactly that - it operates error-corrected quantum memory with surface codes of increasing distance (up to distance 7) and achieves an error of the error corrected systems that is lower than the ingredients. This shows that there are no conceptual and principal show-stopper in quantum error correction and now definitely closes level C of our evaluation scheme. In this sense, it overcomes the main restrictions of the 2022/23 Google paper [AAA+22]. On a more secondary level, the paper also shows real-time decoding and correction on a distance 5 surface code and the error correction goes over many rounds and distances. Also, a large bit-flip code is used to check for the sensitivity to rare events, as well as for scalability of the surface code distance.

This is achieved by a number of engineering improvements – better and more qubits (from 72 to 105), better control, better electronics. The issue of leakage errors, i.e., excursions beyond the computational states 0 and 1 into higher states, was addressed with extra hardware, as well as the selection of the Data Qubit Leakage Removal procedure (DQLR) [MMEA+23]. DQLR successfully mitigates correlated leakage introduced errors in the presented planar surface code, as well as in bit-flip codes.
An exponential fit suggest scaling the surface code distance will divide the error rate by 2 when the former is also increased by 2, up to a first floor of 1e-8 found through the study of bit-flip code distances.

Crosstalk has also been reduced, but no new publication on the subject from Google Quantum AI is available yet.

A main insight is that the background of rare correlated „catastrophic“ events has been significantly reduced - the uncorrectable error rate has dropped by four orders of magnitude and their frequency reduced correspondingly (from every few minutes to every few hours). This leads to the conclusion that the problem of the quantum computer to be interrupted by bursts of ionizing radiation, such as cosmic radiation, has been mitigated - without going to a deep underground facility. It seems that the solution is in better qubit design and use of materials. More specifically the engineering of better gaps in Josephson junctions prevents quasiparticle (QP) tunnelling through the junction – an effect which created correlated errors as it used qubit state transition as part of its process. By imposing a high energy gap between the thin film and the thicker part in the Josephson junction, the qubit state decay can no longer be used by the quasiparticle to stimulate its transition by quantum tunnelling. This is performed by fabricating thinner Aluminium junction leads, which doesn't present a real added complexity in the fabrication process [MEMA+24]. The added benefit of this method compared to the previously used QP traps is that it deals with QP poisoning: an effect which was directly related to the QP density in the materials, i.e. the amount of radiation received by said material. It is however suggested by the authors that gap engineering should be coupled with other methods (most likely QP traps and more) to resolve other issues, like QP scattering and two level system scrambling.

The error suppression floor is currently assumed to lay around 1^{-10} due to a rare large correlated error mechanism appearing roughly once per hour, that still needs to be properly understood.

Future developments will now try to address physical errors as CZ gate errors and data idle errors represent respectively 40% and 20% of the Google Quantum AI error budget.

8.5.3 Global status of error correction experiments

Here we describe some of the central results of some of the most recent relevant experimental achievements in the field of quantum error correction. Most of the pre –2024 experiments are listed in a summary of error correction experiments in [AAA+22] (see Table IV therein). The main update of 2024 is that the platforms discussed below have reached level C of our evaluation scheme, and a question of interest is now whether level C has been completed. Accordingly, we evaluate the experiments along the lines of Section 8.5.2 above.

Most of the error correction codes implemented in the experiments below are discussed in Section 8.2.4. Recall that the surface code features the best (realistic) error thresholds of roughly 1%, corresponding to gate fidelities of about 99%.[11] Further recall that as per the definition given in Section 8.2.1, a quantum error correction code specified by [[n, k, d]] encodes k logical qubits into n physical qubits with a code distance of d.

8.5.3.1 Superconducting circuits

One of the most recent demonstrations of quantum error correction based on superconducting circuits is presented in [Goo+24], which is discussed in some detail above in Section 8.5.2. A major achievement of this work is the reduction of the error rate under the physical error threshold by increasing the code distance from 3 up to 7 and mitigating the quasiparticle adverse effects caused by cosmic radiation events. Qubit leakage, the phenomenon of individual qubits reaching states outside of the two used for data encoding, is also reduced in this new iteration of the Google Quantum AI team experiments.

Another relevant work on superconducting qubits featuring high-fidelity gates is discussed in [KLR+22]. In that work, 17 physical qubits have been used to encode a single logical qubit with 9 data qubits and 8 syndrome qubits. On the contrary of [Goo+24], the observed logical fidelities are still lower than the average physical fidelities, because of which no fidelity gain has been reported. We note that the reported errors are similar to Google Quantum AI's previous experimental achievements [AAA+22]. For example, the average single-qubit gate errors are 0.09% [KLR+22] vs 0.11% [AAA+22], whereas the average two-qubit gate errors are 1.5% [KLR+22] vs 0.6% [AAA+22].

The new [Goo+24] results remove one of the principal roadblocks to successful quantum error correction, as increasing code distance leads to better results once the logical qubit error is under the physical qubit error threshold,

8.5.3.2 Rydberg atoms

In [BHS+22], Rydberg atoms have been utilized to realize a [[16,1,3]] surface code, counting a total of 19 physical qubits (13 data qubits + 6 ancillary qubits), and a [[16,2,2]] Toric code, counting a total of 24 physical qubits (16 data qubits + 8 ancillary qubits). Information is stored in hyperfine states (with relatively small energy differences), while excitations into (high-energy) Rydberg states are the basis for entanglement generation. Optical tweezers (see 14.2.1.3 "Collisional gates") are used to displace the atoms within in a 2D array.

For each error correction code only a single round of error correction has been carried out. In a recent update to this study [BEG+24], a fidelity above the physical error rate has been achieved, with a fidelity of 99.5% for a two-qubit entangling C_Z gate. The surface code has been upgraded to a rotated surface code [AAA+22] with parameters [[d^2,1,d]], where $d=3,5,7$ is the code distance. The two qubit gate uses the juxtaposition of two of these codes. The total number of qubit is augmented by the number of ancillary qubits $(d^2-1)\backslash 2$ for each code. NV centers

[11] Some error correction thresholds are listed in [CTV17] – e.g., for the surface and color codes, see Table 1 therein – and in [Ali07] – e.g., for Steane codes and the [9,3,1] Bacon-Short code used in the context of code concatenation, see Table 5.1 in Chapter 5 therein.

In [AWR+22], a so-called perfect code [[5,1,3]] is realized using a total of 7 physical qubits. This code employs one auxiliary qubit for measuring stabilizers and one flag qubit for the realization of the flag error correction protocol. The experimental setup consists of a single NV center in diamond, which represents the auxiliary qubit, and 27 nearby carbon atoms (13C), 6 of which represent the remaining required physical qubits. Physical operations are carried out using microwave pulses.

In [AWR+22], a comparison is drawn between the preparation of the error correction code following a non-fault-tolerant and a fault-tolerant method. The latter outperforms the former, despite using more quantum gates. The work further reports the realization of (transversal) Clifford gates and fault-tolerant stabilizer measurement with the result that the logical gate fidelities are below physical ones, because the latter are below quantum error correction thresholds (e.g., some of the single-qubit gate fidelities are as low as 95%).

We note that a clear difficulty with this approach is the scaling of this error correction scheme, since it gets increasingly difficult to find more nearby 13C atoms, and to address them using different microwave frequencies. An alternative, systematic route of scaling is based on connecting multiple NV centers, which requires additional interactions beyond those featured in [AWR+22].

8.5.3.3 Ion traps

The work [dSRABR+24] reports on quantum computing experiments run on a commercially available 32-qubit quantum processor [MBA+23]. The paper's most important claim is the achievement of logical memory errors that are smaller than the physical error rates by up to two orders of magnitude, while using quantum gates that represent common elements of logical circuits. In principle, effective error correction seems possible, since the reported physical error rates (for quantum gates, state preparation and measurement) of around 0.15% are smaller than the error thresholds of various quantum error correction codes.

The main results are increased entanglement fidelities for Bell states production when comparing error-corrected logical circuits (i.e., using error correction) with purely physical circuits. Indeed, significant fidelity increases are found as a result of error correction. However, it should be noted that this is conditioned on the usage of post-selection and (what the authors call) pre-selection, by which together roughly 30% of the experimental runs were discarded. It should be noted that post-selection may impediment the scalability of quantum computing, putting the results.

[PHP+22] presents a demonstration of an error correction experiment in trapped ions. In this work, two logical qubits have been implemented, each encoded into a [[7,2,3]] color code. Using a novel approach called flag fault tolerance [CB18, CC19, CR18, CR20, Rei20] allows usage of only two auxiliary qubits, resulting in a total of 7+7+2=16 physical qubits. Similar to the NV center experiment described above [AWR+22], state preparation is compared for the cases of non-fault-tolerant and fault-tolerant methods, with the latter surpassing the former in terms of fidelity. The novelty of this work [PHP+22] is that a fault-tolerant universal gate set has been implemented, including a T-gate. Nonetheless, due to insufficient physical gate fidelities (for example, the average fidelity of entangling two-qubit gates is only 97.5%) the logical error is not improved when compared to the physical errors.

While the accomplished universal gate set belongs to level D of our evaluation scheme, this experiment does not yield a systematic error reduction in any of the disciplines including storing information, which is at the heart of level C. As a result, the demonstration of [PHP+22] is to be placed in level C of our evaluation scheme.

Another noteworthy quantum error correction experiment with trapped ions is reported in [RAB+22]. The main objective of this experiment has been to compare a [5,1,3] perfect code with a [7,1,3] color code, where the former uses less qubits but has a significantly lower error threshold. As a result of this analysis, the latter appears to outperform the former in terms of logical fidelity due to lower circuit overhead when performing logical operations.

This experiment has reached a notable milestone by achieving logical two-qubit gate fidelities surpassing the underlying physical gate fidelities [RAB+22]. However, this improvement is limited to experiments in which no error detection cycles are performed.

8.5.3.4 Photons

In [LCE+21], an error correction experiment using photons has been conducted. The focus of this experiment is the teleportation of a quantum state onto a logical qubit, which is, for example, needed to implement non-Clifford gates such as T-gates. The quantum error correction code for the logical qubit is the [[9,3,1]] Bacon-Shor code, which is realized using only three photons – the 9 qubits are implemented via three degrees of freedom, namely each photon's path, polarization, and the orbital angular momentum.

We note that merely a single round of error correction has been carried out, and only a single code distance (d=3) has been realized.

8.5.3.5 3D superconducting cavity

The work [CET+20] realizes a bosonic QEC code, which is based on a proposal by Gottesmann, Knill and Preskill (GKP) to use grid states of a harmonic oscillator [GKP01] – see Section 9.3.2. For this, the experiment in [CET+20] creates squeezed states (see 8.3) in a 3D superconducting cavity. Besides that cavity, which stores an ancillary transmon qubit and an ancillary readout resonator are used to extract the stabilizer information. The system encodes a single encoded qubit. This scheme, which allows and realizes the suppression of all logical errors, is compatible with quantum error correction since the readout is non-destructive.

The number of rounds ranges from 1 to 200. A main result of this work is the extension of the cavity's lifetime by the application of quantum error correction, which can be considered as surpassing the break-even point [MPS+21]. As discussed in Section **Error! Reference source not found.**, bosonic codes need to be treated differently from regular error correction codes. The achievement of the break-even point in conjunction with difficulty in scaling this bosonic system places this demonstration in the middle of level C of our evaluation scheme.

8.5.4 Post-deadline achievements in quantum error correction

Right after the aforementioned result by Google, several other results showing the completion of our level C, i.e., reaching the break-even point of quantum error correction were posted. We give only brief accounts of them as they were past the cutoff date (August 31 2024) of this edition, but also, as the Google result stands out in this field as following most closely the standard roadmap towards fully scalable fault tolerant quantum computing. The next edition will add depth to the discussion.

A Microsoft Quantinuum collaboration [PNH+24] has demonstrated going beyond break even on an ion-trap system including the implementation of error-corrected logic gates, which make up level D. It is based on a very compact error correction code, the tesseract subsystem quantum error correction code as well as a preselection method that helps to mitigate the slow repetition cycle of the ion trap architecture. The further scaling of the tesseract code is unclear.

Amazon [BSE+24] demonstrated combining the intrinsic dephasing protection offered by Bosonic codes with an external repetition code. As error correction is intrinsically built into the cat qubit, it is less clear to really certify that break-even was surpassed, yet it is an important demonstration of the viability of that approach.

Researchers at Yale University [RAC+24] have used the GKP code in order to improve quantum computing on Qudits (i.e., quantum information carriers with more than two states) beyond break even in a hardware efficient way.

8.6 Summary

In summary, the recent experiments discussed above are all categorized somewhere within level C of our evaluation scheme. In most cases, the reason for not accomplishing level C is that an increase in fidelity has not been achieved, and in some cases, it is the small number of realized error correction rounds or code

distances. The bosonic GKP code realization needs to be treated as a special case, since the path to scalability of this code is not clearly laid out.

8.7 Glossary for error correction

Coherent error—Error represented by a quantum-coherent operation (here used synonymously with unitary errors). For detailed information, see Section 6.5 in an older version of this study [WSL+20].

Clifford gate / Clifford gate—Normalizer of the Pauli group, Section 7.4.3.

Concatenated code—error correction code consisting of connected layers of error correction codes, see Section 8.1.3.

Depolarizing channel—7.4.3.

Distance — 15.2.1.

Error correction cycle—sequence of initialization of syndrome qubits, mapping of error information onto the syndrome qubit by quantum gates, syndrome readout, processing of errors and corrective operations, see Sections 8.1.4 and 8.2.2.1.

Error rate—probability of an error per operation (see e.g. Section 7.4.3).

Error syndrome – bit value containing information about the location and nature of errors, see Section 8.1.1 and Appendix 15.1.

Gottesman-Knill theorem—theorem stating that a Clifford-only quantum computer can be simulated efficiently on a classical computer see Section 7.4.3.

Logical qubits – an error corrected qubit that is used in an algorithm, see Section 8.1.1 and Appendix 15.2.

Magic state distillation—leading procedure to implement the *T* gate, see Appendix 15.3.3.

Pauli Error—an error described by phase and bit flips and combinations thereof.

Physical qubits – the physical devices whose errors create the need for error correction, see Section 8.1.1

pi/8 gate – see *T* gate.

Stabilizer (of a state)—a set of commuting operators to which the state is an eigenstate with eigenvalue 1 and that uniquely determine the state, see Section 8.1.1.

Stochastic errors— 8.4.

Surface code—currently leading code for quantum error correction, see Section 8.2.2.

Surface code cycle— Error correction cycle of the surface code (see there).

Syndrome qubit – a qubit containing information about an error syndrome (see there).

Syndrome measurement cycle—Error correction cycle (see there) without the last two steps.

Systematic error—errors that occur with certainty (but can be small by another measure), (for more details, see Appendix 22 in [WSL+20]).

Threshold—numerical value of a physical error below which error correction is effective in reducing the logical error, see Section 8.1.3.

T gate – a single-qubits non-Clifford gate used to go beyond the limits of the Gottesman-Knill theorem, see Section 8.1.4 and Appendix 15.3.3.

Unitary error – an error described by a unitary operation. For detailed information, see Sections 6.5 and 7.4.1.3 in an older version of this study [WSL+20].

9 Benchmarking and fault-tolerance on non-standard architectures

Some implementation platforms are not well suited for application of the surface code or other standard error correction models. This can either be because they are not based on the gate model (as in quantum annealing) or because the resource inventory is vastly different from that of most platforms, such as in cluster-state quantum computing. The benchmarking scheme for them deserves separate evaluation.

9.1 Quantum annealing

As described from a hardware perspective in Section 13.1.4, Quantum annealing/adiabatic quantum computing is based on slow global control of qubits rather than on delicate and fast local control. Quantum annealing can efficiently simulate gate-based quantum computing if many-body interactions, which are n-local with $n \geq 3$, are available. Annealing platforms of this type have not yet been realized. Instead, quantum annealing for optimization problems has been implemented by Canadian company D-Wave Systems, using rather incoherent qubits and 2-local couplers. While this platform lacks a fundamental resource requirement for universal quantum computation, it provides a test bed for the evaluation of quantum annealing.

9.1.1 Coherence and control

As quantum annealing strives to use the lowest energy eigenstate of the system, relaxation due to contact with a cold heat bath, i.e., a directed T_1 process, can in principle assist the annealing process. Strong decoherence will suppress any quantum properties, which is why for stronger coupled systems, shorter annealing times are often advantageous. However, the annealing time might still be orders of magnitude higher than the coherence time of the qubits without leading to failure. Realistic devices are also limited by nonuniformity of the qubits and fabrication defects.

9.1.2 Benchmarking quantum annealing

Annealing does not rely on accurate quantum gates, measurements during the computation or exact initializations (in the initial Hamiltonian, the ground state will be one that is easy to reach, and relaxation helps the initialization process), so the typical error rates known from circuit-based quantum computers do not play a big role. It is not necessary to reach the desired state with high probability, since the computation can be repeated and the right result found by comparing energies. For the same reason, even success probabilities below 50% are acceptable.

The most relevant figure of merit of a quantum annealer is the time until the ground state (which is the goal107 of the computation task) is found. This time is dominated by two variables: the running time of a single computation (consisting of initialization, manipulation and measurement) and the number of repetitions. Running the annealer faster results in a lower probability of ending up in the ground state, and thus needs a higher number of repetitions. There exists an optimal balance between both, leading to the lowest overall computation time.

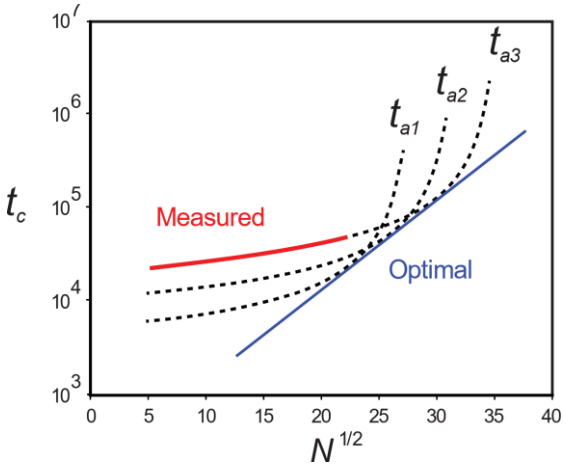

Figure 9.1: Sketch of total time until the ground state is found with desired probability as a function of the problem size. The dotted lines show the performance for several fixed values of per-round run time tf. The blue line shows the optimal result, reached if the run times t_f were optimized individually for each problem size. When measured with a fixed time t_f (for example because of limitations of the annealing device), the slope of the measured curve (red) might indicate a wrong behavior: For small N, the slope is lower than optimal (possibly faking speedup where there is none), for large N, the slope is higher than optimal (which might mask possibly existing speedup) [Ami15]. Reprinted figure with permission from [M. H. Amin. Phys. Rev. A, 92(5):052323, 2015.] Copyright (2015) by the American Physical Society.

A common measure reflecting this trade-off is the time-to-solution (TTS) metric, as explained in [AL17] and [RWJ+14] (Supplementary Materials): It gives the overall time until the ground state is found at least in one of the repetitions with probability p (usually taken to be 99%). It is calculated as $\mathrm{TTS}(t_f) = t_f R(t_f)/\alpha$ where t_f is the time for one repetition, $R(t_f) = \ln(1-p)/\ln(1-p_S(t_f))$ is the corresponding required number of repetitions with a per-run success probability of $p_S(t_f)$ and α is the number of parallel runs that can be performed by devices providing more qubits than required. In some cases, it might be necessary to include initialization and readout times or other time costs that might occur when running the annealer multiple times in series. For current architectures as for example those of current D-Wave machines, these costs are much smaller than the running time and can be neglected. The performance of a quantum annealer is usually compared to classical algorithms by considering a particular quantile q regarding a set of problems, for example the median of $\mathrm{TTS}(t_f)$ for a set of different problem instances and searching for the optimal run time t_q^*, minimizing this quantile. The optimized quantile is denoted by $\langle \mathrm{TTS}(t_q^*) \rangle_q$. High quantiles are usually more informative in terms of scaling, since they include also the hardest problem instances [RWJ+14].

9.1.2.1 Quantum speedup

Quantum speedup is defined to compare quantum devices to classical devices solving the same problem and to find if a quantum computer can beat the performance of a classical algorithm. Especially in quantum annealing this is an important question, since annealers often have the same scaling as classical algorithms, but with different prefactors. Quantum speedup in general is defined as the ratio of the (overall) run time of a quantum annealer $Q(N)$ to the run time of a specific classical algorithm $C(N)$ in the limit of large problem sizes N: $S(N) = C(N)/Q(N), N \to \infty$ [RWJ+14]. A problem with this approach is the definition of the classical algorithm, since it is not always known if a certain algorithm is optimal, and one can only compare the quantum device to the best available classical algorithm.

Another type of comparison is called *limited quantum speedup.* It compares a quantum computer with a classical computer following the same algorithmic approach. For a quantum annealer, the corresponding classical algorithm is for example simulated annealing or simulated quantum annealing: algorithms that run on classical hardware using Monte Carlo simulations. Limited quantum speedup does not prove that a quantum computer is an improvement to classical computers, but nonetheless shows that quantum effects appear and help improve the annealing108108process in a quantum device.

Optimization of the quantum algorithm plays a major role, for example when the optimal per-round run time is shorter than the smallest available time of an annealing device (this time is given by the underlying hardware of the annealing device—even if a solution could be found faster, the annealer will run at least its minimum run time). Then it becomes impossible to determine the optimal overall annealing time $\langle \mathrm{TTS}(t_q^*) \rangle_q$ which is crucial for making estimations for big problem sizes N. The run time needs to be optimized for each N. Fixed values for t_f can lead to a false conclusion, as for small N the total computation time scales only slow with the problem size until N gets too big for the chosen t_f. Then, the slope increases to higher than optimal. Figure 9.1 illustrates this behavior.

Although measurements with fixed (too high) t_f do not represent the large-N behavior of an annealing device, they can still be used to eliminate the possibility for quantum speedup: The slope of the measured curve gives a lower bound to the optimal slope, therefore it is sufficient to show that the measured slope is higher than that of a classical algorithm. Conclusions in the other direction are not possible.

The concept of TTS and quantum speedup can easily be applied to annealers using many-body interactions. However, no such annealers have been built yet and thus no such study has been done.

9.1.2.2 Typical causes for misinterpretation and overestimation

There are many ways of presenting speedup comparisons depending on what the authors want to tell. This section shall give an overview of common situations that might tempt the reader to overrate the performance of an annealer.

Fixed run times

As already mentioned above, although the TTS values for fixed run times lie above optimal, the curves have a smaller slope than the optimal curve for small problem sizes (so, for the problem sizes that can be tested). Hence, if extrapolated to bigger values of N, it wrongly indicates better scaling than the actual optimal curve, as can be seen in Figure 9.1.

Crafted problems

There exist problem instances that are far more suitable for quantum annealing than others. Especially potential landscapes with thin but high barriers are relatively easy for quantum devices. In contrast to thermal hopping (crossing potential barriers classically using thermal energy), for which the probability scales exponentially with the height of the barrier, quantum tunneling depends on the size of the tunneling domain, i.e., its probability scales not only with the height but also with the width of the barrier. Across thin barriers, quantum tunneling is more likely to occur and thereby helps the annealing process to find the ground state faster. However, not all problems can be implemented with such Hamiltonians. So, although comparisons for this class of problems show stunning results [DBI+16], they do not prove that speedup can be observed for other problem instances, especially not that universal adiabatic quantum computing is possibly faster than with classical computers. Furthermore, in many problems tunneling is fast to bring the system in an approximate ground state, but if the task is to find the global energy minimum (which is often separated by a broader energy barrier [AKR10]), also the presence of tunneling cannot bring a significant time reduction.

Low quantiles

Another issue is the choice of the right quantile. Even if the performance of an annealer is determined by implementing a broad set of problem instances, one cannot show all of the results. Providing several quantiles of the distribution can be helpful, but it can also be misleading. Especially low quantiles give information of only the easy problem instances, but a quantum computer should be able to solve all sorts of problems. So, in order to get relevant information on the scaling of an annealer, one should consider the scaling of the highest quantiles, which also include harder problem instances [RWJ+14].

Omitting efficient classical algorithms

In the ideal case, the performance of a quantum annealer should be compared to that of the best known classical algorithm solving the same problem. However, sometimes speedup is only detected in comparison with a certain algorithm, but not with all. One example is the definition of limited quantum speedup: It gives important information on the quantum properties of a device, but not on its computational value. Usually, it is clearly stated what kind of speedup is considered, nonetheless one should always be careful here. Furthermore, it is known that some of the algorithms that outperform annealers for current architectures will soon get ineffective as the devices are improved in terms of connectivity.

9.1.2.3 Further evaluation criteria

Besides the benchmarking available for current architectures, which basically only focuses on the time until the solution is found, future generations of annealers should also be evaluated in terms of their connectivity and control possibilities. Although three-local interactions are said to be sufficient for universal quantum computing with annealers, higher-weight interactions are favorable in order to perform efficient error correction and make the computation scalable. Furthermore, architectures providing more connections between the qubits, for example on a three-dimensional lattice can also overcome the limitation of two-locality since three-local interactions can be mapped to such implementations [LHZ15] with only two-body interactions.

9.1.3 Fault tolerance for quantum annealing

Up to now, there is no scheme known to provide arbitrary fault-tolerance to a quantum annealer, especially, there is no evidence for a threshold. However, there exist several approaches towards error-suppression and some simple error detection and correction ideas. Most protocols aim to increasing the minimal energy gap between the ground state and the first excited state and suppressing coupling to the environment, leading to a higher probability for ending up in the ground state. This energy gap scales as an inverse polynomial in the problem size, so without protection of the gap height, the annealing time would rise polynomially with the problem size, too. Although useful, these methods only suppress errors rather than actively correcting them. Using simple repetition codes, i.e., encoding logical qubits in multiple copies and introducing majority-votes can also provide some ability to explicitly check and correct low-weight errors (i.e., errors involving only few qubits).

None of these methods is a satisfying solution for error correction, since they either do not provide enough error correction ability, or are not scalable, or need many-body interaction and controls that are not feasible with current hardware. This section will discuss various approaches to analyze where they fail and which technological developments might bring them back to relevance. A good overview on the topic can be found in [YSBK13].

9.1.3.1 Error suppression

Energy gap protection

The energy gap protection protocol, as realized in [PAL14] relies on a quantum stabilizer code. By introducing extra qubits, the original qubits can be mapped to logical qubits consisting of several physical qubits. Usually, a simple repetition code is used: Operators are replaced by the sum of equal operators acting on multiple qubits and an extra term in the Hamiltonian, with some extra ancillary qubits is introduced which gives an energy penalty to single qubit flips out of the code space. A code using n times as many qubits as for the original problem can penalize up to $\lfloor n/2 \rfloor$ qubits. The encoding itself already increases the energy scale and thereby also the ground state energy gap by a factor of n. The penalty term additionally lowers the probability of undesired excitations out of the code space. Errors that commute with the penalty term (usually these are phase-flips) are not suppressed. Of course, there are stabilizer codes that can correct all errors; however, these codes require high-weight terms in the Hamiltonian which are experimentally challenging to implement in this scheme. In principle, it is also possible to manually

correct errors by measurement of the stabilizer operators and applying corrective gates, however this is not a technique that is usually available in quantum annealing devices.

Further progress with energy gap protection schemes has been made for minor embedding [VAPS+15]. By introducing penalties that vary with each qubit, corresponding to the respective problem Hamiltonian, the performance could be significantly improved. In the same work, a scalable square code is introduced, which makes concatenated encoding and thereby high error-tolerance (at the cost of an increasing number of qubits) possible.

Dynamical decoupling

In a rotating frame, energy gap protection can also be viewed as modulating the term of the Hamiltonian responsible for coupling to the environment by a fast (depending on the penalty energy) oscillating term so that it cancels out for sufficiently large time scales. Dynamical decoupling takes the direct path to this oscillation, applying a sequence of stabilizer control pulses in time [QL12]. This technique is a well-known method for suppressing errors due to any spurious terms in the system Hamiltonian. However, it does not create an energy difference between code and non-code space, so the code space is not energetically preferred. A big advantage of dynamical decoupling is that also high-weight Hamiltonians can be implemented using many different single-qubit Hamiltonians, as long as the pulses are significantly stronger than the encoded adiabatic Hamiltonian.

Since there are codes that use many two-body interactions and only very few high-weight operators, a combination of dynamical decoupling for the high-weight terms and energy gap protection for all other control might work in some cases. A problem that both energy gap protection and dynamical decoupling struggle with is that they can only rescale the system-bath coupling, a complete suppression would only be possible with control Hamiltonians of infinite energy, or pulses of infinitely high frequency. As the problem size and annealing time increase, the inevitably increasing demands for fault-tolerance will require at least increasing control energies, which will quickly be incompatible with realistic device parameters.

9.1.3.2 Error correction

The easiest way to include error correction to error suppression schemes is to measure the stabilizer operators at the end of computation together with the qubit information and if necessary, to correct the outcome classically. However, besides the fact that errors amplify during long computations, errors occurring during the annealing process might evolve differently in the adiabatic sweeping and become uncorrectable quite soon. This is because the annealing Hamiltonian acts differently on the different subspaces of the code. Correction during the annealing process would require fast quantum gates and measurements, not only in the end. This is not compatible with the general idea of annealing.

Protected Hamiltonians

It is possible to create Hamiltonians that act similar in the non-code space as in the code space, for example if every error maps the ground state of the system Hamiltonian to another eigenstate. This way, it is sufficient to measure only in the end and track the errors back. Again, this is not possible without high-weight terms in the Hamiltonian. A distance d code must have at least d-local interactions. Furthermore, the projected operators must be a sum of an exponentially high $O(2^d)$ number of Pauli operators. It might be possible to lower this number by factoring terms, however this is still an open problem.

Local cooling

Additional resistance against local excitations can be reached by coupling each physical qubit to a low-temperature bath that pulls entropy out of the system. The coupling should be implemented in a way such that the bath can absorb the energy penalty of an unwanted excitation of a qubit out of the code space and put it back to the original state. This only works for local excitations, if one wants to correct higher-weight errors one needs very special Hamiltonian structures that common stabilizer codes do not have, or one needs high-weight Hamiltonians or high-dimensional interactions. However, local cooling can still help to

protect the code space, at least in some way, which, in combination with other error correction techniques might be of some effort. It is possible that novel cooling mechanisms can act on multiple qubits to enact higher-weight protection.

In conclusion, the key point for all error corrected quantum annealing to work is the ability to either implement high-weight Hamiltonians or to include circuit-model techniques like fast measurements and gates into the computations. The latter raises the question if there is an advantage of annealing over circuit-based quantum computing at all. High-weight Hamiltonians might sound like a problem that can be easily solved since high-weight unitary gates are rather easy to implement in circuit-based quantum computation by performing many low-weight gates in parallel. However, there is no comparable way known for Hamiltonians. One approach is using perturbative gadgets [JF08] which create high-weight operators using only weight-two terms. Besides introducing additional qubits, this requires coupling strengths to scale exponentially with the desired weight.

9.2 One-way quantum computing

One-way, or measurement-based quantum computing [RBB03, RB01] is another approach to universal quantum computers using no gates during the computation, but—other than annealing—measurements. However, multi-qubit gates are still required in the preparation of the cluster state that is used as a resource for the computation: In a first step, all qubits are initialized, each in the state $|+\rangle$. Subsequent, CZ gates are applied to pairs of neighboring qubits on a usually two-dimensional lattice. In photonic systems with flying qubits, also higher dimensions are realizable. Note that since this is still a preparation step, the CZ gate may also be performed non-deterministic. Once such a cluster state is created, logic gates are implemented by applying measurements in combination with classical feed-forward. Clifford gates do not need feed-forward as the corrective Paulis can also be accounted for in the end of the calculation. Therefore, all measurements that represent Clifford gates can be performed in a single step at the beginning of the calculation. If we are not restricted to a two-dimensional lattice structure, the state resulting from this first measurement round can also be created directly as a graph state (a state with entanglement connections between arbitrary pairs of qubits). The solution of the encoded problem is found by measuring a certain set of qubits at the very end of the computation, until all other qubits have been measured. Each of these steps is susceptible to errors. Hence, although one-way quantum computing is strictly based on measurements during computation, initialization, gate , and storage errors play a role as well. On a lowest level, initialization and measurement (in an arbitrary basis, so this might include some rotations depending on architecture) accuracies can be assessed in the same way as for circuit-based quantum computing. For gate errors[12] it is sufficient to know the fidelity of the entangling process, since no other explicit gates are applied.

9.2.1 Benchmarking one-way quantum computers

It is important to note that these physical error rates do not directly represent the logical errors in this scheme, since gates are only used in the initialization process and only measurements are used to perform logical gates. Hence, it is desirable to also have a fidelity measure for this logical construct. This can be done by randomized benchmarking (RB) [ATB16], in analogy to circuit-based QC as described in Section 7.4. The protocol can be even simplified using the intrinsic randomness of the measurement processes[13] . Leakage errors (for example photon loss) cannot be characterized with the standard benchmarking protocol. Thus,

[12]Here, gate error means the error of the CZ gates during preparation and not the logical gates that are accomplished by measurements.

[13]Each measurement can lead to two different logical gates, depending on the measurement outcome. Usually this is corrected by adjusting the bases of successive measurements or, in the case of Clifford gates by simply calculating the consequence for the final measurement outcome of the computation. However, this can also be used as an additional source for randomness. As it turns out, fixed measurement patterns are sufficient to reach effective randomized gate sequence. Using this fact, it is even possible to characterize logical non-Clifford gates,as long as the measurement outcomes are all equally probable.

it is important to take this error source into account if it is present. Benchmarking schemes that include leakage errors exist but have not yet been adapted to one-way quantum computing.

9.2.2 Error correction in one-way quantum computing

Possible error sources in one-way quantum computation lie in the preparation of resource states and in the measurements. Imperfections in both processes can be modeled by single-qubit depolarizing noise, i.e., Pauli errors acting on single qubits independently. For faulty Bell measurement (or CZ gates in preparation), both qubits can suffer from Pauli errors, before and after the measurement. Furthermore, a Pauli error can occur while storage and before single-qubit measurements. An additional error source occurring often in photonic implementations is photon loss. This cannot be modeled by Pauli channels.

It can be intuitively understood that there exists a threshold for one-way quantum computation from the fact that it can efficiently simulate any circuit-based computation, including an error-corrected circuit. With the use of a hybrid scheme, as introduced in [ZBD14], connecting small algorithm-specific resource states—in the form of graph states—in a circuit-based manner, a threshold of 13.6% local depolarizing noise can be found for Clifford-only circuits using Shor-type codes [SS07]. With magic state distillation, this can be expanded to universal computation without decreasing the threshold.[14] Clifford-error-correction can be done with moderate overhead: The encoding of a distance d code only requires a d+1 qubit resource state. These resource states might have a complicated underlying graph structure, but any graph state can be either created directly by applying the appropriate CZ gates, or by initially using a (larger) 2D cluster state and performing a round of Pauli measurements to transform the graph. Each elementary building block can already contain a fault-tolerant encoding in the graph structure (error correction works with Clifford-only gates and thus can be fully implemented in the graph without need for additional gates). The blocks are combined sequentially using Bell measurements, which at the same time act as syndrome measurements. It is sufficient to create every block right before it is needed. This reduces storage time and the number of required qubits, since qubits can be reused after measurement.

Depending on the CZ fidelity, creation of the resource states might require additional entanglement purification, for which protocols exist [KMBD06, GKV06]. Even for the modular approach, probabilistic entanglement creation is sufficient (although very resource-consuming).

As an alternative to magic state distillation, non-Clifford gates can also be performed by switching to another encoding and using transversal single-qubit rotations. Switching means connecting a block of standard encoding to a block with different encoding, for example the 15 qubit CSS code (Reed-Muller code, see Section 15.3.3), in which T gates can be implemented transversally, i.e., by single-qubit rotations. The rotations can in principle also be performed by measurements, but they are usually easy to perform directly, so there is no need for a measurement-based implementation. The next building block can then be in the original encoding again, if no other non-Clifford gate follows. The threshold for this method is with 0.64% much lower than for the rest of the code. However, single-qubit gates can usually be performed with very high fidelity; in these cases, universal fault-tolerant computation is still possible with per-qubit error rates of $\sim 1\%$.

The magic state distillation approach allows higher error rates, but this comes at a cost of qubit overhead for the distillation. As long as the magic states have a fidelity of at least 0.8, they can be purified with Clifford operations and Pauli measurements. Thus, with acceptable depolarizing error probabilities of 13.6% and magic state error probabilities of 20%, the threshold of 13.6% is still valid.

A threshold and error-correction for photon loss exists [DHN06b, TB05], but has not been evaluated for the scheme explained above. There are also other protocols for combining smaller graphs, which do not rely on Bell measurement but on using parallel fusion (i.e., compensating the probabilistic character of entangling operations by making several attempts in parallel) [DHN06b, DHN06a].

[14] As noted in [SS07], the noise model considered in that work is oversimplified, because of which this exceptionally high error threshold of 13.6% cannot be directly compared to the thresholds of most error correcting codes, such those discussed in Chapter 8.

9.2.3 Resource calculations

The overhead calculation for error-corrected one-way quantum computation strongly depends on the physical platform and its possibilities. In atom setups for example it is easy to create a big 2D cluster state in a single constant time step. Hence, the bottom-up approach to start with a 2D cluster and create the desired graph state by a round of Pauli measurements suggests itself. On the other hand, flying-qubit implementations like in optics benefit from the freedom to entangle whatever pair of qubits is desired for a certain graph. Here, it would take long times to implement a 2D cluster which will inevitably contain much more qubits and connections.

For each setup, the corresponding method for the creation of graph states needs to be considered, and in a next step, the total resources for running the hybrid code consisting of multiple such graphs can be calculated.

2D cluster states (suited for next-neighbor-restricted qubits)

The number of qubits required for a computation depends on the number of all logical gates applied—including Cliffords—and also on the structure of the computation. We can compare the physical size of the cluster to the size of a picture showing the (logical) circuit diagram that shall be implemented on the cluster. One dimension of the lattice corresponds to consecutive gates: Every logical gate needs a certain number of qubits to be measured along a chain of qubits. The second dimension represents the number of logical qubits operated in parallel: Every chain encodes one logical qubit, multiple chains are arranged in parallel (and multiqubit gates are performed by connecting chains). The chain structure can be achieved by either leaving some qubit positions of the cluster empty, or by disentangling them from the rest of the qubits via measurement. The time for the creation of the cluster state can be constant, independent of its size, in some implementations. After performing all Clifford gates to the cluster (can be done in parallel—feedforward is only needed for non-Cliffords), it has the structure of a graph state. Now all other operations can be performed, with each non-Clifford gate (apart from parallel ones) requiring one measurement + classical processing step.

Algorithm-specific graph states (suited for flying/distributed qubits)

If any graph structure can be created directly by entangling the right qubits, a Clifford-only circuit of n input and m output qubits and arbitrary length or complexity can be simulated with $n+m$ qubits. Each non-Clifford gate needs at least one extra qubit. The creation time for the graph again highly depends on the underlying physical platform, for non-deterministic CZ gates as often used in optics, it scales exponentially with the number of qubits. The graph is designed such that only non-Clifford gates need to be performed, each taking one measurement step. All other gates are encoded in the graph structure.

When using a hybrid (module-based) error correction scheme, the single blocks of the computation are used one after each other and, also in parallel. If qubits are to be reused in later blocks, the computation time for performing calculations on a block and the coupling Bell measurements for each block in a (temporal) row add up. The required number of qubits will be higher than (but in the same order as) the maximal number of qubits in parallel operated blocks, since at the same time, the next blocks already need to be created.

9.2.3.1 What is often not said

The whole graph-state computation itself seems like a very resource-efficient method considering that the calculation can be executed with only measurements. However, many steps need extra resources due to experimental limitations, especially whenever it comes to multi-qubit operations, which cannot be avoided completely (at least at the beginning and during the merging of blocks):

Depending on the fidelity of the CZ gates, extra qubits and time for entanglement purification needs to be considered to meet the threshold. For a non-deterministic creation, the success probability scales exponential with the number of involved qubits, so a high number of attempts to create the desired state is necessary. Furthermore, the Bell measurement might require significant effort (especially in linear

optics [Gri11]) since it cannot always be directly implemented. It can for example be performed by a CNOT operation followed by X and Z measurements on the two qubits, respectively. This again requires on-demand deterministic two-qubit gates, which we originally wanted to avoid with the one-way approach. If the complete graph is to be created at the beginning without adding blocks during calculation, this will result in a huge space overhead and with that increasing error rates due to storage, especially if only 2D cluster states can be created.

9.2.4 Topological cluster states

The topological cluster state [FG09, WF14b] is an encoding similar to the surface code in a special three-dimensional graph state (see Section 8.2.4). The resource state is consumed along one dimension in time by stabilizer measurements. It can in principle be created on-the-fly, however, this requires many parallel successful CZ gates. If this is possible, then only a few layers need to be operated and thus exist in parallel. Otherwise, a huge, entangled 3D lattice is required, which very fast goes beyond the scope of experimental realizable implementations, either in terms of space / connectivity (atoms, solid state) or success probability (linear optics) and especially in terms of error rates due to long storage times.

9.3 Quantum computing based on continuous variables

Most early proposals for quantum computing are based on the concept of using discretized quantum states to represent logical qubits. In the late 1990s, a conceptually different quantum computer based on continuous variables was considered [LB99]. Soon after, continuous variables schemes with an inbuilt fault tolerance were put forth. One of the first that also allow for the active correction of quantum errors is the GKP model [GKP01].

The most common system that features continuous variable states suitable for hosting and manipulating quantum information is the quantized harmonic oscillator (see, e.g., [BvL05,ALS10]). We note that while the harmonic oscillator can be described using continuous variables, such as the quadratures position and momentum (or, equivalently, amplitude and phase), there is also an alternative *discrete* basis of its infinite-dimensional Hilbert space, which consists of energy states.

There are several hardware approaches that make use of the high coherence time of harmonic oscillators. One prominent physical platform employs electromagnetic modes of a superconducting resonator. Many other platforms are possible, such as “flying” photons (see also Section 9.2) or the vibrational mode of a trapped ion. Noteworthy states encoded in an oscillator include *coherent states*, which are eigenstates of the annihilation operator, *squeezed states*, which are eigenstates of superpositions of quadrature operators, and *Fock states*, which are eigenstates of the photon number operator. A detailed introduction to oscillator states can be found in [Fox06]. The perhaps most promising approach of those mentioned above, the one based on superconducting resonators, is discussed in the review paper [MPS+21], and its working principle is circuit quantum electrodynamics (see Section 12.1 and, in particular, 12.1.3). Here, the harmonic oscillator carrying the qubit is a 3D cavity, and universality is accomplished by coupling the cavity to a nonlinear superconducting circuit element, which is often a transmon.

Different qubit embeddings into the continuous state space of harmonic oscillators have been proposed. To consider an example, the analog of the standard $\{|0\rangle,|1\rangle\}$ basis and its dual $\{|+\rangle,|-\rangle\}$ basis, respectively, can be chosen to be eigenstates of the quadrature operators position and momentum. Similar to the action of the Hadamard gate, an eigenstate of one quadrature can then be transformed to an eigenstate of the other quadrature by a Fourier transform. In the same manner, analogies for all Clifford gates can be found for continuous variables by Gaussian operations (non-Clifford gates require photon-number resolving operations/measurements or other nonlinear effects), with the addition of extra variables, creating a continuous set of continuous-variable operators out of one qubit operator.

Continuous-variable entanglement, which is required for universal quantum computation, can be implemented by a multi-mode squeezing process, as facilitated using nonlinear media. Multiple modes could be stored in a single cavity (or waveguide), and so a potential advantage is that even big systems do not necessarily need much space, but instead good frequency-resolving devices. On a different note, creating ideal quadrature eigenstates would require an unphysical application of infinite squeezing,

because of which only approximate eigenstates can be realized. This is a first indication that the application of error correction is essential in this protocol.

At a lowest level, one can estimate the accuracy of quantum gates by measuring the amount and direction of achievable squeezing, or the general distribution of a state in phase space, which can be done analogously to process tomography with homodyne detectors.

9.3.1 Overview of error correction for continuous variables

Error correction protocols for Gaussian states that only use Gaussian operations cannot correct Gaussian errors.[15] This statement, proven in [NFC09] restricts fault-tolerant continuous-variable quantum computing to codes using either non-Gaussian computational states [GKP01], non-Gaussian operations (as in the case of cat codes, see below) [RGM+03], or codes that are only tolerant to non-Gaussian errors [vL10]. However, typical error sources in experiments include also loss and thermal noise, which are both Gaussian.

In the context of continuous variable codes, one does often not refer to an error threshold. This is in part because the encoding into continuous variables implies the usage of a single harmonic oscillator, which is, of course, not straightforwardly scalable. Error thresholds play a role when these codes are concatenated with regular codes. A valuable figure of merit determining whether usage of a code pays off is the lifetime of the oscillator's quantum states that are used as logical qubit states.

The first code introduced for continuous variables [Bra98] was a Shor code, which was obtained by mixing ancilla modes via beam splitters. This code was only using Gaussian methods and thus also could only *correct* non-Gaussian errors. More promising are the GKP codes and Schrödinger cat codes, both of which are described below. Other error correction codes for continuous variables include the binomial codes [MSB+16] and rotation symmetric codes [GCB20].

9.3.2 GKP codes

The well-known GKP encoding [GKP01] proposed by Gottesman, Kitaev and Preskill encodes information in a discrete subspace of non-Gaussian states. Besides a rather high threshold condition and a preference for small errors occurring continually (having low efficiency for rare but large errors), it needs a highly nonlinear interaction for state preparation. For example, such an interaction can be provided by the cross-Kerr effect in nonlinear media.

To also enable the correction of larger errors, the code must be concatenated with other error correction codes. The states needed for GKP can also be approximated by highly squeezed states, and the deviation from a perfectly squeezed state can be modeled as a gate error. This way, for a cluster-state implementation, a threshold for the squeezing strength was found to be 20.5 dB [Men14], when using the GKP scheme for error correction. Another study concatenates the GKP code with the toric code [VAW+19]. GKP codes have just completed level C right after the deadline for this study, see Section 8.5.4.

9.3.3 Cat codes

The cat codes [CMM99,LKV+13,OPH+16] encode a qubit using superpositions of coherent states in a quantum harmonic oscillator. A coherent state is usually specified by a complex number $\alpha = \sqrt{N}\, e^{i\phi}$, which is made up of two central defining quantities, the number N denoting the average photon number (or energy), and the phase ϕ. Such a state behaves in certain ways like the eigenstates of a classical harmonic oscillator. For instance, the coherent-state expectation values of position and momentum undergo the same sinusoidal oscillation as in the classical case. The probably most well-known example of a coherent state is the light emitted by lasers. For these reasons, coherent states are often described as semiclassical states.

[15] A Gaussian state is any state with a Gaussian characteristic function, i.e., with a Gaussian distribution in phase space. Typical Gaussian states include vacuum, coherent and squeezed states. Gaussian operations are operations due to Hamiltonians which are at most quadratic in the quadrature/ladder operators. They map Gaussian states to Gaussian states.

However, *quantum superpositions* of coherent states are true quantum states and are thus a sound primitive for quantum computing.

A Schrödinger cat state, or simply cat state, is a superposition of two diametrically opposed coherent states with equal photon number, one defined by α, and the other defined by $-\alpha = e^{i\pi}\alpha$. The overlap of these two states decreases exponentially in the average photon number $N=|\alpha|^2$, because of which this overlap becomes almost negligible already for moderately large photon numbers (roughly $N > 10$). This property motivates the name *Schrödinger cat state*, since these states are in a superposition of the distinguishable α and $-\alpha$ coherent states, like the cat that is in a superposition of being dead and alive in Erwin Schrödinger's well known thought experiment. The qubit states 0 and 1 of the cat codes are wave functions with even parity (consisting of only even-number photon states) and odd-parity (odd-number photon states), respectively. For example, using the Dirac notation, the cat state $|\alpha\rangle + |-\alpha\rangle$, corresponds to even parity, while the cat state $|\alpha\rangle - |-\alpha\rangle$ corresponds to odd parity. Cat codes are designed for protecting against the loss of photons, which usually accounts for the most important error channel of any oscillator state.

Photon loss can lead to both bit flip errors and phase flip errors, which can be detected due to a change in parity. When increasing the number of photons, N, the likelihood of bit flips decreases exponentially in N, while the likelihood of phase flips *increases* polynomially in N. As a result, a strong asymmetry of error rates, also called a noise bias, can be achieved by choosing large average photon numbers. This bias is limited by the acceptable rate of phase flip errors, as well as by the number of achievable photon numbers in a given experimental setup.

As described above, in the case of superconducting 3D cavities, universal control is achieved via coupling the cavity to a nonlinear element, which is often a transmon qubit [HRO+16,MLA+14].]. This coupling also enables a parity measurement, which, as also mentioned above, is used to detect errors due to photon loss. Most correction schemes of photon loss errors, however, do not reverse the loss of a photon, but rather consist of a remapping of the basis states. For this type of active error correction, the numbers of distinct coherent states used for the qubit states 0 and 1 depend on the proposal, including two states [CMM99] (defined by α and $-\alpha$), four states [LKV+13, MLA+14] (α, $i\alpha$, $-\alpha$ and $-i\alpha$), and more states (also in this case, all states have the same average photon number N) [BvL16,LZA+17].

While the loss or addition of a single (or any odd number of) photon(s) inverts the parity of a cat state, any even-number photon change maintains that parity. There is a second prominent type of cat code operation that makes use of this fact. The proposals for this type of operation are based on special interactions between the host cavity and its environment, which correspond to engineered two-photon loss mechanisms and two-photon driving. This can be realized by driving the harmonic mode in a way that the error-causing single-photon changes are suppressed. The result of this engineered drive is a unitarily evolving steady subspace with a fixed average photon number, in which the desired cat states can be stabilized for sufficient time to carry out a computation. This method can be compared to resonantly driving a damped classical harmonic oscillator, which results in a steady-state time evolution. The perhaps most notable works in this direction realize two different methods for this goal. The first falls under the scheme of holonomic quantum control [ASKP16], the other employs driven dissipative evolution [PBB17]. The above methods ensure the noise bias only in idle mode. Thus, another crucial ingredient to this scheme is the ability to perform bias-preserving operations, which was worked out in [PBB17,GM19]. The viability of this approach has just been experimentally confirmed.

9.3.3.1 Explicit performance analyses of cat qubits

Lately, several theoretical studies explored the role of cat qubits operated using superconducting 3D cavities as a high-quality alternative to discrete qubits on the physical level for regular error correction codes. The operational foundation of the methods outlined below is given by the second paradigm described above in Sec. 9.3.3, which is characterized by creating a stabilized subspace with a fixed photon number using a two-photon loss mechanism and two-photon driving.

Gouzien et al. analyzed the task of solving the discrete elliptic curve logarithm problem by using cat qubits arranged on a two-dimensional lattice with nearest-neighbor connectivity [GRR+23]. Assuming rather realistic device specifications for each cavity carrying a cat qubit, they find that a total of roughly 120,000

physical qubits suffice to solve the 256-bit elliptic curve logarithm problem using Shor's algorithm within 9 hours.

The accompanying strong noise bias allows to carry out a quantum computation for a duration that is given by roughly the lifetime of the qubit (or the inverse bit flip rate), during which only the high-rate phase flip errors need to be corrected. Because of the focusing on a single error type, a simple resource-efficient repetition code is used, which had been introduced earlier in [GM19]. This repetition code does not have an error threshold, because of the asymmetry of the cat code: the only way to lower the bit flip rate is by raising the number of photons kept in the cavity, which, as described in 9.3.3, increases the phase flip rate. However, the authors argue that sufficiently low logical error rates can be achieved so that practical problems can be solved.[16]

At this point we remind the reader that 3D cavities are more space-demanding than the usual, two-dimensional transmons. If we estimate the volume of a single cavity to be 100 cm^3 (taking approximate dimensions of a 3D cavity from [MPS+21]), or 0.1 liter, the minimal volume required for the estimated 120,000 3D cavities of [GRR+23] amounts to 12,000 liters, which means that interconnecting at least several hundred regular-sized cryostats would be required to house the entire setup. This poses challenges on multiple fronts, such as the high-fidelity connection of cryostats and the concomitant limited connectivity between qubits of different cryostats.

Another recent proposal combines cat qubits with classical LDPC codes [RGL+24], which constitutes an improved version of the repetition code and thus reduces resource overhead compared to that of [GRR+23]. We note that like the repetition code, these classical LDPC codes correct only one type of error, because of which they have the same limitation of lacking an error threshold.

The authors put their work into perspective: Besides comparing their results with the surface code and the cat qubit implementation of [GRR+23], they also contrast their code against the recently proposed code [BCG+24] designed for regular superconducting qubits, described in Section 8.2.5.1. The figure of merit used for this comparison is the required resource overhead for operating the system at logical error rates of 10^{-8}. In terms of physical qubit numbers, for all three new codes they find an order of magnitude improvement compared to the surface code. While the physical qubit numbers of the codes [GRR+23,BCG+24] are roughly equal, the high-rate LDPC code of [RGL+24] gives an additional factor-2.5 improvement (approximately). Two important qualitative differences between the newer codes are also pointed out. First, fault-tolerant operations can be carried out when using the two approaches based on cat qubits, whereas no such protocols are known for the code of [BCG+24]. Second, the two cat-qubit based codes (like the surface code) do not require long-range connectivity on a 2D grid, which makes them more compatible with the current technological status of superconducting circuit technology. However, as commented above, we emphasize again that the space requirement of 3D cavities holding cat qubits may be a major obstacle to rapid engineering solutions for such large qubit systems.

If it is possible to operate large numbers of cat qubits in this strongly asymmetric error scheme, the significant advantage is that essentially half of the error correction efforts will be accomplished directly on the hardware level. We conclude that the development of cat qubits based on superconducting 3D cavities may unlock a great potential towards lowering qubit overhead that is currently unrivaled by other types of quantum computing, and so this platform is poised to catch up in terms of its development status.

[16] As stated in Appendix A of [RGL+24], logical errors of 10^{-31} are within reach, if each cat qubit is operated with an average of 38 photons, which corresponds to an error bias of 10^4.

PART IV: Assessment of platforms

This chapter describes and evaluates leading platforms of quantum computer implementation according to the evaluation scheme introduced in Section 3.3. Differing from the previous edition of this study [WSL+20], it disregards some platforms that are abandoned, in the sense that there was no technological development in recent years.

After a general introduction in Chapter 11 we have categorized the platforms according to the nature of the carrier of information: Degrees of freedom of solid state systems (Chapter 12), isolated atoms held in vacuum or a dilute gas and photons (Chapter 13). Within those chapters, subcategories are laid out according to the host material (Chapter 12) or the charge of the atom (Chapter 13). Each of these sub-chapters starts with a short description and an introduction to the key jargon, followed by evaluations of the status according to our evaluation scheme. Each of the chapters concludes with a description of technological and operational challenges anticipated during scale-up.

10 Global operational criteria for quantum computers

While still elusive, quantum computing research is far enough advanced to project and speculate about operational criteria and requirements for a scaled-up machine. This can be driven by experience gained from classical (super-) computers as well as from the bottom-up operational challenges that were collected in the previous chapter. These criteria are separate from the mid-level requirement for operating quantum error correction. We would like to introduce three classes of operational issues:

10.1 Extensive parameters

An attractive way to project operation is to ask how much of a given resource is required per qubit. This is not easy to answer, and the answer should leave space for technological progress. In particular, the last two layers are expected to develop dramatically with the entry of industry and engineering in the field—current setups from research laboratories are optimized for flexibility of experimentation, not integration.

10.1.1 Scales of extensive parameters

As a preliminary consideration, it seems necessary to measure the effort per qubit on four different scales.

The bare qubit

When choosing a platform, a degree of freedom to encode a qubit, there is a certain scale that even most imaginative engineering cannot overcome, posing a fundamental (and often unreachable) bound for the quantum computer. This is the average diameter of a single ion or atom, the nuclear radius in NMR, the size of a superconducting qubit, the size of a quantum dot are bare qubit scales.

The unit cell

Even when building a simple quantum register, a qubit does not go alone. It needs to be addressed by controls (if controls are local, this requires space) that reduce crosstalk (the effect of controls aiming at a specific qubit also affecting other units), it potentially needs to be held in place by external fields. This needs to be treated differently from the bare qubit as different design choices lead to different unit cells. The 3D transmon is, e.g., very small, but needs to be operated in a large-machined cavity, different from the planar transmon which thus can be packed much more densely. Unit–cell limits are described in Sections 13.1.2.1 and 13.4.8.

The periphery layer

The controls and read-out attached to qubit unit cells need to be externally connected to electronic and optical elements. They are typically operated under less demanding conditions than the qubits hence requiring different resources. Also, these elements are often shared between platforms - for example microwave electronics for spins in semiconductors and superconducting qubits or laser systems for neutral atoms and ions. Examples are described in Sections 12.1.3 and 13.4.8.

Infrastructure

Given the strong need for protection of quantum computing systems, they sit in some type of infrastructure providing suitable operating conditions. For semi- and superconductors these involve cryogenics, for atomic systems they include high vacuum and vibration-isolated optical tables. Here, a critical point occurs when the size of infrastructure units in not sufficient and multiple units need to be connected. Infrastructure challenges are described in Sections 12.1.3, 13.1.2.1 and 13.4.8.

10.1.2 Size

An obvious extensive parameter is the size of a qubit. While usually this is a volume, unit cells can also be quasi 1-dimensional (as in the linear Paul trap), 2-dimensional (as in chip-based superconducting and semiconducting circuits) or also 3-dimensional. In most cases, size is dominated by the periphery layer. In solid-state qubits, the long wavelength of microwaves makes microwave elements centimeter-size, in atomic systems, optics miniaturization is a major challenge.

10.1.3 Power consumption

While quantum computing is reversible, a lot of operations around it are not, so the power consumption per qubit is an issue. Currently, the high-power elements are cryogenics and lasers, which belong to the infrastructure layer and probably do not increase with the number of qubits until reaching the threshold of the need for multiple infrastructure units.

10.1.4 Power dissipation and temperature stability

Next to the power being consumed, it is a separate question where this power is dissipated and how that influences the thermal management of the system (and how much cryogenics are required). Unwanted heating, e.g., plagues semiconductors, where the effective electron temperature is often ten times the temperature of the cryostat. One needs to discriminate power consumption by the means of cooling:

- room temperature: A/C system
- 77 K: Liquid Nitrogen
- 4 K: Liquid He
- 1 K: Liquid ^{3}He
- mK: ^{3}He-^{4}He mixture

and calibrate the amount of coolant needed. Note that some of these coolants (specifically nitrogen) are typically consumed during cooling whereas Helium can be preserved in a closed cycle.

10.1.5 Cycle time

Again, one would like to know the clock speed of the quantum computer as given by its slowest ingredient. This critically depends on the technology being used - it often is believed to be the two-qubit gate but in practice it often is qubit reset, which even takes a full relaxation time or extra overhead for classical reset.

10.1.6 Classical data flow

This issue is most pressing in connection to error correction: As the code and control layer of a quantum processor are classical, one is faced with the need to process data fast and close to the device in a way that grows with computer size. In particular, on low-level, this is done with cryogenic electronics, which impacts periphery space and power dissipation.

10.1.7 Reliance on rare materials

Some qubit systems are based on rare materials on some layer. For example, isotopically purified Si without nuclear spins is generated in a laborious process from natural Si. A critical ingredient is ^{3}He that is needed to reach low temperatures. With reports on the shortage of natural ^{4}He probably exaggerated, the non-natural ^{3}He is in short supply already. It has been generated as a by-product of nuclear warfare, specifically hydrogen bombs containing tritium. The little that is generated from US nuclear stockpiles is used for radiation detectors by the US, making ^{3}He unavailable and prohibitively expensive. A vast quantum computer based on ^{3}He would likely require a designated nuclear source for ^{3}He.

10.1.8 Vacuum

Some qubits need to be operated under ultrahigh vacuum. Trapped ions, e.g., use their motional degree of freedom for quantum gates which is at odds with collisions with gas molecules. Given outgassing of materials, one needs to ask to what point vacuum infrastructure can be enlarged.

10.1.9 Production speed

Computers can be scaled based on mass-production. With extreme technology as quantum computers currently made under research conditions, this needs to be addressed. Notable challenges include the enormously long production time for cavities in neutral-atom cavity QED, the difficulty in designated single-dopant implementation in dopant spins in semiconductors. At some scale, also the different speed in mask-production in (parallel) optical lithography as used by the current classical semiconductor industry versus (serial) electron-beam lithography used to make nanostructures needs to be taken into consideration.

- Extensive parameters: numbers characterizing a quantum computer that grow roughly linear with the size of the machine.
- Critical parameters: challenges that need to be overcome in scaling. Operationally, these challenges become critical faster than linearly when scaled.

Further descriptors: Here we look at descriptors that are not growing dramatically and are not critical, but that characterize the operation of a quantum computer and its suitable environment.

10.2 Critical parameters

There are a number of parameters that are mere inconveniences in small laboratory scale systems but that can become prohibitive when scaling up.

10.2.1 Stability

How long can a quantum computer be operated before it needs to be reset/recalibrated? This can be based on effects like the loss of qubits - weakly bound neutral atoms in optical lattices tend to disappear after some time. This can also be due to slow drifts in parameters that occur in imperfectly thermalized systems - it is known that some parameters of Josephson junctions drift on the scale of the day. A crucial example is described in Section 13.2.2.

Unless accommodated in error correcting codes suitable for these problems, these issues can be lethal: Losing a qubit with probability p per unit time means losing a qubit with probability $1-(1-p)^N \leq Np$ in a large quantum computer per unit time, effectively limiting algorithm run-time to $(Np)^{-1}$ time units.

10.2.2 Yield and scatter

On a level lower than instability, one needs to make sure that the production of a quantum computer is reliable: Are all devices close to their design parameters, are all of them performing on a sufficient level? Can good/bad devices be selected before systems integration? How does this limit the size of a module? For example, when qubits cannot be locally controlled but need to be addressed by frequency selection, it is necessary to produce them at the right frequency—is that reliable? This plays a role, e.g., in superconducting flux qubits where some operation parameters depend doubly exponentially on hard to control fabrication parameters, see also 128.

10.3 Further descriptors

Albeit the previous criteria seem to control most of the deciding criteria to operate a quantum computer, it makes sense to reflect on the overall device. How big is it? Can it be operated overground or in a tall building (i.e., does it need to be insulated from vibrations)? Can it be operated by general data center staff?

10.4 Articulated architectural extrapolations

With the increasing maturity of platforms, extrapolating full quantum computer architectures has become a reasonable proposition - what in fact this study addresses in other chapters. Some platforms have been very early in this - the Kane quantum computer [Kan98] - and needed to correct their assumptions about experimental capabilities. Others are rather hesitant - such as the Josephson qubit community which did not want to repeat the experiences of the classical supercomputing community of the 1980s and 1990s. In this period, rapid single flux quantum (RSFQ) was promised to revolutionize classical supercomputing by allowing for fast clock speeds - which never materialized due to challenges in fabrication, large element size requiring many clock cycled for communication, and supercomputing demands requiring parallelism rather than clock speed. Also, we expect that confidential studies exist, in the form of detailed research proposals and in the form of company strategies. Very recently, two of these studies came out of the IARPA-LogiQ program, which has corresponding milestones—and more of these could come out of the remaining LogiQ teams (with two superconducting qubit teams, IBM and TU Delft, and two ion trap teams, Duke and Innsbruck).

A blueprint for a largely microwave based ion-trap quantum computer has been published recently [LWF+17]. It argues that this is possible given that there is no prohibitive challenge of laser adjustment. It concludes that, performing a 2048-bit number Shor factorization will take on the order of 110 days and require a system size of $2 \cdot 10^9$ trapped ions. Shor factoring of a 1024-bit number will take on the order of 14 days. They will require almost the same number of physical qubits because the required pace of the ancilla qubit generation is the same for a 2048-bit and a 1024-bit factorization. Trapping $2 \cdot 10^9$ ions will require 23 × 23 vacuum chambers occupying an area of ca. 103.5 × 103.5 m^2 . Its most surprising result is the power consumption for the surface traps that are made out normal conducting metal, leading to a power consumption of about 1000 W per module, of which this processor requires about 5000, leading to a 5 Megawatt power consumption, which is less than a present-day supercomputer. The paper points on routes with better gates to bring down these numbers.

A competing analysis of the more standard optical ion trap architecture was posted in May [BXN+17].

Other than the first one mentioned, this paper is much less concrete in its conclusions. It is a more detailed version of much of our ion trap chapter. Most notable is its analysis of the color code (rather than the surface code) for trapped ions. The color code has a somewhat lower threshold than the surface code and requires longer parity measurements (which are well adapted to the Mølmer-Sorensen gate), but it is less complicated to compute on it. The authors also state their expectations for next-generation gate errors, which are all expected to improve by more of an order of magnitude and land somewhat above 10^{-4} .

The book chapter [DSMN16] thoroughly analyzes a photonics quantum computing architecture that uses atoms as nonlinearity and proposes concrete modules for achieving that within topological error correction for cluster states, which is its centerpiece. It estimates an error threshold of around 0.6% but does not extrapolate overhead from the performance of this platform as it is very far above that error rate.

What is the significance of these extrapolations? First of all, the fact that they can be made and have a finite result allows to gauge the distance to a viable architecture and to identify the most mission critical developments. As far as technology is concerned, they are optimistic that some quantitative progress can be made and that scaling up has no unpleasant surprises (e.g., that device performance is not affected by integration in a large machine), but also pessimistic as they do not anticipate breakthroughs that sill can change the field. So, they are probably limited predictors of the *science* of building a quantum computer, but good guides to *engineering* it.

11 Quantum technology and computing platforms

This part summarizes physical platforms for quantum computing as well as algorithms that are relevant for cryptography. It identifies main criteria for the successful operation of a quantum computer.

The field of physical realizations evolves at a quick pace and produces an ocean of literature as well as large conferences as a result. Also, given the attention quantum technologies in general and, in particular, quantum computing receive currently, there is a lot of noise created including some research fields trying to relabel themselves. So doing a survey is an impossible task if it is not guided by some clear principles. Here is what we have applied:

1. A serious quantum computing candidate needs to have at least one experimental activity associated with it that identifies the potential existence of a qubit, i.e., check at least the first DiVincenzo criterion (see Section 6.2). Pure theoretical considerations without any experimental activity would not make the cut. Furthermore, there are platforms in which recent developments show that the hope of near-term evolution to a functioning quantum computing device is unfeasible. Therefore, we will disregard “exotic” candidates because it is very unlikely that they can catch up to the main candidate platforms.
2. On the same token, an experiment that is not linked to any theoretical proposal how to meet the DiVincenzo criteria in their simplest, non-quantitative form at least in principle, would also be discarded.
3. Quantum technologies are classified in four broad categories originally formulated for the EU [QE16] but now more broadly accepted: sensing and metrology, communication, simulation, and computing. Clearly, this work singles out computing. The dividing line to simulation is not razor-sharp, specifically in the area of digital quantum simulation one essentially runs a specialized quantum algorithm. Also, the EU classifies some approaches, notably quantum annealing, as simulation, even though they can have some cryptographic relevance, so annealing is included here. When describing platforms, we focus on their quantum computing aspects, not on the others - for example we do not describe the application of NV-centers in diamond in sensing of magnetic fields and forces, neither do we describe the latest atomic clock technology based on trapped ions.
4. A large part of quantum computing is driven by (in the words of Andrew Steane [Ste03, BKCD02]) climbing Mount Scalable—being governed by quantum error correction in needs to improve operation and include more and more qubits. We have tacitly assumed that qubits will ultimately be based on an error correcting code. This field was dominated by the topology-inspired surface code [FFSG09, FMMC12], as it provides high error thresholds and only requires nearest-neighbor qubit-qubit coupling. However, newer developments show that low-density parity check (LDPC) quantum codes only need “a constant fraction of physical qubits devoted to error correction” [BDG+22]. However, these are still based on topological surface codes. For the sake of this survey, error correction could also be done by other popular codes such as color codes or concatenated Calderbank-Shor-Steane (CSS) codes. It needs to be noted that these codes are assembled from physical qubits that are separate functional units - they are agnostic to the type of qubit used as long as their requirements are met. A few exceptions are mentioned explicitly:
   i) It is believed that topological qubits—qubits that intrinsically, in their microscopic physics realize topological protection—need much less error correction
   . ii) In quantum annealing, the role of error correction is under debate—some of its proponents highlight that an intermediate amount of classical noise may actually be beneficial.
   iii) Schemes like cluster state quantum computing are currently in their infancy and connecting them to error correction is certainly a long-shot.
5. The plurality of platforms has some resemblance to the early classical computer age, where implementations went from mechanics to electromechanics, vacuum tubes, solid-state transistors all the way to integrated circuits. This is clearly the stage of the field right now. Even more: Some platforms are quite pluralistic internally, for example semiconductors, whereas others that are more mature are at the same time more focused, such as ion traps. So, chapter length is a poor indicator for the quality of a platform.

The description of platforms is driven by sorting and categorizing at least as much as by finding them all. We have ordered them by what we believe (in no strong contradiction with the rest of the community) an order of decreasing potential. This latter ranking has to be taken as preliminary and is based on the European quantum technology roadmap as well as funding priorities. In the end of each chapter we rank the platform in terms of the evaluation system from Part I. We also needed to make a few deliberate choices that could have been done otherwise: NV centers in diamond are part of the semiconductor chapter even though they are sometimes called nature's trapped ions and borrow a lot of ideas from ion traps. Topological qubits are no longer considered as a serious quantum computation candidate.

Quantum computing continues to have a strong impact on algorithm design, and cryptanalysis remains one of the most prominent potential application domains of quantum computing. It is interesting to observe that more than twenty years after Grover's algorithm and Shor's algorithms have been published, the research community is still working on analyzing their quantitative impact on the cryptanalytic landscape. There are commonly two different aspects to consider when looking at quantum algorithmic innovations in cryptanalysis. First, there is a "true quantum" portion of the algorithmic innovation, which can allow a (sometimes dramatic) speed-up over classical solutions, *assuming appropriate access* to the classical problem description. Second, the classical problem description—which can include things like the arithmetic in a particular cyclic group or the details of a hash function for which a collision is sought—influences the exact operations that need to be mapped to the quantum hardware. The latter aspect can to a wide extent (though not entirely, as elementary operations and cost measures will usually differ) be discussed within a framework of classical reversible computing. Notwithstanding this, the complexity of this "classical portion" is critical for and, can in fact dominate the overall running time of a quantum attack. This part focuses on a qualitative discussion of pertinent quantum cryptanalytic algorithms, and it should become clear that the current implications of quantum computing for symmetric and asymmetric cryptography are very different.

Operational criteria and "scale up science" are much harder to come by, given the tendency of humans to report successes rather than challenges. They were mostly identified bottom-up but then summarized in the end at a workable executive level. Also, there is no shortage of actors and research groups so our main task was to sort them.

A good overview of how advanced a platform is can be given by the number of entangled states as shown in the Figure 11.1.

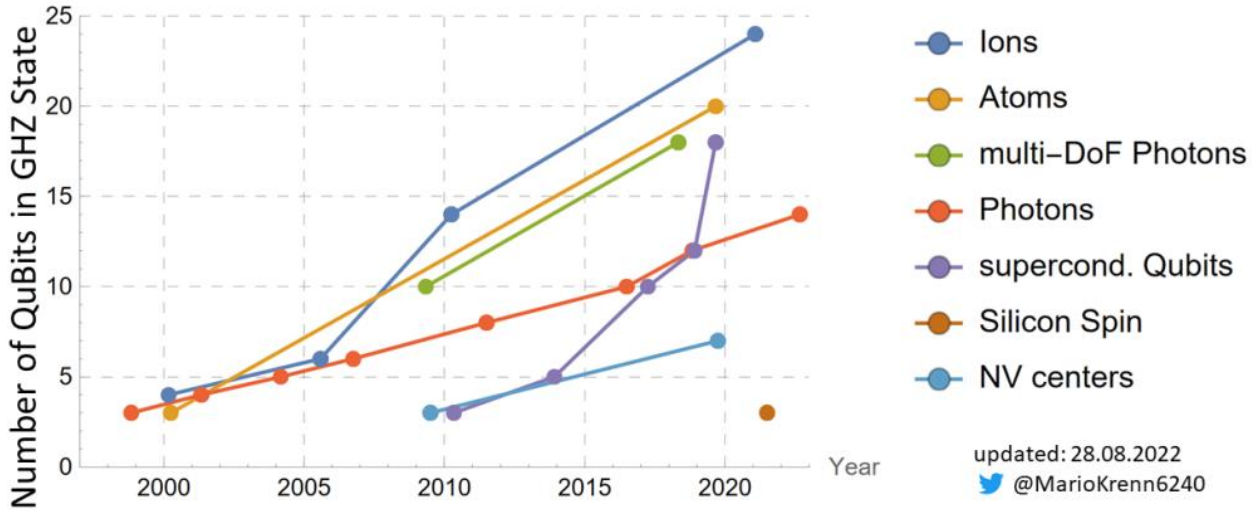

Figure 11.1: Number of qubits in GHZ state that have been realized experimentally. The usage of the figure was granted by Dr. Mario Krenn and is taken from [Kre22].

11.1 Other measures

We list in Chapter 12 and 13 known world-records in gate times, fidelities, and coherence, sorted by platforms. This is a fast-moving target and got updated during the study. Ultimately, the most mature

platforms are better characterized by operation fidelities and compatibility with error correction. We have chosen those measures as they allow us to extrapolate to fault tolerance.

For NISQ, there are new measures of the capabilities of a quantum computing unit mostly driven by IBM which include Quantum Volume (The QV method quantifies the largest random circuit of equal width and depth that the computer successfully implements [QISKITDOC]), which takes into account connectivity of the processor. This is a volumetric measure in the sense that if one of the three key ingredients qubit number, fidelity, and connectivity, becomes inadequate, the whole measure reduces. It is however a rather coarse estimate for our purposes to highlight square circuits – in a situation where we need 1012 Toffolis on 2049 qubits. Also, the absolute execution time does not play a role in this measure. New measures, also from IBM, are Circuit Layer Operations per Second (CLOPS) [WPJA+21]. Here, for the same circuits, a normalization to time is introduced, so machines of comparable quantum volume can be compared along their absolute runtimes – yet still insisting on square circuits . A new measure introduced by IBM, the layer fidelity, is a scalable combination of a volumetric measure and randomized benchmarking and mostly suitable for NISQ [MHP+23MHP+23].

IonQ has introduced the measure of algorithmic qubits [IONQ] . This differs in two ways: It focuses on more skinny circuits (with N^2 entangling gate layers on N qubits) and rather than picking random circuits it chooses application-ready circuity from a library from QED-C [LJV+21], the quantum economic development council of the USA. While the latter is a way to certify NISQ-readiness, it contains no guarantee of hardness (as is the case with random circuits). More skinny circuits make this a better proxy to the needs of cryptanalysis as the quantum volume, yet it cannot replace our fault-tolerance extrapolation. The benchmarking team at Sandia has put out a more global discussion on suitable quantum computing benchmarks, which is fully compatible with this study PRY+17HNG+24; PYB+24].

11.2 Outdated and exotic qubit candidates

As noted above, at this point in time, several qubit platforms do not fulfill the minimum criteria to be relevant for this study and/or had their development stalled for many years. Some of these have been discussed in earlier versions of this study, see [WSL+20], but have been removed in an effort to focus on the platforms that are most viable at this time. Most notable among these are *molecular approaches*, which are not scalable and therefore no longer of major interest, and *electrons captured on liquid helium*, which are in a premature state.

12 Solid state platforms

12.1 Quantum computing based on superconducting qubits

Superconducting integrated circuits based on Josephson Junctions are a solid-state based platform of quantum bits. They are viewed as one of the leading realization candidates by the US government and the EU quantum flagship [NIS16, QE16].

This platform is being pursued as a platform for both adiabatic quantum computing / quantum annealing and quantum circuit-based quantum computing. Its basic unit, the qubit, is currently based either on the transmon or the flux qubit design. Coupling and control is mediated through microwave transmission lines, which can also serve as interfaces to other platforms.

This technology is widely pursued by academic, government, and commercial actors.

12.1.1 Basic notions and terminology

Superconductivity, the property of certain metals to conduct electricity without resistance and completely expel magnetic fields, is a macroscopic quantum phenomenon that occurs at low temperatures. In current research on superconducting quantum bits, the materials used are conventional superconductors—elementary metals and alloys—in which superconductivity is well understood. Unconventional superconducting materials including high-temperature materials are currently not pursued for quantum computing in this platform but play a role in topological quantum computing, see respective chapter. The most common materials are Al and Nb which superconduct below T = 1.2K and T = 9.3K respectively. Hard superconducting alloys such as NbN and InAs-Al play a minor role. This platform naturally operates at low temperatures and electrical charge there is carried by pairs of elementary charges, Cooper pairs. Superconductivity allows to transmit elementary units of information without losses and is thus important for maintaining quantum coherence.

The key element in these circuits is the Josephson junction. This is a weak link between superconductors made of non-superconducting material, primarily realized as Josephson tunnel junctions from electrical insulators. Consistent with the need for superconductivity, this is a reactive (non-energy-dissipating) element which, unlike the commonly known capacitor and inductor, is classically nonlinear. This nonlinearity leads to a non-equidistant energy spectrum that is crucial to selectively address quantum states as computational (qubit) states.

Contact with these circuits—control and readout as well as inter-qubit coupling—is made using electromagnetic fields in the microwave frequency range. This connects to the more established field of classical superconducting electronics that has both high-speed computing and precision sensing applications.

12.1.2 Various types of superconducting qubits

We group qubit types into different categories based on the original qubit design.

A) Charge qubit derived designs

Charge-qubit derived circuits have been developed from ultra-small circuits showing strong charging effects even with elementary charges, such as single-electron transistors. These devices were originally investigated for metrological applications. As they are known to be very sensitive to charge noise, and as charge noise in manufactured nanostructures is a known problem that so far could not be solved, design evolution in these systems is driven by the need for immunity from slow charge noise. The different evolutionary steps preserve their circuit topology. They are different in the ratio E_J/E_C where E_J/E_C describes the Josephson coupling energy for charge exchange and E_C the charging energy of a single Cooper pair. If this ratio is small, the computational states of the system can be well separated by electrical charge, which also means that they are most sensitive to low-frequency charge noise. This number also gives an

indication of geometric size: The Josephson coupling is proportional to the junction area whereas the charging energy is proportional to the inverse capacitance (which in turn is proportional to junction area), hence this ratio is approximately proportional to area squared.

Planar transmons

The transmon [KYG+07] pushes E_J/E_C to even larger values (i. e. $E_J/E_C \simeq 50$ in ref. [SHK+08]) by introducing an external shunt capacitor. This compresses the variability of the energy due to charge even further and leads to near-immunity of charge noise [HKD+09]. As quantronium it is biased at an optimum working point and controlled by microwaves either directly or through a microwave cavity (see below). Measurement is performed through a cavity with photons in the microwave frequency range. Depending on its precise connectivity, it is sometimes called a Xmon (shaped as a cross with four connectors) [BKM+14, BLK+15, BSL+16, KBF+15], a starmon [VPK+16], or a gmon, a transmon with in-situ tunable interaction with neighboring elements [CNR+14]. Its originally perceived drawback of only weakly separated computational states has been overcome by optimal control [MGRW09].

The gatemon [dLvHB+15, LPK+15] replaces the oxide-based Josephson junction by a junction based on a semiconductor nanowire. This offers the additional control knob that the Josephson coupling can be controlled by an external electrostatic gate (rather than by magnetic flux as in conventional Josephson qubits). This offers the advantage of avoiding flux crosstalk by using control voltage—which could be used to pack qubits more densely. While experiments are encouraging, this technique has not been adopted on a large scale.

The planar transmon is the currently most widely used superconducting qubit.

3D-transmons

The three-dimensional transmon is not so much an alternative qubit as it is a way to connect to a transmon qubit. Other than planar technologies, the transmon qubit is encapsulated in a metallic cavity and only accessed through that cavity. This architecture minimizes the participation of lossy oxides and thus has superior coherence properties but is also much more difficult to control and to scale due to the physical size of the devices. It is considered to be a valid contender for certain applications [PSB+11,Randomized benchmarking and interleaved randomized benchmarking RBLD12].

B) Flux qubit derived designs

Structures resembling today's flux qubits were first proposed by Nobel Laureate A.J. Leggett [Leg80] as a candidate for testing quantum physics on a macroscopic scale, even before the conception of quantum computing. They have a loop-type circuit topology interrupted by an odd (effective, see below) number of Josephson junctions and their basis states are described by clockwise and anticlockwise circulating current that produce magnetic fields and fluxes (field integrated over area) of opposite directions that can be used for control and measurement. These properties are very close to other, classical platforms of superconducting electronics, the SQUID (Superconducting QUantum Interference Device)—a sensing platform—and SFQ (Single Flux Quantum) ultra-fast classical digital logic. This gives flux qubits superior connectivity and makes them ideal candidates for quantum annealing but also for reaching ultra-strong coupling to microwaves, a property crucial in quantum simulation. A central challenge for flux qubits is reproducibility, as its non-classical behavior is driven by flux tunneling through a barrier of inductive energy. This term is inversely exponential in $(E_J/E_C)^{1/2}$ where E_J itself is inversely exponential in the thickness of the Josephson junction, a hard-to-control parameter. Still, flux qubits are a serious contender for a range of quantum computing applications including adiabatic computing and annealing. Flux qubits are sensitive to flux noise [ASB+13, KSB+16].

Single-junction loop

The simplest flux qubit consists of a loop interrupted by a single Josephson junction. It makes use of a substantial geometric inductance to form a qubit. As this inductance is roughly proportional to wire length, this fixes qubit sizes at a relatively large value, leading to excellent connectivity but also strong impact of

external noise. There are very few experiments [FPC+00] on coherent manipulations of flux qubits but the single-junction flux qubits is the workhorse of quantum annealing at D-Wave Systems [JAG+11, DJA+13, LPS+14].

Three (active) junction loop

This is the most common flux qubit design for quantum circuit applications. It was conceived at TU Delft and MIT [MOL+99, OMT+99]. It replaces the geometric inductance by additional Josephson junctions hence leading to a much more compact geometric footprint and superior coherence with a wide variability between samples [BGY+11]. Their connectivity and their excellent separation of computational to non-computational states allows strong and fast control [OYL+05]. It was also the first qubit in which interactions could be tuned in hardware [HRP+06].

In order to maximize connectivity, the qubit and its peripheral elements often share lines. Given that Josephson junctions are typically made in a two-layer overlap geometry, this leads to a change of layer when going around the loop twice, similar to a Möbius strip. As this can lead to uncontrolled offsets, sometimes a large-area (hence very passive) fourth junction is inserted in the loop in order to connect the layers in a controlled way [CNHM03,CBS+04].

Capacitively shunted flux qubit

In order to rely less on the precision of junction fabrication, the capacitively shunted (C-shunted) flux qubits has been investigated. Parallel capacitance can be controlled much better than Josephson junctions and leads to more reproducible qubit parameters with a small sacrifice in energy separation [SKD+10]. Not very well developed yet, it is still discussed as a candidate for coherent quantum annealing [CCG+11].

Fluxonium

The fluxonium circuit is related to the single-junction loop, replacing the geometric inductance by a linear array of about 100 Josephson junctions acting as a “superinductor”. These qubits have superior coherence but are very hard to operate and integrate. We are not aware of two-fluxonium experiments [PGC+14, VPS+14]. It has been developed further into a new proposal called flatsonium [SRDR17].

0-π qubit

The 0-π qubit proposed by Brooks, Kitaev, and Preskill [BKP13] is a device which increases protection from spontaneous relaxation and dephasing by invoking topological ideas. It has a slightly different geometrical arrangement of the circuit elements resulting in an interleaved double well potential. Both ground state wave functions are highly localized, and the qubit is not sensitive to charge and magnetic flux noise.

C) Phase qubit derived designs

The phase qubit operates in the regime of large E_J/E_C. Other than the flux qubits, its computational states are not classically macroscopically distinct. Phase qubits are very simple consisting of only a single biases Josephson junction as qubit and readout, a setup already investigated in the 1980s to demonstrate macroscopic quantum tunneling [DMC85]. Initially very successful, this qubit turned out to be plagued by defects in the Josephson junction [SLH+04, CMB+10, LBM+16] and have not reached long coherence times. Only very few groups, notably Ray Simmonds at NIST and Alexey Ustinov at KIT use them.

D) Other designs

A number of other designs have been explored but are of mere historic value:

- The fluxon qubit uses internal degrees of freedom of a long Josephson junction. This work culminated in the demonstration of macroscopic quantum tunneling [TM96, WLL+03].

- Junctions from high temperature superconductors in place of conventional superconductors could be appealing to operate at higher temperature. Given their difficult materials science and intrinsic damping, only basic quantum tunneling has been demonstrated [TKL+04]. Keeping all components coherent still requires low temperatures.

The specific properties of complex high-temperature junctions were speculated to be useful in the early era of Canadian company D-Wave Systems (and are responsible for their name), but were never experimentally implemented [SZW93,Zag97].

12.1.3 Peripheral elements

With the increasing maturity of this platform, connectivity and peripheral elements play a more and more crucial role in identifying these systems along with their operational challenges.

A) Cavities and waveguides

Superconducting qubits are operated at microwave frequencies between 1 and 20 GHz. This range is dictated on the low end by the ability to cool the system to the ground state in a robust dilution cryostat that can reach about 10 mK base temperature but often cools the electronic load only to about 50 mK, and on the high end by the observation that superconductors lose their superconducting properties at frequencies around their energy gap, which for Al as the weakest superconductor that is widely used is around 80 GHz. In order to manage electromagnetic fields at those frequencies, superconducting coplanar waveguides are used, both as transmission lines and as cavity resonators of finite length. Use of these resonators defines the field of circuit quantum electrodynamics (cQED). These resonators possess better coherence than the qubits (but are not controllable without them) and are used to connect qubits to each other over long distance, as well as in some instances for control [BGW+07, Poz12].

B) Direct couplers

Interactions between qubits can be mediated by direct coupling elements based on electrical capacitance or inductance. These couplers are used over short range. In principle, as a key advantage of superconducting qubits over other platforms, these couplers can be made tunable in hardware. This tunability has been demonstrated in [HRP+06, CNR+14]. While feasible, it currently is mostly applied in niches whereas the tuning of interactions in scalable quantum computer platforms is done using resonance methods [SMCG16, BKM+14, KBF+15].

C) Amplifiers and detectors

Superconducting qubits in principle offer a variety of read-out options. Specifically, much of the underlying technology has originally been developed for magnetic flux sensing using SQUIDs [CB06] which can go up to high frequencies in a microstrip geometry [KC11]. Also charge sensing using single electron transistors has been pursued. These technologies of direct qubit measurement have largely been replaced by measurement of microwave radiation scattered off the qubits using high electron mobility transistors (HEMT [HMB+15]), Josephson Parametric Amplifiers ([BSM+10,CBIH+08,HVS+11]) and their broadband multi-junction version, the traveling wave parametric amplifier (TWPA [MOH+15]). An alternative but currently less developed approach uses photon counting [GPX+14, GPP+15, Il'16].

D) Cryogenics

Superconductivity is a low-temperature phenomenon and requirements of coherence require temperatures below 100 mK. This is achieved by dilution cryostats [Pob96] - multistage cooling systems whose coldest stage uses a mixture of the Helium isotopes ^{3}He and ^{4}He. These are commercial devices that in some cases are customized to hold a large number of microwave lines. While currently hassle-free workhorses, they pose three challenges: i) Their limited cooling power at low temperatures requires to direct energy dissipation to higher temperature stages ii) the requirement of good shielding and heat management

restricts the available sample space to small volumes challenging scaling and iii) worldwide supplies of Helium are low and of the (not naturally abundant) isotope ^{3}He are critically low. Large scale production of this isotope requires nuclear facilities.

E) Microwave components

Requirements of low dissipation at low temperatures as well as isolation and routing of signals require microwave peripherals close to the sample, typically at 1 K. A critical component are non-reciprocal elements, elements that transmit radiation differently depending on their direction, such as gyrators, circulators, isolators, and directional couplers. These all have to be longer than the wavelength of a few centimeters, hence strongly limiting miniaturization and scaling. Several efforts to overcome this limitation are under way [KLC+15,CMR+16,CR14,BGW+15,VD14].

12.1.4 Quantum annealing and its status with superconductors

Adiabatic quantum computing describes the process where the solution of a hard computational problem is encoded in the ground state of a complex Hamiltonian which is hard to reach classically, and using an adiabatic sweep that starts out from an easy Hamiltonian to reach that ground state. A variation of this, quantum annealing, allows faster sweeps as long as the combined action of thermal relaxation and quantum tunneling take the system back to its ground state. These techniques have in common that they require much simpler time-dependent control (ideally only a singly, slowly varied parameter) than implementing a quantum circuit. This is in particular true for the case of Josephson qubits, where it is a major engineering challenge to apply qubit-specific microwave signals.

In discussing adiabatic quantum computing, one needs to sharply distinguish two classes of applications. We start with the less popular but more cryptographically relevant one.

A) Adiabatic realization of quantum circuits

It has been shown that adiabatic quantum computing is as efficient as circuit-based quantum computing [AvDK+07]. The mapping proposed in this paper takes any quantum circuit and maps it onto an annealing architecture and it shows that the energy gap above the ground state (whose inverse sets the time scale for execution of the adiabatic algorithm) shrinks polynomially with the number of gates in the circuit, hence proving that annealing can be as powerful as circuit-based quantum computing—e.g., for Shor's algorithm. This result assumes that each lattice site in the annealer contains a six-state particle—which can either be directly implemented or simulated by putting more than one physical qubit at each site. It also assumes the presence of three-body couplers, i.e., terms in the Hamiltonian that contain non-trivial operators at three distinct qubits (also referred to as 3-local couplers). Physically, this corresponds to a three-body interaction, which famously does not exist in nature—and, in particular in superconducting qubits the capacitive and inductive interaction are all two-body.

As a way out, three- or more-body couplers can be implemented by a technique called perturbative gadgets [KKR06, JF08, BLAG14] that formalize the idea that nonlinear higher energy degrees of freedom can introduce a low-energy interaction whose properties resemble that of a many-body interaction . There is a wealth of current proposals [AvDK+07, Bia08, LHZ15, CZW16], none of which has been realized or even seriously attempted. Realizing these is the next frontier in quantum annealing.

B) Adiabatic optimization

Quantum annealing / adiabatic quantum computing naturally lends itself to the solution of hard constrained optimization problems such as 3SAT (an NP complete problem). For these, no efficient quantum circuit i**s** known. There is no proof (or disproof) of quantum speedup for this problem**.** Current experimental scaling on the D-Wave machine (comments below) indicate that speedup is questionable at best [RWJ+14]. It has been shown that for certain extreme cases, there is significant speedup [DBI+16] but the result does not allow conclusions for scaling and for generic problems. Currently, it is highly disputed

whether this experimental evidence only points at shortcomings of the d-wave machine or hints at the lack of speedup in quantum annealing for 3SAT.

C) Experimental situation

A lot of early aggressive scaling in quantum computing as a whole has been performed in adiabatic quantum computing/quantum annealing. This was largely driven through the Canadian company D-Wave Systems. The D-wave architecture is optimized for a subclass of hard optimization problems. Even within the paradigm of adiabatic optimization, this machine is not fully general. It does not contain sufficiently general couplers (many-body couplers are not implemented and competing non-commuting interactions are not implemented). Also, the qubits are not very coherent—they would not allow to implement any meaningful quantum circuit. While quantum speedup has first been questioned [RWJ+14] in comparison to specialized, sufficiently restricted classical algorithms, there is increasing evidence that more modern devices are able to deliver quantum speedup

[KAHL22, KSR+22] . Newer architectures of d-Wave improve their ability to embed problems efficiently by improved connectivity [BEL+21].

There has been an effort to build a more general annealer at MIT Lincoln Laboratory that does not have these shortcomings, supported by the IARPA Quantum Enhanced Optimization (QEO) program. It has not led to any sizable machine available to the public but has demonstrated elements of higher-order coupling [MBB+22]**.** New quantum-simulation inspired Rydberg atom platforms aimed at gate-based optimization can also perform quantum annealing see Secction 13.2**.**

12.1.4.1 Planar transmon

The planar transmon is currently the leading Josephson qubit circuit, being on a sweet spot with high coherence, connectivity, and reproducibility. The largest known processors (IBM Eagle with 127qubits and Bristlecone 72 qubits at Google) are built from these devices.

DiVincenzo criteria

A) Scalable qubits

Various organizations have reached large multi-qubit devices

- Intel: up to 49 qubits on chip, no significance difference in coherence or fidelities compared to two-qubit chips
- Google: Bristlecone with 72 qubits published with 99% readout, 99.9% 1-qubit and 99.4% two qubit gate fidelities is the direct successor of Sycamore which was the first device demonstrating a quantum advantage over a classic computer for a constructed problem.
- IBM: Eagle with 127 qubits, they claim to have same coherence times as Falcon r8, while reducing crosstalk and an improvement of measurement fidelity. They plan to publish a 1121 qubit device in 2023. [BDG+22]
- Intel: Tangle Lake 49 qubits with a reported fidelity of 99,7 %
- Zuchongzhi 2: 66 qubits which in 21 claimed to be current world’s fastest quantum computer (being 10 million times faster than Sycamore)

B) Initialization

The initialization of superconducting qubits requires high speed, high fidelity and independence of initial conditions. Currently it is possible to initialize a qubit and its resonator within 80 ns with 99% Fidelity. Higher fidelities are possible with longer initialization times.

C) Universal gates

High gate fidelities have been reported in various architectures and gate implementation schemes. Systems with higher numbers of qubits have shown no significant decrease of fidelities. Also, the possibility for parallel gates has been demonstrated. For the most sophisticated platforms it is difficult to get data from each player in the field. However, they should be close to Sycamore which is shown in the following Table 12.1. In smaller experiments the record numbers are generally a bit better, because they do not have to fight crosstalk between qubits.

Table 12.1: Data taken from [Bar22].

Qubit metric	***Mean***	***Std. Dev.***
$f_{01,max}$	6.93 GHz	110 MHz
$F_{01,idle}$	6.66 GHz	57 MHz
η	-208 MHz	4.7 MHz
T_1	16.04µs	4µs
1 qubit error (XEB)	0.12%	0.03%
2 qubit error (XEB)	0.62%	0.24%

D) Coherence

Coherence in 2D transmons is consistently high, following its design principle [KYG+07,HKD+09]. IBM seems to be leading in terms of coherence with a T1 of roughly 50-80µs. Note that we have not included the longer coherence time of Tantalum transmons [PRM+21] (yet), as those have so far only been tested at small scale.

E) Readout

- Wallraff, ETH: dispersive readout of transmon qubit with 0.9825 readout fidelity in 48ns or 0.992 in 88ns [WKG+17]
- Martinis: 0.998 in 140ns was best reached fidelity, a more average value is 0.99 in 200ns [JSM+14]
- IBM 5 qubits: Single-qubit readout fidelities typically ~ 0.96 [LMR+17]
- IBM QX3: readout error $\sim 5 \cdot 10^{-2}$, measurements can be done simultaneously
- The use of Purcell filters enables faster readout with a 0.991 fidelity in 40 ns [SKI+22]

DiVincenzo criteria: summary and estimation of device quality

Table 12.2: Summary of DiVincenzo criteria for planar transmon qubits. ✓: Met routinely, ?: Met sometimes or meeting them is controversial, ×: not met.

Criteria	***met?***	***Comments***
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

Table 12.3: Optimistic assumptions for different error rates and operation times combining the best reached values for each operation. This does not describe a current available setup but shows what is in principle possible right now or in near future. Times are initialization, 1- and 2-qubit gate and measurement time. Probabilities are error probabilities for the respective processes. A surface code cycle contains 4 two-qubit gates, 2 one-qubit gates, measurement and initialization as well as classical processing. (Again LDPC) are favorable.

t_I	t_1	t_2	t_M	p_I	p_1	p_2	p_M	T_2
140ns	10ns	40ns	140ns	$2 \cdot 10^{-3}$	$8 \cdot 10^{-4}$	$6 \cdot 10^{-3}$	$2 \cdot 10^{-3}$	80µs

Fault-tolerant extrapolation

With current experimental advances, running successful error correction is imaginable, although high physical error rates make it quite resource-demanding and long measurement times give a limit to the problem size that can be solved in reasonable time. Faster measurement is possible, but at the cost of lower fidelities.

In an earlier version of this study [WSL+20] an estimation of physical qubit costs for running dlog and factoring algorithms was made using the Autotune tool Polyestimate [Fow13b]. This was done using a combination of best reached values for measurement, initialization, gates, and coherence as given in **Error! Reference source not found.**. Figure 13.1 in [WSL+20] shows possible realizations given target runtimes of 1 to 100 days and the limit of parallelization due to T depth. Factoring algorithms would only be possible for really long runtimes: For the chosen sets, only $n = 1024$ is possible in 10 days, with $\sim 3 \cdot 10^{10}$ qubits (or in 100 days with 10 times less qubits), $n = 2048$ and $n = 3072$ already require 100 days runtime. Larger problem sizes cannot be parallelized to runtimes as low as 100 days as that would violate the temporal order of sequential T gates. The chosen dlog problem sizes seem much more reachable: Problem sizes of up to $n = 356$ could theoretically be run in 1 day, with 10^{10} - 10^{11} qubits. Even for those problems, distances still over $d = 100$ in the Clifford part and two distillation rounds for T gates (with distances ~ 130 and ~60) were required.

Analysis and outlook

2D transmons have demonstrated error correction [AAA+22]. For the steps ahead, challenges in engineering, operation, and scale-up science are clearly visible:

- **consistency**—qubit fabrication, in particular fabrication of Josephson junction, currently has limited yield. Making a chip where every junction work needs to improve this. As in other areas this has been achieved, it is likely that professional process control will enable this. Companies like Rigetti pride themselves of their fabrication consistency but do not publish any verifiable details.
- **size**—the microwave periphery still consumes majority of space: Per transmon, which has a size of around 0.1mm^2 on the chip, two circulators of about 10^{-5}m^3 are currently required for readout. Challenges are towards smaller circulators [VD14,MCP+17], multiplexed readout—requiring a lower number of circulators, or digital readout [MVP+17] without any circulators at all.
- **room temperature electronics**—rack-mounted classical control electronics currently is mostly laboratory equipment, hence optimized for flexibility, not for space. Conceivably, making this smaller will not be as hard as other scaling challenges. Also, papers in signal routing show how to use generators for multiple qubits [ADL+16].
- **packing**—closely packing multiple chips, 100.000 qubits would fit on a cold plate of a large commercial cryostat. Assuming 10 readout channels per circulator and somewhat more compact circulators, also 10.000 controls at 1K would fit. A concerted effort that would require to build a cryostat that is ten times as large appears to be possible. With additional effort in miniaturizing controls and qubit footprints and customizing and integrating pulse generation, even 10s of Millions of qubits would be conceivable.

- **connecting cryostats**—building larger systems would only be possible with superconducting microwave interconnects. With a speed of approximately $c/2$ it would take around 25ns to transfer a signal between two cryostats. However, current remote entanglement protocol require detection and are estimated at around 750ns, creating global slowdown for the clock of such a processor. Accelerating this is a major challenge.
- **connectivity**—even though qubits can be arranged on two-dimensional lattices, enabling both-way coupling between all neighboring qubits only works if all engineering targets are met.

The roadmap of IBM [IBM22] addresses these questions: It builds custom cryostats and electronics and anticipates the processors being large multi-chip modules with connected chiplets and ultimately multi-cryostat systems.

12.1.4.2 3D transmon

3D transmons reach superior coherence but less flexibility and thus slower control.

DiVincenzo criteria

A) Scalable qubits

Multiple qubit devices were realized - Multiple cavities can be coupled through bridge-qubits, i.e., qubits coupled to multiple cavities at once.

B) Initialization

Is done by measurement and post-selection: a fidelity of 0.988 [RvLK+12] has been measured.

C) Universal gates

Single-qubit gates are realized with local microwave drive, two-qubit CZ gate via driven common resonator.

Single qubit gates with 0.999 RB-fidelity in 36.7ns, two-qubit gates with 0.98 RB-fidelity in ~ 400ns [PMS+16]

D) Coherence

The 3D transmon was designed with maximum coherence in mind, hence numbers are superior

- T_1 = 90µs, T_2* = 48µs, T_{2E} = 86µs [PMS+16], cavity decay rate κ = 7.7kHz
- Lincoln Lab: T_1 = 80µs, T_2 = 115µs, T_{2E} = 154µs [JKS+15]
- T_1=240µs , T_2*=45µs , T_{2E}=85µs [TSD+20]

E) Readout

Readout of 3D transmons is done analogous to 2D transmons [PMS+16]. A readout fidelity of 0.99 has been reached and 0.999 seems theoretically reachable.

- 0.981 with homodyne detection enhanced by JPA [RvLK+12]
- 0.99 [RD15]
- 0.999 in 60ns theoretically proposed [DDBA13]

DiVincenzo criteria: summary and estimation of device quality

Table 12.4: Summary of DiVincenzo criteria for 3D transmon qubits.

Criteria	*met?*	*Comments*
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

Table 12.5: Optimistic assumptions for different error rates and operation times combining the best reached values for each operation. This does not describe a current available setup but shows what is in principle possible right now or in near future.

t_I	t_1	t_2	t_M	p_I	p_1	p_2	p_M	T_2
60ns	40ns	400ns	60ns	0.99	10^{-3}	$2 \cdot 10^{-2}$	0.99	115µs

Analysis and outlook

3D-transmons are about to cross the fault tolerance threshold, going from B to C. Still, their size leads to technological challenges to scaling, making it unlikely that they will overtake 2D-transmons.

- **benefits vs drawbacks**—The higher coherence of 3D-transmons comes with a reduction of flexibility, lower fidelities and much higher volume cost that overcompensate the gains. A single 3D-transmon in its cavity requires $50cm^2$ on the cold plate of a dilution cryostat. If one manages to remain modular with multiple qubits per cavity, this number can be brought down to $\sim 20cm^2$, which is still a large infrastructure challenge compared to 2D-transmons.
- **Frequency crowding in larger networks** [PMS+16]—Many 2-qubit gates work by tuning the frequencies of two qubits into a specific resonance condition. This involves higher energy levels, which might cause other energy levels to intervene between the qubits. Using WAHWAH [SDEW13, TMW16] control pulses is a possible solution to this.

3D-transmons have their largest potential in realizing oscillator encodings.

12.1.4.3 Evaluation: Flux qubit

The flux qubit is dominating quantum annealing due to its high connectivity (see Section 9.1 for comments on fault-tolerance and benchmarking). It also presents a superior interface to other quantum systems such as spin, which is interesting for building quantum repeaters.

Flux qubits have demonstrated all DiVincenzo criteria and due to their large anharmonicity allow for ultra-fast gates.

DiVincenzo-Criteria

A) Scalable qubits

Large arrays of flux qubits, albeit with low coherence, have been demonstrated for quantum annealing by D-Wave Systems [BHJ+14,BCI+16,KXB+16,LKEH17]. This seems feasible with more coherent qubits as well. When going to gate-based quantum computing, precise frequency allocation is important which is difficult as it requires unusually precise fabrication. This can be mitigated by using a capacitive shunt or a two-loop design [SKD+10,GBY+11,SGJ+13,YGK+16] which are so far not tested as much as the simple flux qubits. With an eye on these challenges, flux qubits can be viewed as scalable.

B) Initialization

Initialization is achieved via cooling, assisted by the large available energy splittings

C) Universal gates

- IQC: single-qubit gate in ∼0.5–1ns with fidelities of 0.996–0.999 [DOS+15]
- Mooij: CNOT demonstrated, but with fidelity of 0.4 [PdGHM07]
- Optimal control: single-qubit gates below 1ns and CNOT in 2ns [HG14], limited by leakage (10^{-6}) and decoherence errors ($\sim 10^{-5}$) theoretically proposed and simulated
- Two-qubit gates with fidelity >95% demonstrated

D) Coherence

Lincoln Lab: T_1 = 40µs, T_2 = 85µs, T_{2E} = 40µs [YGK+16]

E) Readout

Single shot readout via inductively coupled dc-SQUID [LmcHM05], with measurement time $T_m \approx 300$ns and fidelity > 0.8.

DiVincenzo criteria: summary and estimation of device quality

Table 12.6: Summary of DiVincenzo criteria for flux qubits.

Criteria	*met?*	*Comments*
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

Outlook

The key problem for flux qubits is consistent fabrication given the exponential dependence of the flux tunnel splitting on the Josephson energy, small tolerances in the Josephson energies lead to large errors of that term making targeted placement in frequency space that is needed for scaling up a major challenge. It is expected that they will show high gate fidelities also for two-qubit gates but there is doubt whether reaching level C will be attempted soon. Flux qubits are a great platform for quantum annealing but trailing behind transmons for gates.

12.1.4.4 Evaluation: Fluxonium

DiVincenzo-Criteria

A) Scalable qubits

Scaling is challenging due to the space required. Every single qubit needs to be built of up to hundred Josephson Junctions [VPS+14].

B) Initialization

Can be done via cooling.

C) Universal gates

CZ with 99.9% fidelity demonstrated [FNS+21]

D) Coherence

- T_1 increase to values above 1ms [PGC+14,VPS+14].
- Theoretical proposal of flatsonium [SRDR17], with expected dephasing times of T_ϕ ~10ms.

E) Readout

Quantum non-demolition projective measurements within a time interval much shorter than T_1 , 5µs single-shot projective measurement [VPS+14]

DiVincenzo criteria: summary and estimation of device quality

Table 12.7: Summary of DiVincenzo criteria for fluxonium qubits.

Criteria	*met?*	*Comments*
Scalable qubits	?	
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

Outlook

Fluxonium has enjoyed a strong boost: Two-qubit gates have now been realized, Fluxonium has been made more compact and making the large number of Josephson junctions is not a challenge anymore. Fluxonium is clearly on level B and the most promising runner-up to transmons.

12.1.4.5 Evaluation: 0-π qubit

The 0-π qubit uses topologically protected states as computational states by introducing a specific geometric design (loop) of the components. Therefore, the coherence times are enormously large but come with the cost of an increase of control times. No promising data have been shown yet and thus it is on level A.

DiVincenzo-Criteria

A) Scalable qubits

Similar to fluxonium, every qubit needs an array of Josephson junctions, and current experiments are at the scale of a single qubit.

B) Initialization

Currently, there are no definite numbers of how well and in which time initialization can be done but coherent control has been demonstrated. [GMdP+21]

C) Coherence

Due to the design extremely high coherence times in the order of milliseconds are reported. T_1=1.6 ms, T_{2E}=25 us, T_R=9us [GMdP+21]

D) Readout

Readout is done by dispersive readout.

DiVincenzo criteria: summary and estimation of device quality

Table 12.8: Summary of DiVincenzo criteria for fluxonium qubits.

Criteria	*met?*	*Comments*
Scalable qubits	?	
Initialization		
Universal gates	?	
Coherence	✓	
Readout	✓	

Outlook

The 0-π qubit is a promising future candidate for performing at outrageous fidelities. However, it remains questionable if this justifies the increase of control times.

12.1.5 Operational challenges for superconducting platforms

Many of the following information is resulting out of private communication with a leading expert (Rami Barends working at PGI-13 in Juelich).

Size

Current devices allow up to ~100 qubits on a single chip. The chip operates at sub 15mL such that it has to be placed in a dilution refrigerator. The equipment for control fits in a laboratory, which includes all control and cooling components.

Power Consumption

For a 50 qubit device there are roughly 30kWh required for cooling and additionally 10 kWh for control and other things. This results in an energy consumption of about one kWh per qubit. In future devices it might be possible to reduce this figure by a factor of 100 if the cooling power of one refrigerator can be shared for multiple chips.

Power dissipation and temperature stability

Integrated control and readout at low temperature require a low power dissipation because of the limited cooling power of dilution refrigerators and the high-frequency interconnects from room to cryogenic temperatures. Therefore, the use of those high-frequency interconnects should be minimized and future devices will be in need of cryogenic CMOS devices instead. The creation of such devices is an ongoing research field which is currently not able to deliver sustainable results yet [AGD+22].

Cycle time

Two qubit gates can be performed in the order of ten to a few hundred nanoseconds. Single qubit gates are faster but in the same order of control time. Theoretical calculations suggest that these control times can be pushed down to the order of hundreds of picoseconds [ZJHR21].

Classical data flow

This issue needs to be addressed in near future and is crucial for the use of error correcting protocols. Some components that may offer improvement of cost, size or performance and thereby increasing the classical data flow are (non-ferrite) isolators, (non-ferrite) amplifiers and scaled signal delivery systems [BDG+22]. Combining these advancements with new error correcting code techniques leads to significant improvement to be done in the next few years.

Reliance on rare materials

For the production of the superconducting chips are no super rare materials required. However, the scarcity of Helium^3 will pose a major challenge for future devices if experiments both increase in size and number. Currently the yearly consumed Helium^3 is about 8kg (~60k liters). Because of nuclear weapon reduction and an increase of applications He^3 is a really rare and costly resource and for the realization of large-scale superconducting quantum computers it would require to produce way more of it within nuclear reactors for civil uses.

Vacuum and low temperature

For this platform vacuum is not an issue (as it is a natural result of low temperatures). Maintaining thermal budget [VAVD+22] is an engineering challenge that needs to be monitored: While creating the low operation temperatures of 10 mK (300 times lower than outer space) is not a problem per se, the cooling power of cryostats scales with T^3 thus energy dissipation at the coldest part of the system, i.e., close to the quantum chip must be avoided as a design rule. It is not clear, how this can be managed at scale.

Stability

Opposite to the ionic platform there a no total qubit losses since the artificial atom is located in the electric circuit. However, some parameters of the qubit like frequency or noise sources can drift over a timescale of multiple hours or days. An example of this disturbing effect are quasiparticle events, which are mainly caused by cosmic rays and can reset a qubit or distort its phase. However, one can reduce effects by moving the laboratories underground or using alternative designs like the 0-π qubit [BKP13]. However, there are also other noise sources present which currently cancel out the possibility of building larger scale quantum computers underground.

Yield and scatter

The production of superconducting chips is currently reliable and fast for small devices. Here, 5-16 qubit devices are manufacturable in roughly a week. In contrast, the production of state-of-the-art devices such as EAGLE takes several months [BDG+22]. In this field there is need for more modularity and an ecosystem with rather speculative demand and risk affine suppliers. This affects, e.g., the applicability of quantum error correction, where uniform errors are assumed [AAA+22].

More generally, in the superconducting platform the biggest challenges are improvements at fabrication of the devices. The qubit quality is mainly limited by the variability of the Josephson energy E_J which controls the qubit spectrum and is a key ingredient to the quantumness of the system. Especially, the traditional fabrication technique (double angle evaporation with required lift-off) introduces unwanted resist contamination and polymer masks.

Furthermore, some fabrication methods are not compatible with CMOS fabrication and therefore will have a big disadvantage in production reliability when scaling up to larger devices.

Extrapolation to future devices

For problem sizes of practical interest Error Correction (EC) will roughly need a system size which is 10^6 times bigger than current devices. Therefore, there seems to be no alternative to interconnecting many

devices. This is doable in multiple ways starting with direct coupling of multiple chips in one cryostat, going over to classical parallelization of sub-QPUs and the need of long range (quantum) inter-connectivity between multiple refrigerators [BDG+22].

This technology is in its infancy right now [FRP+21, MSK+20]. The natural idea of distributing quantum calculations over multiple remote processors has been explored in [XQLM22], and it has been shown that the least overhead is incurred by teleporting data registers (compared to using quantum gates across processors) [vMM+08]. At the time being, this technique is quite challenging on the hardware side – specifically because of the low speed of connections between remote QPUs, but in principle efficient. It has gained new interest with IBMs „circuit knitting“ technique from the family of probabilistic error mitigations – which has so far not been applied to Shor's algorithm [PS22].

12.2 Quantum computing based on semiconductor qubits

Semiconductors are a natural platform for scalable quantum computing [Hei03]. On the one hand, standard semiconductor devices are in fact simple quantum technologies—transistors, diodes, and semiconductor lasers are based on engineering a quantum material and its energy spectrum. On the other hand, the semiconductor industry provides enormous experience in all aspects of semiconductor fabrication and has shown the potential for large-scale integration of classical processors.

Nevertheless, semiconductor platforms are not yet consolidated to the extent that others are, hence providing a complex community with varied approaches. The comprehensive review [BLP+23] by Burkard and coworkers covers semiconductor qubits encoded into electron spins and nuclear spins.

12.2.1 Basic notion and terminology

In this part of the study, we are providing some background on the systematics between the plethora of semiconductor platforms. Readers interested in performance data can skip ahead.

12.2.2 Various types of semiconducting qubits

We can categorize semiconductor-based approaches along these three dimensions:

- the degree of freedom is used to encode quantum bits—charge/orbital degrees of freedom, electron spin, nuclear spin, or coupled degrees of freedom,
- the method of confinement of the continuous degree of freedom of semiconductor material into discrete logical elements for qubits—quantum dots, single defects, topological mechanisms,
- the material system that is used—elementary semiconductors (C, Si, Ge), III-V Materials (GaAs family), or more exotic semiconductors.

These dimensions are correlated as described below.

A) Degree of Freedom

Electron charge / Orbitals

A straightforward way to encode quantum information is to use the position of a charted quantum particle—electrons or holes in semiconductors. These are thus often referred as *charge qubits* and are straightforward to control by electromagnetic fields. By their charge, they also couple well to unwanted degrees of freedom of the semiconductor materials hence strongly limiting coherence times in particular due to charge noise intrinsic to most materials. Pure charge qubits have shown simple single-qubit operations very early [HFC+03].) but are hardly investigated any more [CRFG17,THWZ16,WKS+16]. However, some advanced spin-qubit designs contain use of the charge degree of freedom. When investigating charge qubits, it is important to evaluate their sensitivity to decoherence by lattice vibrations (phonons) which is very strong in piezoelectric materials.

Electron spin

Electrons have spin—an intrinsic angular momentum associated with a magnetic moment. When bound in materials, the orbital angular momentum and spin combine (see below). Spin is a natural two-state system that can be addressed using magnetic fields. Note that spin resonance in molecules is described in a different chapter.

Electron spin states are sensitive to spin environments, most notably nuclear spins. These couple magnetically to the electron spin and move slowly, given the much larger mass of nuclei compared to electron spins, driving protocols, device designs, and choice of material.

Nuclear spin

The nuclear spin degree of freedom resembles that of the electron with a few key differences: It is extremely well isolated from its environment thus very quantum coherent. It is usually not mobile and much more difficult to engineer. Nuclear spins play a role as auxiliary degrees of freedom in some semiconductor platforms where they are typically manipulated through interaction with an electron.

Coupled degrees of freedom

Some semiconductor implementations use more complex degrees of freedom. Specifically, candidates for topological quantum computing encode quantum information non-locally in complex many-body states, including the 5/2 fractional quantum Hall effect state, a collective state of electrons and magnetic field in a thin film in a very strong magnetic field, and Majorana fermions in topological systems that originate from the combination of semiconducting materials with a strong spin-orbit interaction and superconductors.

Hole qubits

A well-known concept in semiconductors which is also used in conventional electronics is that of a missing electron, a hole, as a positively charged carrier, induced by doping with other atoms or polarizing with other voltages than electron-based qubits In silicon, hole qubits have the feature that their spin degrees of freedom couples to their orbit stronger than electrons, which on the one-hand allows for more compact all-electrical control, on the other hand poses the risk of being exposed to similar electric decoherence as charge qubits. There have been first demonstrations [PBS+22] but it is too early to evaluate these qubits in full.

B) Method of confinement

Electrons in semiconductors are generically free to move in the material. This stands in the way of quantum computing as this makes it impossible to address qubits selectively to drive single-qubit gates. It also leads to an undesired continuous energy spectrum that is a source of decoherence and disallows initialization of qubits by cooling.

This means that the electrons need to be confined to a small structure in space, small enough to address them selectively. Depending on the details of the confinement potential, the energy splitting of orbital states of electrons confined to a small region of size L is $\Delta E \propto m_*^{-1} L^{-2}$ where m_* is the effective electron mass, described later. There are three main ways of confinement:

Quantum dots

A quantum dot is an artificial nanostructure that confines electron motion. They are either defined by nanofabricated metallic gate structures that repel electrons from regions where they are not wanted (lateral quantum dot) or produced free-standing by a materials-growth or etching procedure. The former are very flexible as the gate voltages can be used to fine-tune dot properties, the latter can be made smaller. It needs to be noted that the terminology of quantum dot has several meanings in literature and is quite fashionable, not all of them are suitable for quantum computing.

Donors and defects

A key component of all modern semiconductor technologies is doping the material with atoms of other materials to change the effective properties of the material. For quantum computing functionality, it is possible to use the electrons around single, isolated dopants or defects. Electrons there are bound relatively tightly. Again, several realizations of this scheme exist and will be described below. The common challenge to those is that atomically precise placement of donors and scalable control of qubits is a frontier in nanotechnological fabrication.

Topological effects

An attractive way to reach confined elements are topological effects. There, interactions between many degrees of freedom create a bound state that, in principle, is stable against any external perturbation: Locally perturbing the state of the system does not change the topological genus of the state hence not compromise quantum information.

C) Materials

Semiconductors are based on half-filled electronic shells, hence there is a restricted choice of semiconductors. This state can be reached either by using elements from the fourth column of the periodic table (C,Si,Ge) or compounds that are in the fourth column on average only (GaAs, InSb). Key properties include

- Electron effective mass: Effective mass is a property describing the motion of electrons that are exposed to the crystal lattice, it can substantially deviate from the bare electron mass. Smaller effective masses give larger energy splitting or, given target values for energy splittings, allow to reach those values in larger, more manageable confinement length scales.
- Valley degree of freedom: This is a property of the motion in the crystal that identifies that there are multiple electron states that behave similarly [YC10] which makes it difficult to isolate a single qubit (rather than a single qubit per valley). As valley degeneracy is a result of symmetry of the crystal it can be removed by breaking that symmetry through mechanical strain.
- Content of nuclear spins: Their presence is a strong perturbation to electron spin qubits through dipolar and contact interaction.
- Piezoelectricity: Electric fields produced from mechanical deformation. This is a property of the compound and the crystal structure. Piezoelectricity implies strong interaction of lattice vibrations with the orbital degree of freedom and is serious detriment to quantum coherence.
- Spin-Orbit interaction: In principle, spin and orbit are coupled degrees of freedom but strength and relevance of this interaction depend on the material. In general, this interaction is strong in semiconductors made from heavy elements. If the spin degree of freedom is used to encode qubits, spin-orbit interaction is detrimental as it contributes to decoherence via the orbital degree of freedom. On the other hand, it is necessary to have strong spin-orbit interaction for topological qubits.

Gallium Arsenide

GaAs is a III-V semiconductor (third and fifth column) with traditional applications in opto-electronics. It has no valley degree of freedom and low effective mass. Every nucleus of every isotope has nuclear spin. GaAs is piezoelectric and has weak spin-orbit interaction at least in lateral quantum dots. Initial confinement is reached by sandwiching the material with AlGaAs.

Silicon

Si is a semiconducting element that is the backbone of traditional computers. It has a valley degree of freedom and large effective mass. It can be isotopically purified to be nuclear spin free. It is not

piezoelectric and has only very weak spin-orbit interaction. Initial confinement is reached by sandwiching with SiGe which also applies the required strain to remove its intrinsic valley degeneracy.

Carbon

Carbon comes in a number of allotropes. The most interesting allotrope for quantum technologies is currently diamond, wide-bandgap semiconductor with the same crystal structure as Si. Defects in diamond, specifically the Nitrogen-Vacancy (NV) center are a leading system for quantum technologies, mainly in quantum sensing. An approach to quantum computing with NV-centers is described below. Diamond is not piezoelectric and can be made nuclear spin free.

Indium Antimonide

InSb is a heavy III-V semiconductor that can be easily grown in nanowires. Its strong spin-orbit interactions, alongside InAs and Si/Ge core - shell nanowires, make it the leading platform for topological qubits [SLTDS10,LSDS10,PSV+12,vWPB+13]. Mercury Telluride (HgTe) is used for similar purposes.

12.2.2.1 Concrete semiconductor platforms

Based on the background and classification above, this section describes the known and experimentally relevant semiconductor platforms. In fact, since the first concrete proposal by Loss and DiVincenzo to use a single spin in a quantum dot to represent a qubit [LD98], roughly a dozen further proposals have been put forth. Figure 3 in the review [BLP+23] gives a graphic overview of these variants by categorizing them according to how many electron spins and how many sites are used per qubit. Here we cover the most relevant ones.

A) Lateral quantum dots: Loss-DiVincenzo

In this scheme [LD98], lateral quantum dots containing one electron hold the quantum information encoded in the spin of that electron. Placed in a strong magnetic field produced by a superconducting permanent magnet to produce a Zeeman splitting that is large enough to allow initialization by cooling. Single-qubit gates are performed by microwave fields resonant with that Zeeman splitting. Two-qubit gates rely on the exchange interaction between neighboring quantum dots. This interaction can be tuned by an electrostatic gate between the dots that controls the wave function overlap. Readout is based on spin-to-charge conversion and then fast charge readout by a quantum point contact [EHWvB+04,TED+05].

In materials with nuclear spin such as GaAs, this scheme is very sensitive to noise. A further challenge is related to addressability: Microwaves even in near field cannot be focused on only one quantum dot and not its neighbor. The most popular solution [OPLTT12] is to prepare a micromagnet next to the dots that produces a magnetic field gradient, hence changing the resonance frequency of the dots, and then selecting quantum dots by that frequency.

B) Lateral quantum dots: Singlet/Triplet

In order to combat nuclear spin decoherence, the S-T qubit was invented at Harvard [SDP+12]. It physically encodes a single qubit in two spins in two neighboring quantum dots and only uses the unpolarized subspace spanned by $\{|01\rangle,|10\rangle\}$ that are not sensitive to the magnetic field. In this subspace, tuning the exchange energy provides single-qubit gates. Two-qubit gates rely on electrostatic interaction between double-quantum-dots, all other techniques resemble the Loss-DiVincenzo technique. One of the challenges here is scaling given this very complicated architecture. Also, this qubit is sensitive to charge noise, albeit weaker than a pure charge qubit.

C) Lateral quantum dots: Encoded universality

Taking the idea of noise protection further, [BKLW00] and [DBK+00] show that even simple interactions that are not inherently universal for quantum computing can be made universal by introducing a

decoherence-free subspace. This requires encoding a logical qubit using three or four physical qubits. When the physical qubits are represented by electron spins, the only resource that needs to be turned on and off, or pulsed, is the Heisenberg exchange interaction. For this reason, this scheme is also known as exchange-only quantum computing. Early on, this has been attempted in lateral quantum dots grown in GaAs/AlGaAs heterostructures [LTD+10], and was later realized with higher quality in Si/SiGe heterostructures [WRJ+23].A fundamental difficulty for this qubit encoding is the realization of two-qubit gates. While an arbitrary single-qubit gate can be facilitated by sequentially pulsing the exchange interaction between the three spins of a qubit at most three times, a minimum of 18 nearest-neighbor pulses are required for an (entangling) two-qubit gate, assuming the qubits are oriented on a linear array [FW11]. The development of theoretical understanding of this optimal known pulse sequence made it clear that this number can be reduced to no less than 12 pulses, assuming all-to-all connectivity [ZB16]. Carrying out such a long sequence of pulses takes a long time, which results in loss of coherence and thus constitutes an impediment for achieving high-fidelity two-qubit gates.

D) Lateral quantum dots: Charge qubits

Originally, pure charge qubits where only the position of an electron in a double quantum dot is used were also pursued [HFC+03]. These are sensitive to phonons in piezoelectric GaAs and to slow charge noise in Si and have been abandoned for quantum computing [CSF+21].

E) Si-Donors: Kane proposal, historic work

Implantation of single donors to provide discrete states is primarily done in Silicon. The Kane Proposal [Kan98, Lan95] provided an early blueprint for this architecture, using P donors as long-lived quantum memory, hyperfine interaction to interact with electron spins used as processing elements, and exchange interaction between electron spins to make two-qubit gates. Control is applied by metallic gate fingers like those used in quantum dots to tune interactions and drive single-qubit gates. The Kane proposal states that single-qubit gates are performed through magnetic resonance, and two-qubit gates are implemented via the exchange interaction.

Current efforts on single donors are heavily updated versions of the Kane proposal. The coherence times for electrons are ~1s and for the nuclei ~30s largely limited by complex spin-spin interaction [TMS+15]. The resulting operation of the nuclear degree of freedom as quantum memory was shown in [FSL+17]. Single-qubit gate infidelity errors around 10^{-4} were achieved for electron and nucleus [MLS+15] and similar values have been verified by gate set tomography (GST) [DMBK+16], which also verifies Bell's inequality. Initialization by relaxation is very slow given those relaxation times but can be improved by Bayesian methods. The combined fidelity of initialization, gate, and readout ("Triple-Triple") is 99.9%.

Two qubit gates with high fidelities (~98%) were demonstrated in multiple experiments [HFS+20,VYH+15,WPK+18,ZSR+18].

F) NV-Centers: Distributed quantum computing

(Artificial) diamond is an unusually pure and stable wide-gap semiconductor. Its color centers provide a natural trap for electrons with discrete states usable as qubits. The most studied is the NV (Nitrogen-Vacancy) center, i.e., a defect created by replacing a carbon atom with a nitrogen atom and creating a vacancy in the lattice. The primary quantum technology in which color centers are used is quantum sensing, followed by quantum communication. The simplicity and stability in NV centers also make them quantum computing candidates. A single NV-center contains an electron and a nuclear spin hence presenting a natural two-qubit register, which has been successfully operated [NBS+10,DCJ+07,RCB+11]. This work has in fact been taken to up to ten qubits demonstrating error correction, exhausting the natural limit of the electro-nuclear spin systems [BRA+19, AWR+22]. As its properties are dictated by the rules of crystallography (it needs the nuclei to be very close to the color center), it is unlikely that this electro-nuclear approach can be taken any further.

For a scalable alternatives two proposals are pursued: Distributed non-deterministic quantum computing connecting remote NV centers by photonic links [NTD+14,TCT+10,AHWZ18], and implantation of NV

centers at suitable positions, similar to spins in silicon [YJG+12,JGBW+16,GBKJ+19]. This is more difficult than for the case of silicon given that it cannot rely on experience of the semiconductor industry. Another approach is the coupling via a superconducting transmission line resonator [ANP+17]. Although coherent coupling of two NV centers was observed, these first experiments could not address the degree of entanglement that can be reached between the spins yet. The next few years will be very informative about this approach. Note that the Australian company Quantum Brilliance and their German subsidiary work on commercializing NV-center based co-processors, but do not publish technological details.

G) Topological qubits

Realizing topological bound states that promise resistance to noise and decoherence requires well fine-tuned models [DSFN06,NSS+08,Wil09]. The most pursued route is based on a one-dimensional system with strong spin-orbit interaction that creates a topologically nontrivial band structure with superconductivity. This could be realized in InSb or InAs Nanowires [SLTDS10,LSDS10,PSV+12,vWPB+13]. These are not naturally superconducting, but superconductivity can be induced by covering with a superconducting layer, a phenomenon known as the proximity effect. The carriers of topological quantum information in these systems are called Majorana Fermions.

On the experimental side, two groups have claimed to have observed Majorana fermions through a specific feature in the conduction characteristic, a so-called zero-bias anomaly [PSV+12,vWPB+13,AHM+16b]. It has always been under dispute if they can be unequivocally assigned to Majorana states. Note that two Majorana fermions are needed for one qubit. The field has received a setback as a few of these publications have been retracted or received a note of concern based on the substantiated accusation that experimental data were selected in order to match expectations, which has led to the termination of large portion of these projects [GCZ+17, ZLG+18, ZLG+21,GCZ+22,HPS+17,VWvH+20].

A more recent publication highlights the topological gap as a more convincing indicator of topological states, but as there is again a wealth of mechanisms that can lead to an energy gap, this has not convinced the community [PvHK+21].

The search for Majorana Fermions in this platform is certainly not over but is now considered basic research with long timelines. While this is the most promising platform for topological qubits, at this point in time, others have been attempted and are listed in the previous edition [WSL+20].

12.2.3 Evaluation

12.2.3.1 Evaluation: Spins in quantum dots

In quantum computing with semiconductor quantum dots, research activity is highest for the Loss-DiVincenzo scheme [LD98], which encodes a qubit into a single electron that is captured inside a single quantum dot. Only a few of the other types of quantum dot-based schemes are actively pursued in the laboratory. While initial experiments often started using GaAs as a host material, the bulk of experiments are now based on the Si/SiGe family. This is mostly because high coherence times are achieved by isotopic purification of Silicon.

Experimental results and device parameters, including coherence times, gate speed and fidelity reports, are documented in the technical review [SL22]. Most notably, universal quantum gates, qubit initialization and readout have all been realized with fidelities above the surface code threshold of 99%, see below for details. Furthermore, first error correction experiments have been realized, however, due to small system sizes only a single type of error can be corrected in those demonstrations [TNN+22,vRLR+22]. Still, these experiments elevate this technology beyond level B to the beginning of level C.

A necessary architectural primitive for scaling is the implementation of long-range couplings. This enables the possibility of packing additional components into the system, including readout sensors or control circuits. Research teams pursue two main tracks. One is the coupling of spins to microwave resonators, similar to circuit QED in superconductors [SSK+18,SZK+18, BCM+20, BCP+20]. The other is the shuttling of electrons, which has been analyzed theoretically [LKF+22], and whose proof of principle was recently realized [SSX+22].

DiVincenzo criteria

A) Scalable qubits

To maintain spin coherence, silicon needs to be isotopically purified. Only systems with less than ten quantum dots have been demonstrated so far, but proposals for scaling exist and have been shown (with inferior coherence) in related semiconductor structures. Similarity to current microelectronics makes it likely that this can be achieved, and preparations for the fabrication of 300-mm wafers that may host large numbers of electrons in quantum dots are already under way [NZW+24]. The largest realized sample consists of a linear array of nine quantum dots plus three quantum dots for single-shot charge readout [ZHM+16]. The current record is entanglement of four qubits, the European Flagship project however is expected to have 10-16 entangled qubits in near future.

B) Initialization

State preparation for a single spin with a fidelity of 99.76%, verified via gate set tomography, has been achieved in [MGF+22]. Here the used device can host up to six quantum dots, only one of which was used for the work in the paper. Earlier, Si/SiGe double quantum dot initialization fidelity > 99% was demonstrated in [WPK+17]. Initialization and readout of one dot done with spin-selective tunneling to a reservoir [EHWvB+04] (Pauli Spin Blockade), initialization of the other dot at a spin relaxation hot-spot [SNS+13] and readout via a controlled rotation and dot 2. It is assumed that waiting $7T_1$ leads to 100% initialization of dot 2.

C) Universal gates

Full single-qubit control above the surface code threshold level has been achieved [MGF+22], where interleave benchmarking indicates 99.95% single-qubit gate fidelities. Before these results, arbitrary single qubits gates are achieved with magnetic and electrical controls, see [TvdWOT06,PLOT+08,TKO+16].

In 2022, two-qubit controlled-Z gates have been realized by two teams with fidelities of 99.8% (taken from interleaved randomized benchmarking) [MGG+22] and 99.65% (taken from gate set tomography) [XRS+22]. To put this into perspective, in 2018 two-qubit gate fidelities were at 98% [HYC+18]. Quantum state tomography of Bell state 85%–89% [WPK+17]. Two-qubit gate (CZ) in 75 ns and CNOT in 75 ns, with T_2* = 120 µs(61µs) and T_2 = 28 ms with CPMG [HFS+20].

With the complete gate set, full benchmarking of two-qubit gates has been done, we have already quoted key data above. Fast single qubit gates are already at threshold with single-qubit RB results for the left (right) qubit 99.3% (99.7%) and 98.8% (98%) [WPK+17]. Gate set tomography leading to improved calibration of single-dot [DMBK+16], with average gate fidelity 99.942% of single-qubit gates. They are compatible with RB data, pointing at no major artifacts in RB.

D) Coherence

Ramsey and Hahn echo measurements for the left (right) qubit T_2* = 1.2(1.4) µs $T_{2,echo}$ = 22(80) µs [ZSR+18]. Spin relaxation time T_1 > 50 ms (= 3.7 ms), T_2* = 1.0 µs (0.6 µs), $T_{2,echo}$ = 19 µs (7 µs) [WPK+17]. Together with the gate time this leads to a coherence limit of gate fidelity based on T_2* of 84%, so gates are coherence limited. The contrast between this and the spin echo time highlights the potential for improvement by composite pulses.

E) Readout

Readout fidelities of 99.76%, verified via gate set tomography, is reported in [MGF+22]. The readout fidelities of the experiments that allow for two-qubit gates are not reported in [ZSR+18] and relatively low with 73% (81%) [WPK+17].

DiVincenzo criteria: summary and estimation of device quality

Table 12.9: Summary DiVincenzo criteria for spins in quantum dots.

Criteria	***met?***	***Comments***
Scalable qubits	✓	***Needs isotopically pure silicon***
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

Analysis and outlook

Si/SiGe qubits meet all DiVincenzo criteria in samples up to 4-6 qubits. The realization of partial error correction in small systems constitutes another significant step forward [TNN+22,vRLR+22]. There do not seem to be any principal obstacles to realizing larger systems.

Gate fidelities on small samples surpass threshold values. Nonetheless, a key challenge of this architecture is to overcome intrinsic charge noise —even though we are fundamentally looking at spin qubits, effects like the exchange interaction or spin-orbit interaction inevitably lead to some orbital / charge structure in the qubit state. Charge noise has been well known for a long time independent of quantum computing, so it cannot be assumed that this is easy to solve. The neighboring Josephson qubit community has overcome noise problems by reducing the impact of noise rather than eliminating the source which could be an option here. Another challenge already described above is to scale the multi-electrode layouts needed for larger processors. Given the proximity of this technology to classical CMOS technology, one can expect shortcuts in operation once these obstacles are overcome.

12.2.3.2 Evaluation: Other quantum dot platforms

Given the consolidation of the field, most other quantum dot platforms are currently not being pursued as they got stuck on level A. For completeness and to provide context if some of these problems are solved, we mention the state of the art. Unless mentioned otherwise, techniques resemble those of SiGe spin qubits.

Double-dot qubits, or singlet/triplet qubits

The single-triplet qubit is pursued as a strategy to overcome the impact of nuclear spin noise hence, it was originally pursued in GaAs which, due to the lack of progress in that platform, is relegated to the previous edition.

However, there were some papers on silicon based singlet-triplet spin qubits which reached coherence times of above T2* = 1µs and single gate fidelities of 0.996 [JJR+22, TNY+20].

Table 12.10: Summary DiVincenzo criteria for spins in quantum dots.

Criteria	***met?***	***Comments***
Scalable qubits	✓	Needs isotopically pure silicon
Initialization	✓	
Universal gates	×	
Coherence	✓	
Readout	✓	

Triple-dot qubits

While developmental efforts based on the GaAs quantum-dot platform has been discontinued, new work is carried out using Si/SiGe materials [BPK+22,WRJ+23]. Here, quantum dots are aligned in a scalable architecture in two dimensions with conventional microelectronic technique.

In [WRJ+23], initialization and measurement fidelities have been reported at 99.75%, while randomized benchmarking results for single qubit operations are fidelities of 99.83%. In the same work, two-qubit operations are not operated at the same quality: the controlled-NOT operation only reaches a fidelity of 96.3%. A higher fidelity of 99.3% was reached only for a non-entangling (encoded) SWAP gate.

Table 12.11: Triple-dot qubits.

Criteria	*met?*	*Comments*
Scalable qubits	✓	Needs isotopically pure silicon
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

12.2.3.3 Evaluation: Donors in Si/SiGe

In [MAY+22] , high-fidelity quantum gates have been realized. The fidelities of single-shot readout, single-qubit gates and two-qubit gates are well above 99%, and thus exceed the error threshold of the surface code. This fact places the donor at the intersection between levels B and C. However, we note that perhaps the main difficulty for this qubit encoding is to scale up the qubit count in a single processor, because there is no established method of placing large numbers of donor atoms at a well-defined inter-donor distance.

In previous work, the coherence time measured using dynamical decoupling is T_2 = 400 µs, and the Ramsey decay time T_2* = 1 µs, RB of single-qubit gates gives 98.99%, initialization and readout times are around 4ms [KJS+16]. Long coherence times of electron and nuclei, see list of records [MDL+14]. The latter motivates the theoretical proposal of the flip-flop qubit [TMS+15]. RB of 99.95% and 99.99% for the electron and the nuclei, respectively [MLS+15]. Gate set tomography yields a fidelity of 99.942% for the same sample [DMBK+16]. Also, conditional rotations (CROT) have been performed [MPBJ20], including CNOT with low fidelities. Besides, theoretical considerations could improve the CNOT fidelity to 99.98% [KRG+23]. These excellent numbers with combined slow progress on two qubit fields are characteristic, but also show strong potential once the bottlenecks have been overcome.

We also note that alternative readout and two-qubit gates have been proposed by coupling donors dispersively to microwave resonators [MPB21,MB23].

Table 12.12: Summary DiVincenzo criteria for Single Donors in Si/SiGe.

Criteria	*met?*	*Comments*
Scalable qubits	✓	Needs isotopically pure silicon
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

12.2.3.4 Evaluation: NV-Centers

DiVincenzo criteria

A) Scalable qubits

The key challenge in this platform is to integrate beyond the two qubits (electron and nucleus) at a single center without sacrificing its great properties.

Coupling NV-center crystals through a transmission line resonator [ANP+17] has been achieved with ensembles, but not with single NV centers. NV center interconnection with optical photons [NTD+14] is very successful [HBD+15], but generates significant overhead. Spacing of NV centers around 10 to 100nm [BSA17] is theoretically achievable. So far, attempts at direct implantation of an array of NV centers have not been successful.

B) Initialization

Initialization takes a 3µs laser pulse [NMR+08] and including waiting times can be done in ≤ 8µs , with a fidelity of ≥ 0.9 [DCJ+07]. Now, so called clean-up operations are used after initialization and fidelities over 99% are doable [HZS22].

C) Universal gates

Single qubit high fidelity (>99,2%) operations can be done in 63ns [DFZC+21] and two-qubit gates with (96%) in 354 ns. However higher fidelities are possible using GRAPE optimization and allowance of longer evolution times yields (single qubit: 0.99995 fidelity in 340 ns, two-qubit gate: 0.992 fidelity in 696 ns) [DFZC+21].

D) Coherence

The typical spin coherence time is 10µs [BSA17]. The phase memory time T_2 is found to be around 0.6ms [NMR+08] with two nuclear spins. Very short coherence of T_2 ~6µs were reported in [JGP+04], but up to 60µs possible. Ground state manifold nuclear decoherence is T_2 = 480µs [BFBA10], and Hahn echo of nuclear spin at T_{2e}* = 495µs[DCJ+07], such that coherence times span two orders of magnitude.

E) Readout

Projective optical readout [RCB+11] at 8.6K has been shown. Nuclear spins are read out by CNOT and electronic spin readout. Electronic-nuclear flip-flop transitions can reduce optical readout fidelity. In principle this allows scaling for multi-nuclear-qubit readout. The average fidelity is 0.93. Single-shot readout fidelities are >0.99 [BGN20] .

DiVincenzo criteria: summary and estimation of device quality

Table 12.13: Summary DiVincenzo criteria for NV centers.

Criteria	***met?***	***Comments***
Scalable qubits	?	Optical link only so far
Initialization	✓	
Universal gates	✓	Local, not long-range
Coherence	✓	Low coherence for long range interaction
Readout	✓	

Outlook

This may be the most controversial evaluation across the range of platforms. NV centers have demonstrated a lot, but not at the same time.

We place NV centers at level C, since several of the relevant milestones have been met. Specifically, quantum error correction for multiple electron spins has been demonstrated in [WWZ+14], and the recent experiment [AWR+22] (described in Section 8.5.3) shows quantum error correction with 7 physical qubits with high fidelity.

We caution, however, that the need for scaling the system systematically is a difficult undertaking for reasons of fabrication difficulties.

12.2.3.5 Evaluation: Topological qubits—Majorana fermions

The setback described above, which negates that even a single Majorana Fermion has been observed (where multiple are necessary to define a qubit) in semiconductor nanowires means that no DiVincenzo criterion is even close to being met. In fact, previous – now considered to be historic - platforms potentially hosting topologically protected state such as Josephson Junction Arrays, Quantum Hall Systems, or vortices in Strontium Ruthenate, must now be considered to be the front runners of topologically protected qubits.

12.2.4 Operational challenges for semiconductor platforms

Materials, fabrication, charge noise

Some of the materials involved are difficult and unsystematic to fabricate, i.e., in mass production there is a question of yield. GaAs films are grown by molecular beam epitaxy (MBE) by specialized growers [PWW+05,PTR+17,BHP+14,YSP14,RFB+10]. Silicon fabrication leverages techniques from commercial fabrication and, based on limited experience, is more reliable [CSF+21]. For spin qubits, isotopic purification is required which is a laborious and expensive but unproblematic process. Nanowires for topological quantum computation are grown in a process that, again, only a small number of groups master. The process of contacting them is currently not scalable but is not the primary concern of these systems. Beyond the material, a current challenge is the layout of large multi-qubit systems: While on the one hand the small size and footprint is viewed as an advantage [VBC+17] it hinders tight integration of the many electrodes needed to define quantum dots.

Cold electronics, complexity

Challenges related to cryogenics as well as to microwave resemble those in Josephson qubits. Cold CMOS logic is pursued as a cold control layer and first demonstrations have been successful [XPvD+21]. This implies that both platforms can simultaneously profit from cold electronics and therefore combined research resources can help find new solutions.

Readout

Not a problem in general but a higher attention is needed. The higher complexity on the chip increases the distance of the qubits and therefore increases gate-times.

Coherence

Charge noise is one of the major challenges to circumvent, cryo-electric semi-conductors have higher coherence, but the super-conducting require more space. Densely packed qubit arrays are not scalable for larger number of qubits. This is why the field is looking into high range interactions techniques such as moving electrons.

13 Atomic and optical platforms

13.1 Quantum computing based on trapped ions

Trapped ions are among the most promising candidates for the realization of quantum computers and quantum simulation. They are currently leading the field in both number of qubits and gate quality. The hyperfine levels in the ground state of the ions that encode the qubit have high coherence times and can be controlled with lasers.

13.1.1 Basic notion and terminology

This platform is part of atomic, molecular, and optical (AMO) physics. The qubits are encoded in the quantum states of single electrons in the outer shell of a positively charged ion. Given their positive charge and the relative strength of achievable electrostatic forces, there is a well-defined handle to trap ions. It is in fact possible to hold ions trapped very close to a well-defined position and spaced far enough so the ions can be individually addressed externally to drive gates with only limited and easy active cooling. This technology has been originally developed for a number of applications including metrology in the form of atomic clocks, which is compatible with the requirements of low error rate posed by quantum computing. It turns out that the trap is intimately related to the coupling of qubits hence it will be described under the qubit heading. Ion trap setups are typically placed on large vibration-isolated optical tables and operate in ultrahigh-vacuum systems and are addressed by lasers.

13.1.2 Various types of ion-based qubits

A) Ions

Simple atomic ions with a single valence electron such as alkaline earths and particular transition metals are used for storing qubits. The choice of ions is driven by the desire to only have a single electron in the outer shell of the atom after ionization, hence ions used are earth-alkali metals (second column of the periodic table) such as Be^+, Mg^+, Ca^+, Sr^+, and Ba^+ [MK13][Bra17] as well as a few transition metals (Zn^+, Cd^+, Yb^+, and Hg^+). The atoms have to be isotopically pure for the trap to work (see there) which is natural as all ion evaporation techniques can be made mass selective. Choice of ion is driven by the preferred way to drive single qubit rotation (see there) and within that range by convenience of lasers and other devices used to manipulate the electrons. The amounts of material are minimal, scarcity is not a problem even if the preferred isotope is not the most abundant. Quantum simulation with trapped ions [BR12, KCK+10, JLH+14] is another driver for technology development.

There are limited applications of molecular ions currently in quantum simulation but not in quantum computing besides few very early basic investigations [DM12].

B) Trap technologies

While the electrostatic force is very strong on the atomic scale and allows for excellent access to the motion of the ion, it is not possible to hold an ion in a stable position due to electrostatic force alone, a fact known as Earnshaw's theorem in electrodynamics. Solutions to this problem involve the use of slowly time-dependent field that compensate for any instability by synchronization to the motion of the ion (this synchronization requires the ion mass to be known, i.e., the ion system to be isotopically pure). There are several common technologies to achieve this.

The linear Paul trap

Named after Nobel laureate Wolfgang Paul [PS53], and reviewed in [Pau90], this trap holds ions in a linear crystalline (i.e., nearly evenly spaced) string in a quadrupole geometry. It is the current workhorse of ion trap quantum computing given its excellent optical access and the relatively small amount of metal needed.

Its linear geometry and the resulting potential instabilities and vibrations of the ion string lead to the expectation that the current world record of 14 entangled ions [MSB+11] achieved by the Blatt group exhausts its capabilities - even if more ions can be trapped, it is unclear whether they can be coherently manipulated.

The Penning trap

The Penning trap is an ion trap mostly used in high-energy physics applications. Although it allows to trap 2D-arrays of qubits for quantum simulation with ~ 300 ions [BSK+12], it lacks addressing and control of individual qubits and is not currently implemented for quantum computing [BKM16].

Surface traps

In surface traps, all electrodes are part of a flat, segmented metallic surface providing potentials similar to that of a Paul trap [KMW02]. The segments can be controlled separately allowing to move and transport ions on top of the surface, hence not facing the limitation of 1D ion crystals imposed in Paul traps and allowing for much more flexible scaling and implementation of quantum algorithms [HLBH11]. As a general trend, linear surface traps can perform close to regular Paul traps and at least Sandia has reported high-fidelity two-qubit operations in a segmented trap at the APS March meeting in March 2017 [Mau07], but not published yet. More details are described below. Also, 2D surface traps are an active research field [SRW+14].

C) Single-qubit gates, encoding and control

There are multiple approaches to identify what states of the ion are used as qubit states. These are driven by the trade-off of long and stable quantum coherence and accessibility for control.

The optical qubit

Qubit logic states are encoded in fine structure levels of the ion separated by frequencies that are in or close to the optical range. In order to maintain quantum coherence, the state that is higher in energy is metastable and can only decay through rare quadrupole transitions, with the flip side being that rather strong lasers are required to drive single qubit gates. The most common ion in this application is ^{40}Ca and it is used by the Blatt group (Innsbruck University) and its many alumni. Fault tolerant topological encoding in Paul traps with 7 ions [NMM$^+$14] and repetitive quantum error correction [SBM$^+$11] have been demonstrated. Early basic studies attempt to use the Rydberg levels of an ion [FBS$^+$15] (Rydberg physics is described below for neutral atoms).

The hyperfine qubit

Qubit logical states are encoded in hyperfine levels of an ion. These are states of the electron that are differentiated only by their interaction with the atomic nucleus but otherwise are both part of the ground state manifold of the system. This makes them immune to decay and leads to enormous coherence time > 1000s [BKM16], 50s without magnetic shielding [HAB+14]. Their transition frequency is given by the properties of the ion and is in the microwave frequency range (12.6 GHz for $^{171}Yb^+$). Gaps to hyperfine splitted excited electronic states lie in the optical regime and allow for laser access for Doppler cooling to confine the ion near the bottom of the trap. To drive these microwave transitions with lasers, a scheme called Raman drive is used, which has the transition frequency as a difference of two (generally much higher) laser frequencies. The single qubit gates can be made ultra-fast ~ 50ps [CMQ+10] and robust [RWL+18]. Recently, microwave-based quantum gates [MW01,LWF+17] were proposed and implemented in conjunction with static magnetic field gradients, making lasers unnecessary for single qubit gate operations (see under scale-up and technology).

D) Entanglement and two-qubit gates

Local operations

The electrostatic Coulomb interaction between ions is used for entangling gates. Ion strings have, very much like a string of pearls connected by springs, collective modes of vibrations that can be used to couple ions, even over long distances. The original Cirac-Zoller gate [CZ95] is used as well as the Mølmer-Sørensen gate [SM00] which has the advantage of being independent of the background vibration of the ion string. Qubit superposition is transformed to superposition of the ion's position mostly done with laser fields to perform two-qubit gates [BW08a]. The gate speed in a string of N ions is proportional to $N^{-1/2}$ implying slower gates in longer chains, with typical gate times ~ 10--500µs [BHL+16]. These were improved using frequency modulation [LLF+18]. In surface traps, these gates would be implemented between short strings of qubits that are assembled using qubit transport for the gate of interest. Individual optical addressing and pulse shaping techniques enable error-correcting encoded qubits [MK13], with up to 100 qubits. Given these limitations, further scaling of that type of limitation requires functional surface traps. Alternatives rely on microwave control fields [OWC+11,TBJ+11] using microwave dressed states which are robust against magnetic field noise.

Very recently, high-speed (0.2ns) gates that do not rely on the Coulomb interaction have been demonstrated with promising yet not leading fidelities [WMJM17].

Long-range operation by communication

As an alternative to surface traps, long-range communication via photonic links is used for two-qubit gates in a distributed network of manageable-size Paul traps [MK13]. As most photonic methods (see there) these protocols involve post-selection, i.e., some operations are executed probabilistically. The overhead for this mode of operation is not problematic for scaling statements, albeit practically quite substantial. The conversion from stationary to flying qubits, i.e., quantum state transfer from an ion to a photon, has been demonstrated [SCB+13], as well as quantum teleportation between two ions via photons [OMM+09].

E) Initialization and read-out

The electronic fine-structure ground state is easily initialized by simple cooling given its large energy separation. Initializing hyperfine states requires a laser-driven technique called optical pumping [Kas50, Kas67]. Readout is performed by attempting to drive a transition between one of the computational states and an auxiliary state and collecting the resulting fluorescence using photodetection (electron shelving technique) [MSW+08]. All these techniques are well established and reliable but require additional lasers.

13.1.2.1 Scalability and peripheral elements

The first proposal of a quantum charge-coupled device (QCCD) [KMW02] for scaling beyond ~100 qubits assumed a large number of interconnected ion traps. It introduces interaction regions for logic operations and memory region for storage. Shuttling of ions between these smaller trapping zones requires exquisite control of shuttling ion positions. Also different types of ions are used for gates and transport [HHJ$^+$09, BKM16]. A different approach is based on microwaves ion trap X-junction arrays [LWF+17] with different zones, microwave-based gate zones, readout zones and loading zones, using global laser fields for state readout and fast ion shuttling. Short distance ion transport was discussed in [BOV$^+$09].

A) Trap heating

For scaling up and operation it needs to be noted that anomalous heating is a problem not completely understood yet [BKRB15]—ion traps in vacuum heat up in time hence perturbing everything that is trapped in them. Known to be an effect of the metal surface, this can be addressed using surface science, for example with in-situ ion bombardment [HCW+12], but also by minimizing the amount of metal used in the trapping system. Reduction of noise can also be achieved by using cryogenic traps [LGA+08]. Inevitable

Johnson noise [Joh28, Nyq28] can be almost completely canceled in high-temperature superconducting surface ion traps below the critical temperature.

B) Lasers and temperature

The precision of the ion trap setups requires high stability of the ambient temperature, below 0.1K. This is in parts because of the important role of the trap that cannot tolerate any thermal expansion. The sophisticated techniques behind the different steps of these setups, including gate drive, optical pumping and readout require a multitude of lasers at different frequencies. Also, the motion of the ions needs to be constantly cooled. Other than in solid state setups, cooling here is not done by heat exchange with a coolant such as Helium, rather, by further laser-based techniques [Phi98]. This leads to very complex setups containing many lasers all of which consume power (not a big problem per se as this only grows slowly with the number of qubits) but most importantly all of which dissipate heat. This requires, in most cases, to operate lasers in a separate room, contributing to the complexity of the system. A separate problem is anomalous heating of the trap, which is only partially understood.

C) Vacuum systems

Ion traps need to be operated in ultrahigh vacuum, as the motional degrees of freedom used for two qubit gates cannot tolerate collision with residual gas atoms. While small ultrahigh vacuum units as part of the research infrastructure are reliable routine equipment, new challenges arise when these grow to large volume.

D) Crosstalk

When driving operations, qubits need to be clearly addressed, i.e., it is important to make sure that controls are qubit specific. The absence of this capability is called crosstalk. Achieving this with lasers requires spacing out ions by more than a focus area hence preventing dense packing of the ions. Solutions include avoiding crosstalk via different types of atomic species, such as $^{171}Yb^{+}$ and $^{138}Ba^{+}$ [BKM16]. They also include selecting hyperfine transitions by frequency by putting the ions into a strong static magnetic field.

13.1.3 Evaluation: Ions

DiVincenzo-Criteria

A) Scalable qubits

The largest devices are the IonQ chain with 79 qubits and complex algorithms executable on a sub-chain of 11 ions. Quantinuum (Fusion of Cambridge Quantum and Honeywell) has a fully connected 20-qubit device.

The total number of qubits that can be manipulated in a single ion trap, or chip, is expected to be limited. One route to scalability is to enable a modular approach by transferring single ions from one trap to another. Reference [ABL+23] achieves such a high-fidelity connection between ion trap chips. However, we note that the device realized in that work is limited to kHz frequencies, which would slow down the trapped ion computer.

B) Initialization

- Default initialization method is Doppler cooling and additional sideband cooling $^{43}Ca^{+}$ [SBT+17].
- Doppler and sideband cooled and optically (re)pumped $^{9}Be^{+}$ ion(s) [BWC+11,GTL+16], sideband cooling [BHL+16].
- $^{40}Ca^{+}$ qubit reset in 50(10)µs with error 5×10^{-3}, with expected values in parenthesis [BXN+17].

C) Universal gates

- Gate times are in the range of microseconds for both single and two-qubit gates
- Shortest two-qubit gate is done in 700ns [ZPL+20], faster gate operation can be achieved by use of Rydberg like interactions
- 99.9999% fidelity in [Harty14] for single qubit gates
- Fast 99.9% fidelity for two-qubit gates is demonstrated in [SBK+21] and is doable with infidelity of 6e-4 in 35µs for Ca_{40}^{+} Ions [CTS+21].
- LASER free approaches caught up in terms of fidelity and 99.99 % are doable with them but they still require much longer pulse times
- A summary of some of the latest experimental devices can be found in TABLE I. of [BCMS19]

D) Coherence

- Coherence time is nowadays typically in the order of one minute for atomic clock states
- T_2 = 0.38s [BWC+11] with $^{9}Be^{+}$.T_R = 1.5s [GTL+16].
- T_2* = 50s [HSA+16] for $^{43}Ca^{+}$.
- Coherence times in segmented Paul trap and $^{40}Ca^{+}$ ions enhanced by dynamical decoupling to 1.1s [KRS+17].
- Coherence time of 1000s for $^{171}Yb^{+}$ [FSLC97]. $T_2 \approx 0.5$s magnetic field noise [LMR+17] in hyperfine ground-level qubits. Suppressing magnetic-field noise for improvisations.

E) Readout

- Individual qubit measurement of $^{171}Yb^{+}$ with nearly 99% efficiency [ZPH+17].
- Measuring the fluorescence signal [GTL+16] with $^{9}Be^{+}$ single-qubit readout fidelity is 99.7(1)% for state $|0\rangle$ and 99.1(1)% for state $|1\rangle$
- Average readout fidelity for an entire 5-qubit state is 95.7(1)% ,limited by because of crosstalk [LMR+17].
- Measurement of $^{40}Ca^{+}$ in 400(30)µs with error 10^{-3} [BXN+17].

DiVincenzo criteria: summary and estimation of device quality

Table 13.1: Summary DiVincenzo criteria for trapped ions.

Criteria	***met?***	***Comments***
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	Focus on faster readout

Table 13.2: Optimistic assumptions for different error rates and operation times combining the best reached values for each operation. This does not describe a current available setup but shows what is in principle possible right now or in near future. Times are given for initialization, 1- and 2-qubit gates, and measurement. Probabilities are error

probabilities for the respective processes. A surface code cycle contains 4 two-qubit gates, 2 one-qubit gates, measurement, and initialization as well as classical processing.

t_I	t_1	t_2	t_M	p_I	p_1	p_2	p_M	T_2
50µs	2µs	10µs	30µs	$5 \cdot 1s0^{-3}$	$5 \cdot 10^{-5}$	10^{-3}	10^{-3}	1s

Fault-tolerance extrapolation

Ion trap systems are among the leading platforms in quantum error correction. They typically do not use the surface code, but the similar color or other adapted codes. The status of error correction experiments in ion traps is reported in Section 8.5.

As a guideline, ion traps enjoy very low error rates, but are challenged by a rather slow clock speed of their two-qubit gates and slow readout compared to superconductors.

Analysis and outlook

Trapped ions are extremely clean and flexible controlled quantum systems which in the context of atomic clocks have reached metrological precision, hence providing an excellent platform for high-quality quantum operations. They are currently the most consistent platform in reaching the error correction threshold and thus most definitely in category C. This platform advances continuously. It is currently working on overcoming a steep scaling obstacle: Changing trap technology from Paul to surface traps while maintaining high operational quality.

A) Resources: Space and time

Both measurement and gate times in trapped ions are quite long. While due to their excellent coherence this does not impede high-fidelity operation (level B), it does affect overall algorithmic performance and, given the effectiveness of error correction, eats up the lower overhead. Thus, the needed processor sizes for cryptographic tasks are comparable if not larger than for Josephson qubits. A further challenge is the size of the surrounding apparatus: While ions are small, ion traps are not, hence again, the required machine is comparable to Josephson qubits.

B) Technical feasibility

An excellent analysis that we agree with has been described in [LWF+17]. Brute-force scaling up of an ion trap quantum computer to the required sizes for attacks on cryptography would lead to a machine the size of a soccer field and include the challenge of engineering a large ultrahigh vacuum system. Its power consumption (dominated by trap currents) would be comparable to that of a supercomputing facility. Again, this would be a focused and visible research project comparable to the Apollo or Manhattan programs. Rare materials are not needed. As industrial uptake of ion traps is slower than for solid-state platforms (mostly for reasons related to leveraging existing computer technology), crypto-related ion trap research will likely profit less from industrial activities than solid-state programs.

C) Trapped Rydberg Ions

While brand-new and currently incomplete, it is worth pointing out the alternative route of using Rydberg ions. On a $^{88}Sr^{+}$ ion in a linear Paul trap the π-phase gate has been determined by quantum process tomography with a fidelity of 0.78 [HPZ+17], using double STIRAP (sequence Stimulated Raman Adiabatic passage) and a lifetime of the Rydberg state of τ_{42S} = 2.3µs.

13.2 Quantum computing based on trapped neutral atoms

13.2.1 Basic notions and terminology

The field of neutral atom qubits uses electrons in atomic shells to carry quantum computing. These atoms are not ionized but neutral, hence not containing the possibility to couple to them with electrostatic forces to trap and couple them. This challenge can be used to structure the field. The lack of electrostatic interaction also means lack of electrostatic repulsion allowing to bring atoms very close together, which allows fast gates and dense packing of atoms. Over the last years, Rydberg gates have emerged as the only serious candidate for neutral atom quantum computing. We will also describe the approaches of collisional gates and of cavity quantum electrodynamics, which are seriously pursued for quantum technologies other than quantum computing as well as fundamental research. We will describe the obstacles that would need to be overcome to be quantum computing contenders.

13.2.2 Platform designs: Rydberg atoms

It needs to be stated upfront that despite their name, Rydberg atoms are by no means special atoms - they are atoms prepared in so-called Rydberg states.

A) Qubits

The qubit states are encoded in electronic states of the atoms of interest. In order to have only one atom in the outer shell and the resulting simple spectrum, Alkali metals are used. The particular states that are used are hyperfine states, i.e., ground states split by interaction with the atomic nucleus. This scales with the number of protons Z as Z^4 hence motivating the use for heavy elements like i.e., Rb and Cs*. Dark states can also be used to minimize intermediate state scattering errors.*

The atoms need to be held in a specific place to be addressable and the qubits to be well-defined. This is accomplished with laser-induced dipolar forces, an indirect effect, which are intrinsically very weak. [SWM10]. Given the weakness of trapping forces, active cooling (again by lasers) using a variety of methods is imperative and loss of qubits still a risk. Motivated by neutral atoms research, the impact of qubit loss on error correction is currently being studied [Smi16].

The central device to combine trapping and cooling is called magneto-optical trap (MOT). Holding qubits by light makes it natural to produce regular qubit arrays by trapping with standing waves, however, local addressability by laser led to systems with larger lattice spacing such as bottle beams [IIS+13] (light beams with high intensity in a tube, similar to the outside of a bottle) and other geometries.

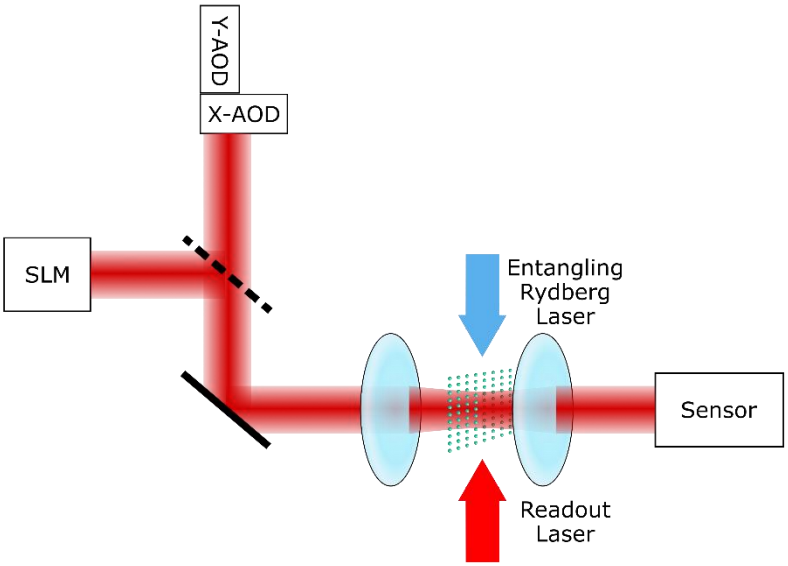

Figure 13.1: Schematic of a neutral atom platform, inspired by [EWL+21]. Atoms are set in ab optical tweezer array defined by a spatial light modulator (SLM) arranging them through use of a pair of crossed acousto-optical deflectors (AODs) in a 2D lattice. Two driving lasers come stimulate the lattice to provide necessary operations: gates and readout.

A new development is to combine these traps with optical tweezers. These work with the same dipole forces but provide a stronger trapping potential and individual addressability. Optical tweezers are well-known (see also the 2018 Nobel prize) but only recently were they made compatible with quantum technology [LKS+19] and more details can be found in [Ash97, SM85].

New techniques involve moving atoms from the MOT to an optical tweezer array defined by a spatial light modulator (SLM) arranging them through use of a pair of crossed acousto-optical deflectors (AODs) in a 2D lattice, which can be arbitrarily defined. Improvements are regularly brought to the experimental setup [BEG+24]. A schematic of the experimental setup inspired by [EWL+21] is presented in Figure 13.1. This general mode of operation allows the qubits to be moved around, hence the implementation of algorithms is not limited by connectivity of qubits fixed on a chip.

B) Operations, Rydberg gates

Single qubit operations are achieved with the same techniques as in trapped ions. Two-qubit operations are based on Rydberg blockade [SWM10, Saf16, BBL16, RLB+14, PBA14]. An electron is in a Rydberg state if it is prepared in a state of very high principal quantum number, i.e., to energies very close to ionization, typically to values of n = 50…100. The size and dipole moment scales with n^2, and the interaction strength scales with n^4 for long-range dipole-dipole, and n^{11} for short-range van-der-Waals interaction.

Driving atoms into Rydberg states is achieved by precisely tuned lasers. By choosing which atoms are driven through Rydberg states, gates are made selective and given the long range of the dipole-dipole interaction which decays only with distance cubed, these can be long-range. Initialization and measurement are performed analogous to that in trapped ions. Two qubit operations can be further selected through physical displacement of neutral atoms arrays, increasing coupling between chosen qubit pairs [BLS+22]. The combined operation of surface code and atom array displacement is reproduced in Figure 13.2.

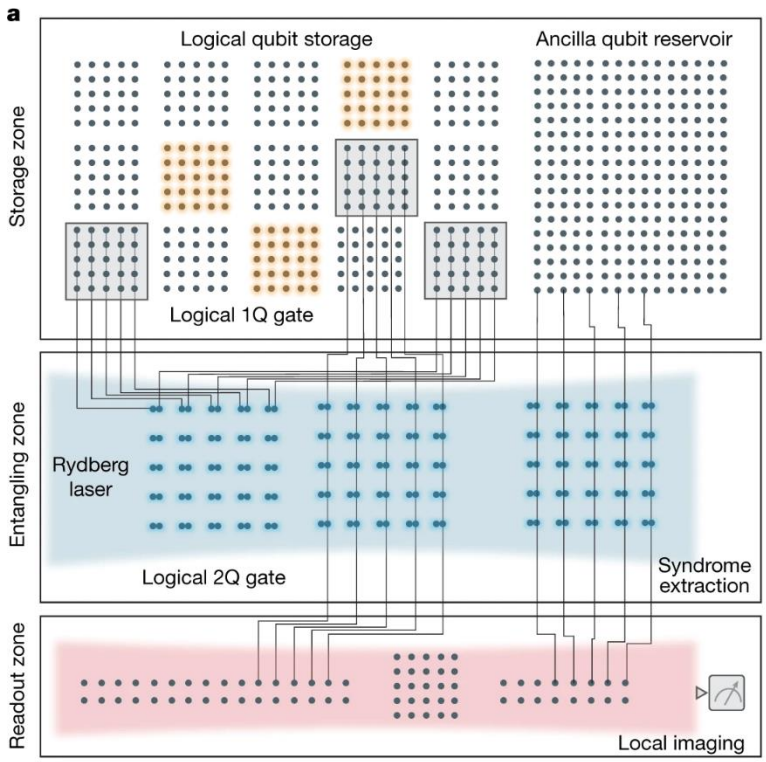

Figure 13.2: Schematic of the operation of the neutral atom platform as depicted in [BEG+24]. Logical qubits are moved in unison from storage to the entangling zone to perform operations, while preserving the surface code structure.

Currently, spinoffs of quantum simulations have made strong progress in Rydberg atom-based quantum computing, notably involving the companies Q-Era, Atom Computing, and Cold Quanta (USA) as well as PASQAL (F). Here, one forgoes in the first step individual addressability of qubits, but with this simplification reaches large qubit arrays. This can e.g. natively implement NISQ algorithms like QAOA for certain restricted graphs, which however are NP hard. This is important if cryptanalytically relevant NISQ algorithms are discovered while the implementation of simple algorithms and applications has already been demonstrated [GSS+22, EWL+21].

C) Status of the field and challenges

Currently, physics problems need to be solved for Rydberg atoms. One is improvement of atom loading into their traps, cooling, and long-term storage—qubits still disappear or never appear. Also, gate quality needs to improve. The NISQ-driven approach outlined above is however a strong contender in that domain.

Collisional gates

As an alternative to Rydberg gates, two-qubit interactions can be implemented using collisional gates [MGW+03,NTC11,ALB+07]. In this case, the trapping field holding the atom is manipulated such that atoms come in close contact, comparable to the length of a molecular bond, i.e., with overlapping electron clouds. The energetics in this state depends on the internal state of the atom, a phenomenon called Feshbach resonance. This approach is highly successful in cases when a lot of two-atom interactions need to be controlled in parallel, i.e., in quantum simulations in optical lattices, where the whole trapping laser field can be moved as a whole. It has been proposed to extend this to quantum computers by moving atoms with a selective optical tweezer - a beam of light that uses dipole forces to interact with the neutral atom similar to the optical lattice but is tightly focused [WKMS11]. Typical moving times of rearranging arbitrary 2D

arrays of Rydberg atoms are 50 ms [BdLL+16] and an interaction strength of neighboring atoms in the MHz range. These tweezers are developed for low speed in quantum simulations, fast optical tweezers needed for gates are a far-fetched projection [WKMS11]. Collisional gates have not been considered a promising route to quantum computing since the establishment of Rydberg gates.

Cavity quantum electrodynamics

Cavity quantum electrodynamics with neutral atoms uses the coherent interaction between atoms and photons, single quanta of light. It is primarily a very clean platform for basic research in quantum physics [HR06,Har13] and has applications in quantum communication [Kim08]**.** Its basic functional element are neutral atoms in Rydberg states are sent through cavities in order to precisely interact the photonic state of the cavity. As this was an early coherent and controlled quantum system, quantum computing proposals were put forward, either using atoms as qubit and cavities for interaction or vice versa. Given the enormous size of the cavity (which is dictated by the requirement to have modes that are resonant with Rydberg transitions) and the complexity producing these, scaling to any reasonable size processor is not pursued. The tools of cavity quantum electrodynamics have been taken over to other approaches involving cavities, specifically circuit QED, described with superconducting qubits. They can also be used for long-distance gate in quantum networks [WHD+18].

13.2.3 Evaluation: Rydberg atoms

DiVincenzo criteria

A) Scalable qubits

Quantum gates with a fidelity above the error correction threshold have been performed for a set of up to 280 atomic qubits trapped and manipulable in a 2D lattice, opening the path to efficient quantum algorithms implementation in the near future. The experimental setup is highly scalable as the trapping and control are executed by an SLM and a 2D AOD, regardless of the number of trapped atoms, providing a scalable control setup for qubits. Optimal control techniques are considered to minimize errors and decrease operation time during atom shuttling [BEG+24].

B) Initialization

Laser cooling and optical pumping leads to state preparation fidelities of 0.95 [JHK+16].

C) Universal gates

Single qubit gates with RB have average fidelities of 0.9991 in 2D [BEG+24] using ^{87}Rb atoms. Single qubit gates with RB have average fidelities of 0.998 in 2D [XLM+15] and 0.996 in 3D [WKWW16], using ^{133}Cs atoms. Bell-state fidelity to verify two-qubit gates have been shown with fidelity 0.79 [MLX+15] and 0.81[JHK+16] in ^{133}Cs, and 0.634 in ^{87}Rb [KLFF+15]. Optimal control methods might help to improve two-qubit gate fidelities [TMWS16]. Two-qubit gates are either performed via Rydberg-blockade [MLX+15,JHK+16] or local spin-exchange with optical tweezers [KLFF+15]. Two qubit gate fidelity reaches 0.9954 in ^{87}Rb [EBK+23] on logical qubits delocalized on a 2D array of neutral atoms, with SPAM correction.

D) Coherence

Coherence time in ^{133}Cs has been confirmed to be $T_2' = 7$s in [WKWW16] and $T_2^* = 7$ms in [XLM+15]. Effective coherence time reaches more than 1s with ^{87}Rb [BLS+22]. Lifetimes of the Rydberg state are around 40µs [JHK+16].

E) Readout

Readout through measurement of the fluorescence signal similar to ion traps. Local imaging fidelity reaches 99.8%, taking into account possible atom loss for ^{87}Rb [BEG+24].

DiVincenzo criteria: summary and estimation of device quality

Table 13.3: Summary DiVincenzo criteria for Rydberg atoms.

Criteria	*met?*	*Comments*
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	High fidelity two-qubit gates
Coherence	✓	
Readout	✓	

Outlook

A blueprint for a fault-tolerant quantum computer built of optically trapped Rydberg atoms has been developed [ABB17], aiming for 10^4 qubits. Recently, gate fidelities as well as atom loss rates have reached a level where these extrapolations are no longer speculative—level C.

13.3 Operational challenges for atomic and ionic platforms

Size

On a 30mm chip is enough space for about 10-100 qubits, meaning space is not really an issue for the ionic platform. Currently the total consumed space including LASERs, control electronics, computer hardware and vibration-isolation for 20-30 qubits can be packed into two server racks.

Power Consumption

The two racks are currently using about 1.7 kW for 20-30 qubits, scalable up to ~100 qubits meaning a low power consumption of 20-80W per physical qubit. Assuming 20W per qubit this would scale to a power consumption of 20 MW for a million-qubit device. This is comparable to large high performance computing centers like Frontier which consumes ~21 MW. Additionally, saving potential lies in the use of diode-based LASERs because they have better efficiency converting electric power into light (up to 60% efficiency).

Power dissipation and temperature stability

Since the power consumption is very low dissipation is a minor issue. Additionally, the chamber containing the qubits is in ultrahigh vacuum so heating of the ions can be reasonably suppressed.

Cycle Time

Cycle time is one of the biggest issues for ionic quantum computers. Entangling gates can be executed in a few microseconds [Schaefer18], but 50-500 µs is the usual time scale, while single qubit gates can be executed in a few µs. This is already reflected in the temporal estimates.

Ion transportation meanwhile has a similar timescale, meaning that the overall clock time of the platform is in the order of a kilohertz.

However, new ideas such as using Rydberg interactions for entangling gates have shown significantly improvement towards a timescale of hundreds of nanoseconds [ZPL+20].

Classical data flow

This issue is most pressing in connection to error correction: As the code and control layer of a quantum processor are classical, one is faced with the need to process data fast and close to the device in a way that grows with computer size. While this is not a problem in general (realization in server racks makes it possible to access nearby infrastructure easily), the platform is still facing the problem of how to bring many (classical) signals to the processor in a way that is both scalable and not error prone.

Reliance on rare materials

There are no rare materials required for an ionic quantum computer.

Vacuum

Trapped ions use their motional degree of freedom for quantum gates which is at odds with collisions with gas molecules. Given outgassing of materials, one needs to ask to what point vacuum infrastructure can be enlarged. However, single traps are not in need of high volumes and there exists the possibility to couple multiple traps with photonic interconnections.

Stability

Unless accommodated in error correcting codes suitable for these problems, these issues can be lethal: Losing a qubit with probability p per unit time means losing a qubit with probability $1-(1-p)^N \leq Np$ in a large quantum computer per unit time, effectively limiting algorithm run-time to (Np)-1 time units. However, this is also a rather small issue for ionic systems because their charge allows for reliable trapping. With current devices and new control techniques it is possible to trap ions reliable for a duration on the order of days [SVE+20]. However, it is still questionable if this is still true if devices are scaled up to a million or more qubits.

Yield and scatter

On a level lower than instability, one needs to make sure that the production of a quantum computer is reliable. Ions naturally have reliably the same transition frequencies and there are almost no differences in the qubit system itself. Instead, there are more issues related to the peripheries like reliable optical fibers and couplers to bring the photons to the system.

Addressing and coupling is not a crucial point, but it limits the size of a single chip to about 100 qubits due to optical resolution, which gets worse if you pack too many qubits in a small area.

Further Challenges

In the ionic platform one of the biggest challenges is the integration of all components into a working system. It would need decent control of the qubits and therefore require transporting many (classical) control signals in a scalable way to processing ions. This is why the ionic platform will make significant progress if there are new developments in the field of classical control electronics.

Another challenge is the need of progress in enabling technologies.

One of them is the development and production of waveguides in the 400-700nm range of wavelength of light, because these are the typical transition frequencies of the ions. In this context there is still little choice, series production is expensive and hard to find industrial partners for.

Also ongoing is the search for trap materials which do not oxidize and transitions within ions which can be used as qubits or for doing gates between them.

While energy consumption and scarcity of materials are not problematic, the search for qualified employees is and the instruction of new people is taking a long time. Missing interdisciplinary exchange does make the hiring process even more difficult. In this context there are also problems in finding good, risk tolerant investors and converting ideas into real-world applications.

Extrapolation to future devices

Recent developments hint that the number of simultaneous controllable qubits is scaling linear in time with a rate of about one qubit a year meaning that if we assume roughly ten physical qubits per logical qubit and a need of at least 2000 logical qubits to attack cryptographic methods it would take roughly 20000 years till a device would meet the required criteria. Furthermore fault-tolerance requires T-gate injection meaning one qubit initialization per gate! This is why it needs more innovative concepts such as the usage of surface traps which could allow for accelerated scaling.

13.4 Quantum computing based on photons

13.4.1 Basic notions and terminology

Photonic qubits comprise qubits that are encoded in quantum states of the light field. The structure of this field is given by a very unbalanced set of quantum computing resources: While light is very flexible to use and can be very coherent, and while single qubits can be easily manipulated with optical elements (mirrors, phase shifters, beam splitters), photons are not known to interact with each other (classical electrodynamics described by Maxwell's equations in vacuum is a strictly linear theory), leading to no natural pathway towards a two-qubit gate. Approaches to photonic qubits can be classified by the way how they work around this challenge. While some of these methods try to imitate matter qubits as much as they can, some others are using different computational models that in parts are not compatible with our evaluation scheme. Remarkably, the technological strengths of photons in many other quantum technologies have attracted investments specifically to the second group of quantum computers based on exotic computational models. Next to this aspect, evaluation is further hindered by the secrecy of some actors. An operational peculiarity is that, given the immense size of the speed of light, manipulating photonic states in time is very challenging, thus most proposals focus on arranging a quantum algorithm in space.

Note that boson sampling [AB16a,AA13,LBH+16,CHS+15] is known as a road to quantum supremacy that is very well adapted to the capabilities of linear optics. It aims at outperforming classical computers in the application of computing the permanent of a matrix but is believed to not have any applications beyond that (nor has computing the permanent any cryptographic implication), Boson-Sampling can thus be considered a synthetic benchmark whose ingredients may be transferable to more general quantum computers. Quantum advantage has been claimed by [ZWD+20] using Gaussian states (see below under continuous variables) with 50 photons. Canadian company Xanadu has advanced this even further and their technologies allows programming – that is, programming of the matrix whose permanent is computed. Later theoretical research has found a classical algorithm specifically designed for simulating Gaussian Boson sampling going up to 92 photons [BBC+22] and reducing the simulating time for state-of-the-art GBS experiments to a few months hence almost canceling the quantum advantage. However, the research on Boson sampling still provides important benchmarks for the underlying components [MLA+22].

13.4.2 Qubit encoding

There are multiple methods to encode quantum bits in the light field [OFV09]. One is the use of mode occupation. A mode of the light field is a classical solution of Maxwell's equations typically characterized by its spatial structure and polarization-type properties. In quantum optics (quantum field theory in the limit of non-relativistic matter) [Fox06], the quantum states of these modes are described analogous to harmonic oscillators, with the degree of excitations being interpreted as the number of photons.

In this framework, binary encodings of qubits in single photons are most natural for quantum computing. In polarization encoding, a single qubit is encoded in the polarization state (right circular or left circular) of an otherwise identical spatial mode. In dual-rail encoding [KLM01], polarization is not used, rather, the presence or absence of a photon in a spatial mode, for example in arms of an interferometer, defines qubit states. The main challenge is to produce the qubits, as deterministic on-demand single photon sources are difficult to implement (even despite the best efforts of the photonics and quantum cryptography communities).

An alternative encoding is Gaussian quantum information [BvL05, WPGP+12]. There, quantum information can be encoded in semiclassical coherent states that are widely separated [RGM+03]. These states are naturally produced by lasers and can be separated using phase shifters. Their nonorthogonality in the form of a small overlap can be compensated for, furthermore there are protocols that make it easy to correct errors caused by photon loss [CMM99]. An even more exotic approach is using squeezed states for continuous variable quantum computing, where the computational basis consists of all squeezed eigenstates of some quadrature variable [BSBN02]. These states can be produced from coherent states using nonlinear elements.

13.4.3 Enhanced nonlinear optics, integrated optics

One way how photons can interact with each other is by using nonlinear optics [Boy03]. Nonlinear optics describes the interaction of light with matter in a way that the matter mostly introduces nonlinearity into the Maxwell equations. These naturally lead to terms in the quantum optical Hamiltonian of powers larger than quadratic in photon amplitudes. These terms are interpreted as effective photon-photon interaction. An example is the Kerr effect, the dependence of the index of refraction on light intensity. This leads, e.g., to four wave mixing, the scattering of two incoming photons into two outgoing photons, hence naturally implementing a two-qubit gate. Another nonlinear interaction is two-mode squeezing, which leads to correlations in the quadrature amplitudes of two modes that can be used in continuous variable quantum computing.

This approach is challenged by numbers. Even very effective nonlinear materials such as barium-borate in samples that are thin enough to not absorb the photons have conversion efficiencies below 10^{-6}, making two-qubit gates hugely ineffective on the single photon level.

Proposed solutions include confining the light to very small volumes using cavities and integrated optics (i.e., optics on a chip rather than discrete optics) [HBR+16,PLP+11]. This uses the concept of *mode volume:* The energy of a photon of frequency ν is inevitably $h\nu$. The energy density per volume, on the other hand, is E^2/ϵ_0, thus the typical electric field of a photon is $E \simeq \sqrt{h\nu\epsilon_0}$ /V. Stronger fields can exploit nonlinearities more. Another perspective is that confinement of light into a slightly open cavity makes the photon cross the nonlinear medium many times, giving it more opportunities to interact. Some of these approaches use atoms in cavities as a nonlinear medium. While impressive science, the success probabilities of these direct gates by engineered nonlinearity are still too low to be practical [FFE+08,FEF+08].

13.4.4 KLM proposal

The Knill-Laflamme-Milburn proposal [KLM01] is a very elegant approach to avoid the use of optical nonlinearity and replace it by the (also nonlinear) resources of single photon generation and detection as well as post-selection. The key element is the nonlinear sign (NLS) gate—a gate that conditions a phase shift on the number of photons—that is simulated using ancilla modes and that is only carried out with 1/4 success probability, but this success is certified by ancilla detection. Two of these NLS gates can be combined into a two qubit gate. The overhead of probabilistic gates and post-selection does not alter the complexity class of algorithms, but increases the hardware effort in practice. To be viable, the data qubits are held in optical memory, the entangling gate is performed on ancilla qubits and once successful, the data are teleported. The KLM gate has been demonstrated [OOHT11] with a process fidelity of 82% that has been gradually improved [MBB+16] and is currently at 99.69% [SXZ+22].

13.4.5 Cluster states, one-way quantum computing and fusion-based quantum computing

At face value, the teleported KLM protocol creates an entangled ancilla state and teleports data on it. This idea can be taken to its extreme the concept of an ancilla factory in preparing all entanglement non-deterministically first and, if successful, proceed with the computation only through measurement and single-qubit operations [BR05]. This one way quantum computing approach, originally proposed by Raussendorf and Briegel [RB01] is equivalent to regular quantum computing. Cluster states can be generated using parametric downconversion in nonlinear crystals [WRR+05], coupled quantum dot emitters [ELR10] or, in the continuous variable case, from frequency combs in nonlinear media [FMP09]. In fact, large cluster states have been produced, yet functional one-way quantum computing which also requires photonic memory has not been implemented. The so far largest cluster state was realized with over one million modes by continuous variable entanglement [YYK+16], 30,000 entangled modes in a 2D structure [LGB+19], while in the discrete (conventional) case, the cluster size is still in the order of several photons [WRR+05,SCS+16].

This concept has been taken to the next level by the idea of Fusion-based quantum computing [BBB+21] promoted by the company PsiQuantum (and believed to be the computational model underlying their hardware developments). In this approach, entangling measurements (e.g. Bell-Basis measurements) which are a hardware primitive in linear optics are used as the main element of the quantum computation, acting on a highly entangled resource state (a generalization of the cluster state described above). It is shown that this model allows for fault-tolerant computation using topological ideas similar to those underlying the surface code and have high error tolerance. However, in this one publication, component performance indicators that would allow to gauge the progress of PsiQuantum are not described and they look daunting with a long ramp-up phase. PsiQuantum is also not publishing performance data but relies on press releases for communication, making them hard to evaluate. They also use integrated optics – not for enhancing nonlinearities but simply for reducing the physical footprint of their devices.

Dutch company Quix is using integrated optics in an original way to make programmable array of linear elements that can be combined with the required sources and detectors to implement KLM-derived and cluster state proposals. So far, only that part – validated by Boson sampling – has been published, not this additional integration. The interfaces are well-developed [GSV+22, TAG+22]

13.4.6 Continuous variables

The continuous variable encoding has already been described above. It encodes information in squeezed states and uses the squeezing effect for two-qubit gates, a nonlinear mechanism based on the Kerr nonlinearity that entangles the field amplitudes of both modes. The gate is usually performed by a two-mode squeezing process [CMP14], or by combining (one-mode) squeezed states of light at beam splitters [YUvLF08,SHD+13]. This can be more effective than using nonlinearity for single photons. Creation and measurement of the qubits can be performed with current experimental equipment (creation via lasers and nonlinear media, measurement with homodyne detection).

13.4.7 Evaluation

13.4.7.1 Evaluation: Single photons

Many elements of processing single photons are developed in the framework of optical quantum communication and cryptography but can be useful also for quantum computing. Furthermore, single photons are good candidates for flying qubits in distributed quantum computing, as they can interact with other, fixed qubits.

DiVincenzo criteria

A) Scalable Qubits

Single photon sources are available using single atoms/ions [HSG+07,KLH+04], color centers in diamond [MMK+12,BKH+17], quantum dots [LDP+17], or optical parametric oscillators [KGPUK16] (e.g. nonlinear crystals) combined with heralding. All optical elements can in principle be integrated on chips [HDM+16], which makes scaling more reachable. Especially because performance of silicon photonic components and integrated circuits has improved both in size and quality in recent years [XJH+21].

A problem arising in all encodings is leakage due to photon loss. Also, a number of these strategies occupy a comparably large amount of space.

B) Initialization

Initialization is usually done directly with the creation of the photons.

Direct creation of entangled photons is also possible for example with parametric down-conversion and beam splitters, cluster states of up to 6 photons have been created in several groups, although fidelities are still to be improved [ZHL+16,LZG+07]. Larger cluster states, and on-chip generation are a matter of ongoing research.

C) Universal gates

A universal gate set is available; however, entangling gates are typically non-deterministic and require additional post-selection. Single-qubit gates with free-space optical elements are typically very fast and accurate.

- direct two-qubit gates F_2 = 0.87 [OPW+03], 0.894 [XMC+22]
- KLM: CZ gate with 0.68 (0.93) process (Hilbert-Schmidt) fidelity [MBB+16], entangling gate fidelity of 99.69 [SXZ+22]
- on chip: CNOT with 0.94 fidelity [PCR+08]
- three-qubit gate: controlled-SWAP gate with fidelity 0.85 [OOT+17], 95.4 [WRW+21]

D) Coherence

The most limiting effect is photon loss, leading to leakage. Apart from loss, photons usually have high coherence times and only weak interaction with their environment. It needs to be noted that the use of media and integrated optics reduces photon lifetime [HBR+16].

E) Readout

Readout is done with photon detectors. When polarization encoding is used, the polarization information can be translated to dual-rail encoding with polarizing beamsplitters or polarization filters. Photon detectors still need to be developed in terms of photon-number resolution, efficiency, dark count rate and speed. Since single photon detectors are required in a lot of different situations, this is still a field of active research.

DiVincenzo criteria: summary and estimation of device quality

Table 13.4: Summary of DiVincenzo criteria for single photons.

Criteria	*met?*	*Comments*
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	

Criteria	*met?*	*Comments*
Coherence	✓	
Readout	✓	

Outlook

Single photons quantum computing fulfills all DiVincenzo criteria, thus is a level B platform, but still in an early stage as the ability for larger algorithms or error correction is not yet reached. Major efforts in scaling, loss-reduction, photon indistinguishability and deterministic gates would be necessary to lift this platform on a higher level. Also for cluster states, due to the probabilistic nature of entangling gates, scaling to larger computations is still the biggest problem.

On the other side, the increasing demand for secure communication, pushing research in single photon quantum key distribution techniques, might also bring up some benefits for universal quantum computation.

13.4.7.2 Evaluation: Continuous-variable and Gaussian encodings

Continuous-variable encoding is mainly used in the framework of one-way quantum computing, where in principle, two-qubit gates are not required on-demand, but only as an initial process in the creation of the cluster. However, keep in mind that protocols for merging clusters (as described in Section 9.2.2), which will be inevitable in large algorithms, also use additional deterministic (or at least high probability) entanglement operations on demand.

An important measure is the strength of the initial entanglement gates. When using two-mode squeezing processes, this is given by the squeezing strength.

Cat states are currently still at the stage of (bad) quantum memory: They can slightly increase the coherence time, but good protected (multi-qubit) gates that make additional error correction redundant are still far. Furthermore, scaling is challenging since every qubit needs its own cavity.

DiVincenzo criteria

A) Scalable Qubits

Creation of huge cluster states is not a problem but creating them with sufficient fidelity is. States as large as 10^6 qubits in a CV cluster state [YYK+16] have been created, with the possibility of creating even larger states, however, most states are still below 10 qubits.

B) Initialization

CV cluster states can be created with optical parametric oscillators using for example entanglement between modes of a frequency comb [MFZP07,MdARC+14,FMP09] or time multiplexing [YYK+16].

Both methods set a limit on the number of “qubits”, either in time or due to the frequency window available experimentally.

Cat states or other coherent encodings in resonators can be initialized by external coupling, for example to a transmon qubit.

C) Universal gates

In the one-way quantum computing scheme, gates are already included in the initialization and measurement process. For coherent state encodings, single-qubit gates already work quite well, two-qubit gates are problematic:

- Hadamard gate on coherent states with 0.94 state fidelity [TDL+11]

- cat states, controlled via transmon: universal single-qubit gates with 0.985 fidelity in 1μs from RB and 0.9925 process tomography [HRO+16]. Two-qubit gates are proposed [MLA+14], and have just been realized [RGR+17] with a process fidelity of 0.83.

D) Coherence

Unprotected states are typically vulnerable to single photon loss, destroying for example superpositions of coherent states.

Cat code qubits are protected against photon loss, the limiting factor is the coherence time of the transmon coupled to the resonator. Error corrected cat states reach T_1 = 2.7ms [HRO+16].

E) Readout

- homodyne detection, can measure arbitrary quadrature (meaning arbitrary basis for two-mode squeezed cluster states)
- coherent states stored in oscillators can be read out with transmons

DiVincenzo criteria: summary and estimation of device quality

Table 13.5: Summary DiVincenzo criteria for CV and Gaussian encodings.

Criteria	***met?***	***Comments***
Scalable qubits	✓	
Initialization	✓	
Universal gates	✓	
Coherence	✓	
Readout	✓	

Outlook

For continuous variables, two qubit gates have barely been demonstrated. While in principle protected, fidelities are actually below any known error correction threshold. Improving these will be crucial. Level B.

13.4.8 Operational challenges for photonic platforms

Space

Given that here gates are performed in space, by sending light through an apparatus representing the algorithm, optical quantum computers need more physical space the longer the algorithm becomes. With discrete optical elements this becomes forbiddingly large, also given the overhead of post-selection. Integrated optics creates elements of sizes comparable to other qubits (but still adding a time dimension).

Photon sources

All discrete-variables need single photon-inputs [VBR08]. Single-photon sources that are deterministic (i.e., we know when a single photon is coming) and on-demand (i.e., we can trigger injection of a photon) are a field of current research and are most likely reached with self-assembled quantum dots [SSA+15,SFV+02] .

Appendix

14 Example: Digitized adiabatic quantum computation for factoring

Hegade et al. introduce a quantum factoring algorithm within the digitized-adiabatic quantum computing paradigm [HPAA+21HPAA+21]. In this type of computing, an adiabatic quantum algorithm is implemented on a digital quantum computer rather than on an adiabatic quantum computer or a quantum annealer. We evaluate the algorithm of Hegade et al. in Section 5.2.1. Here, we give details on how the factoring problem is encoded.

Suppose we are given an input biprime number N, which is a product of integers p and q, i.e., $N = pq$. The basic idea of the procedure of [HPAA+21HPAA+21] is to encode the prime factors of N into the ground state of a Hamiltonian, denoted H_1, acting on a collection of qubits. To arrive at such a Hamiltonian, consider the task of finding the prime factors x and y of a biprime, $N = xy$. This leads to the introduction of a cost function for the optimization problem,

$$f(x,y)=(N-xy)^2.$$

Using n_x many qubits to represent x, and n_y many qubits to represent y, we write quantum operators $X = \Sigma_{i=0}^{nx} 2^i(I-\sigma_z^{(i)})/2$, and, similarly, $Y = \Sigma_{i=0}^{ny} 2^i(I-\sigma_z^{(i)})/2$, where $\sigma_z^{(i)}$ is the Pauli-z matrix acting on qubit i, and I is the 2x2 identity matrix. This results in the Hamiltonian

$$H_1(X_1, X_2, \ldots, X_{nX}, Y_1, Y_2, \ldots, Y_{ny}) = (N-XY)^2,$$

which acts on $n = n_x + n_y$ qubits.

An alternative method for obtaining a problem Hamiltonian H_1, which encodes the prime factors p and q in its ground state, is to consider the "longhand" binary multiplication table of pq. This exercise, referred to as classical preprocessing, yields a set of equations that define p and q. Simplification of these equations, which can be accomplished efficiently in $O(\log(N)^3)$ steps (see, e.g., the supplementary material of [XXL+17]), leads to a set of clauses, which can be used to generate a Hamiltonian H_1 whose representation requires significantly less qubits than the one described above. White the number of required qubits in the former case (without preprocessing) requires $O(\log(N)\log(\log(N)))$ qubits, for the latter case it has been found empirically that $O(\log(N))$ many qubits are sufficient [AOGC19].

In the paradigm of adiabatic quantum computing, the set of qubits is initialized into the ground state of a starting Hamiltonian H_0 whose ground state is known and which must fulfill $[H_0,H_1]\neq 0$. For example, initializing all qubits to the "0" state results in the initialization of the Hamiltonian $H_0 = \Sigma_{i=1}^{n} \sigma_x^{(i)}$, where $\sigma_x^{(i)}$ is the Pauli-x matrix for qubit i. The computation then consists of slowly deforming the Hamiltonian H_0 into H_1 over a duration T, or realizing the instantaneous Hamiltonian

$$H(t) = [1-s(t)]H_0 + s(t)H_1,$$

where $s(0)=0$ and $s(T)=1$, such that the starting and final Hamiltonians are, respectively, $H(t=0) = H_0$ and $H(t=T) = H_1$. The adiabatic theorem states that if this manipulation of the system Hamiltonian is carried out sufficiently slowly, the quantum state will remain in the ground state of the instantaneous Hamiltonian [Kat50,Mes67]. Ideally, measurement of the n-qubit state at the end of the calculation yields the ground state of H_1, and thus the desired prime factors p and q.

15 Introduction to surface code quantum error correction

In this Appendix we present details on error correction and the realization of quantum gate in the surface code. We first describe how to correct and stabilize the substrate state in Section 15.1. This strong protection requires extra effort to compute within the states, which is described in Sections 15.2 and 15.3.

15.1 Error syndromes

15.1.1 Single errors

Given that the stabilizer measurements detect X and Z errors independent of each other, the surface code can also detect Y errors as a combination of an X and a Z error. Single (physical) qubit X or Z errors always lead to a change of the two adjacent stabilizer measurements: An X error on a qubit a will lead to a sign change of the measurement outcome of the operator product $Z_iZ_jZ_kZ_l$ for $a \in \{i,j,k,l\}$, and no change for X stabilizer measurements, analogous an Z error will lead to a sign change only in the corresponding X stabilizer measurements. Thus, each pair of neighboring X or Z stabilizer measurement sign changes can be identified with an Z or X error, and sign changes on all four stabilizer outcomes around one data qubit therefore corresponds to an Y error. There is no need for an extra consideration of errors that are not Pauli operators, since the stabilizer measurements will map all qubit states to either the original state or to a state with a Pauli operator applied to it. Take for example an error of the form $|\psi\rangle \rightarrow (\alpha \cdot 1_i + \beta \cdot X_i)|\psi\rangle$, acting on one qubit of the array. The stabilizer measurement will map the state $(\alpha \cdot 1_i + \beta \cdot X_i)|\psi\rangle$ to either $|\psi\rangle$ (i.e., directly projecting to the error-free state) or to $X_i|\psi\rangle$ (i.e., creating but also detecting an X error at qubit i), depending on the amplitudes α and β. In general, any code that can correct a set of error operators can also correct any linear combination of them [Bac13]. A detailed and more general discussion of this is found in Chapter 22 in an older version of this study [WSL+20] or reference [Bac13, Section 2.6].

A special case happens at boundaries, where a data qubit is only surrounded by three measurement qubits, and therefore an error can lead to a sign change of only one stabilizer measurement. This is the case for an X error next to a missing Z stabilizer or a Z error next to a missing X stabilizer.

15.1.2 Error chains

Whenever two identical errors happen to neighboring data qubits, the effect on the measurement qubit in between will cancel out, so one will only detect sign changes at the two outer measurement qubits. Similar, for longer error chains, only the measurement qubits at the ends of the chain will show an effect. This is not a problem if the chains are not too long and there are not too many errors along the array. Then, one can deduce the error chain leading to a several measurement outcome by error path with the highest possibility to occur. However, if errors get too dense, the stabilizer results might be misinterpreted, and the syndrome extraction algorithm will correct a wrong path. This is not a problem as long as both paths can be topologically deformed into each other (i.e., without crossing any holes - needed for logical qubits, or changing connections to boundaries) since the changes resulting from original error + correction will then only be a closed (empty) loop of sign flips which does not change the logical state.

A worse case are error chains that start and/or end at boundaries (as will be shown, deactivating stabilizer measurements and introducing additional boundaries is a fundamental part of the computation process in the surface code). If the sign changes at the ends of a chain fall on two deactivated or not existing measurement qubits of the same kind (X or Z), the error chain remains undetected: Along the chain, all sign changes cancel out and at the ends, sign changes are not measured. This is already a problem if only one end lies at a boundary and the other is close to a boundary. In general, whenever more than half of the qubits along a chain connecting two boundaries have an error (all of the same kind that is not measured at the corresponding boundaries), then this will result in a logical error, since the syndrome extraction algorithm will misinterpret the sign changes and correct the wrong qubits (see Section 15.2). A more

detailed analysis of the impact error chains can be found in [FSG09]. The physical mechanisms leading to error chains are also discussed in the Appendix.

15.1.3 Measurement errors

A faulty sign change of a stabilizer measurement can also be caused by an error of the measurement qubit. Since for every surface code cycle the measurement qubits are reinitialized, such an error will probably vanish in the next round (see also [FMMC12], Section V) unless there is a massive correlation. Similar to spatial error chains it is, however, possible that such an error occurs multiple times in a row (with very low error probability). This might look like a real sign change instead of an error on the measurement qubit. Interpreting this the right way is part of the classical software layer of error correction.

To distinguish between measurement and data errors better, it is necessary to compare several rounds of syndrome extraction and see if a sign change stays or withdraws in the next round: If the changed sign remains a single event (or very rare), it is probably due to an error on the measurement qubit and can be ignored. So, in general, more fault-tolerant implementations will not only need more qubits but also more time-steps during which syndrome measurement is activated. Fault-tolerant computation includes turning syndrome measurements on and off, so the main implication of being able to detect measurement errors is that whenever a syndrome measurement is turned off (i.e., a measurement qubit is not used), after reactivation it needs to stay active for several rounds of error correction—the more, the better.

15.1.4 Syndrome extraction

The errors that are most likely to cause a measured syndrome are found by Edmonds' minimum-weight perfect matching algorithm [Edm65], which basically matches all sign change events to pairs (for two sign changes in the same basis) or connections to a boundary with shortest possible chain lengths. In order to include measurement errors, which correspond to pairs of sign changes in time, the algorithm uses a three-dimensional space-time lattice, as shown in Figure 15.1.

The basic approach takes an equal error probability for all possible errors, always assuming the shortest possible path leading to a given error syndrome to be the right one—it involves the lowest number of errors. However, it has been shown [FWMR12] that, considering different probabilities for different errors to happen, more accurate handling of errors and less misinterpretation is possible.

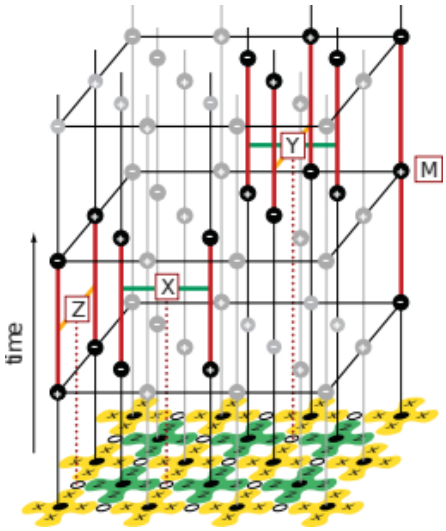

Figure 15.1: Three-dimensional space-time lattice of syndrome measurement outcomes. One horizontal layer corresponds to one round of syndrome measurement, where the signs indicate the outcomes. Red lines show where a change of measurement outcome occurs. A single error (X or Z) of a data qubit leads to a neighboring pair of sign changes in a spatial dimension—with the faulty data qubit lying in the middle, a single error on the measurement qubit leads to a pair in temporal dimension—with the error happening between the two changes (M). Error chains lead to pairs of sign changes lying further apart [FMMC12]. Reprinted figure with permission from [FMMC12] Copyright (2012) by the American Physical Society.

15.2 Logical qubits and Pauli operations

The computational subspace still has two degrees of freedom, describing a logical qubit and one can find two operator products (linear independent of the stabilizers and commuting with them) to define a logical basis. A logical X operator can be defined by choosing a path connecting two data qubits from the two X-boundaries and performing *X* operations on all data qubits on the path - this does not change the outcome of any stabilizer measurement. The same can be done for a logical Z.

For a bigger number of qubits implemented in the same lattice, one can create holes in the array, meaning that some measurement qubits are turned off and do not measure the corresponding stabilizer of the surrounding data qubits anymore. These holes act like additional boundaries, and give extra degrees of freedom. Usually, logical qubits are implemented using two holes of the same type. This also leads to two types of qubits: The so-called double X-cut qubit (sometimes called rough or primal qubit) consists of two deactivated measure-X qubits, with the logical Z consists of a path of Z operations connecting both holes, and the logical X of a loop of X operations around one of the holes. An equivalent construction can be done for the double Z-cut qubit (sometimes also called smooth or dual). Both types of qubits with their corresponding logical operators are shown in Figure 15.2.

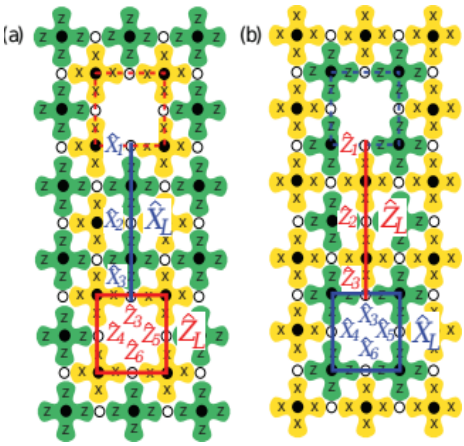

Figure 15.2: Implementation of logical qubits: (a) Double Z-cut qubit, (b) double X-cut qubit. The logical operators XL (ZL) consist of X (Z) operations on the physical qubits along the blue (red) lines [FMMC12]. Reprinted figure with permission from [FMMC12] Copyright (2012) by the American Physical Society.

Similar to detected errors, in realistic implementations logical X or Z operations do not actually need to be performed by doing all the single qubit gates but can rather be carried (and commuted) through the control software.

15.2.1 Distance

The distance *d* of the logical qubit is determined by minimum number of physical operations needed to perform a logical operator—up to $n = \lfloor (d - 1)/2 \rfloor$ errors can be corrected, larger order errors (i.e., including more physical qubits) might be misinterpreted as a logical operator. For even distances, an error chain of half a distance cannot clearly be corrected since the decoder has to guess. Thus, one usually uses odd distance codes. The distance of a logical qubit can be increased by putting the holes further apart, although with this approach the maximal distance is limited by the number of qubits around the hole to $d = 4$. However, one can also make the holes bigger by turning off more qubits and thereby reach arbitrary distances. The number of physical qubits thereby is quadratic in the desired distance—not only must the two holes corresponding to the same qubit be separated far enough (for which an increase of qubits in one dimension would suffice), any pair of holes of the same kind (X/Y) must be separated by at least *d* data qubits to prevent from undetectable errors. However, a Z cut and an X-cut can be close because they have different kinds of boundaries, and an error chain beginning at one kind of boundary cannot end at the other without leaving a trace in the stabilizer measurements.

In an array of only one kind of logical qubits, the number of physical qubits per logical qubit is quadratic in the distance, for single-qubit holes it is $n(d) = 8d^2$. For larger distance it is slightly more, according to the

extra rows and columns needed due to bigger holes. We can lower-bound the number of required physical qubits by $n(d) = 8(d + d/4)^2$: We need holes of width $\geq d/4$ to ensure that an error chain around a hole has minimum length d and additional d data qubits to separate holes from each other. Additionally, we need a factor 2 due to the arrangement of qubits, a factor 2 for measurement qubits and a factor 2 since one qubit consists of two holes.

Keep in mind that this is only the spatial distance: One must also preserve the distance in time, so for a distance d code, the temporal spacing of operations that involve turning off measurement qubits (for example logical initialization or measurements, see Section 15.2.2) must also be at least d to distinguish between measurement and data errors. Measurement errors (any error on the measurement qubit, see Section 15.1.3) vanish after the next initialization, whereas a data error leads to a sign change that persists. If one wants to also detect the rare cases of measurement errors happening in a row, the number of measurement cycles must be larger than the biggest temporal error chain one wants to detect.

15.2.2 Logical initialization and readout

A logical X (Z) operator surrounding one of the holes of a double X (Z)-cut qubit is equal to the stabilizer operator that the deactivated measurement qubit in the hole would measure—if it was not deactivated. Therefore, creation and initialization of a logical qubit in one of its corresponding eigenstates can be done easily by just turning off the measurement qubits. The logical state is then given by the previous stabilizer measurement to be in one of the corresponding eigenstates (depending on the measurement outcome of the hole defining the logical operator).

Implementation in the other basis is more complicated. However, it is still easier than performing a Hadamard gate, as will be seen later. The implementation for a logical X (Z)-cut qubit into a Z (X) eigenstate is done in three steps:

1. Turn off all measure-X (Z) qubits along a path, exclude all data qubits along the edge of the thereby created hole also from Z (X) stabilizer measurements (see Figure 15.3 (b,c)) and perform Z (X) measurements on all measurement qubits of the hole
2. Initialize all measurement qubits of the hole to the same (desired) eigenstate of Z (X)

Turn all but two measurement qubits on again, leaving two holes at the edges and switch the stabilizer measurements to measure all four surrounding qubits again.

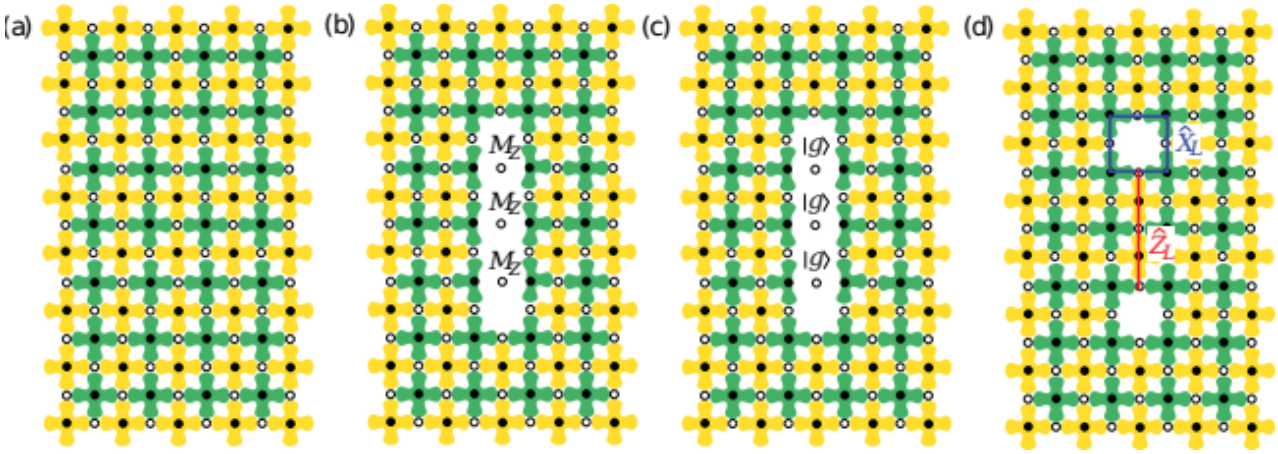

Figure 15.3: Schematic protocol for creating and initializing a double X-cut qubit in a logical Z eigenstate. MZ denotes measurements in the basis of Z, $|g\rangle$ denotes initialization of the data qubits in the ground state [FMMC12]. Reprinted figure with permission from [FMMC12] Copyright (2012) by the American Physical Society.

Measurement works similar to the readout protocol; the easy variant is to measure a double X (Z) cut qubit in the logical X (Z) basis and is performed by turning on the stabilizer measurements for the two holes again—the result of the stabilizer of the hole that defined the logical operator gives the measurement result. For measuring in the respective other basis, stabilizer measurements in between the holes are turned off (or to three-qubit measurements) again, Z (X) is measured for the data qubits along the path—

determining the measurement result—before they are reset and all stabilizers are turned on again and the qubit is destroyed.

15.3 Logical gates: H, T, CNOT

15.3.1 Multi-qubit gates

An interaction between different logical qubits can be achieved by moving holes around the physical lattice. However, the logical CNOT can only be performed between two qubits of differing kind. Usually, this problem is solved by having mainly one kind of qubits, and using the other kind only to transmit the logical CNOTs.

Moving one hole to another position (preserving the logical qubit information) along an arbitrary number of cells in the lattice takes two surface code cycles for the actual move (+ d-1 cycles to preserve fault-tolerance), independent of how far the hole was moved: In the first step, the hole is enlarged up to the final position for the move (so that the initial and the desired final position get linked with a chain of deactivated stabilizers), additionally the data qubits that lie fully inside this large hole are measured. In the second step, the hole is shrunk to its original size, but at the new position by activating all other stabilizer measurements again. To assure fault tolerance at distance d one needs to wait another d-1 steps to identify measurement error chains, so the whole action takes d+1 cycles.

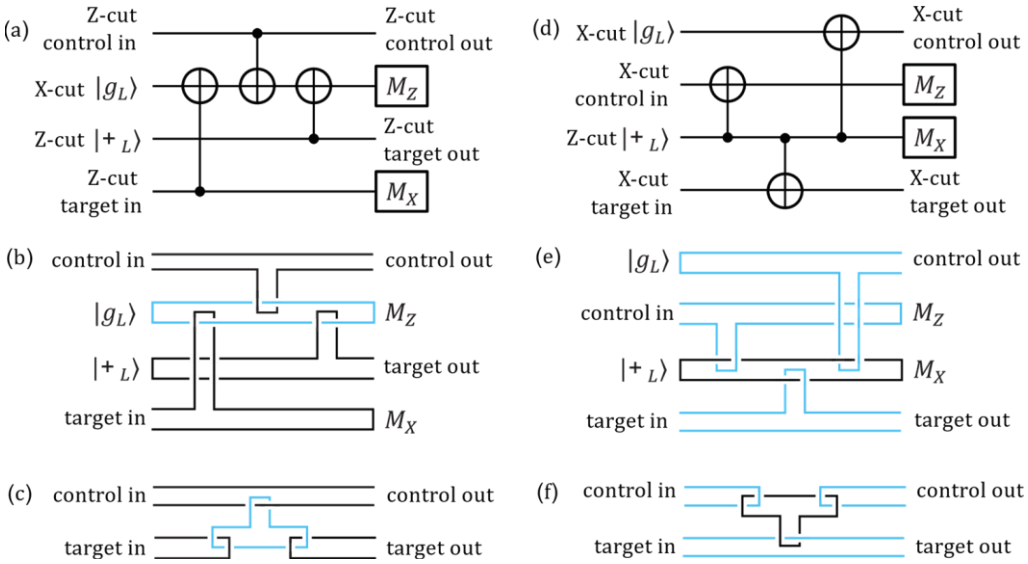

Figure 15.4: (a) Circuit diagram for a logical CNOT operation between two double Z-cut qubits, mediated by a double X-cut qubit. During the process, the target qubit is measured, and a new double Z-cut qubit is initialized in |+⟩ to take the place of the target qubit. (b) Description of the braiding of holes that is done to perform the three CNOT steps: Every double Z(X)-cut qubit is represented by a pair of black (blue) lines, where the movement of the holes in time is shown along the x-axis. Two lines corresponding to two holes of the same qubit join when the qubit is initialized or measured. (c) Simplified representation of the braiding, showing the double X-cut qubit only as an intermediate tool for the gate. In fact, the double Z-cut qubits do not need to be moved at all and the new target qubit can be initialized at the position of the measured old one. (d)-(f) Equivalent representations for an indirect CNOT between two double X-cut qubits. [FMMC12]. Reprinted figure with permission from [FMMC12] Copyright (2012) by the American Physical Society.

To perform a logical CNOT, one needs to move a hole of a double X (Z) cut qubit in a closed loop around a double Z (X) cut qubit, ending up in the initial position after two separate moving steps (i.e., 2(d + 1) surface code cycles). A direct CNOT between two qubits of the same kind is not possible, but one can use one type of qubit to mediate the gate between two qubits of the other kind, as shown in Figure 15.4. Therefore, three concurrent logical CNOT operations (6(d+1) cycles), two logical measurements and initializations (only constant time cost) and one additional logical qubit (but with different boundary, so without extra space cost) are required. Measurement and initialization are always in the complicated basis with respect to the qubit type. Given that holes can be moved arbitrary far, there is no fundamental constraint on how far the

target and control qubits are away from each other. An application of an CNOT between two qubits of the same kind does not require any physical qubit overhead since the mediating qubit can be created arbitrary close to the other qubits. A schematic representation of the stabilizer measurement pattern for a mediated CNOT between neighboring qubits is shown in Appendix 25.2 of [WSL+20].

In the same manner, also multi-target CNOTs are possible by just braiding a mediating qubit around more than one target qubit. This can be done in the same amount of steps as the regular CNOT.

15.3.2 Hadamard

The Hadamard gate does not need additional qubits but additional physical gates on the underlying physical qubits between the syndrome measurement cycles. Besides multiple ($O(d)$) stabilizer measurements after some of the actions to preserve spatial distance, one needs to

- isolate an area around the targeted qubit by turning off stabilizers on a ring large enough to preserve the distance inside[17]
- deform the operator loop around one of the holes to an operator chain connecting the two new outer boundaries
- reduce the size of the isolated area to a $d \times d$ (data qubit) array between the two holes by deactivating even more stabilizer measurements
- perform Hadamard gates on all data qubits in the isolated region (simultaneous)
- perform SWAP operations between all data qubits and their neighboring measurement qubits (this happens in two steps operating first between vertical and then horizontal pairings - during each step, all SWAP gates are performed simultaneous)
- turn on some of the stabilizer again to create two holes and deform an operator chain to get a double cut qubit again, but now rotated by 90°
- move the holes to rotate the double cut qubit to its original orientation
- turn the stabilizers on the isolating ring back on.

Thus, the logical Hadamard gate can be performed in $O(d)$ overall time steps, requiring the ability to perform simultaneous physical Hadamard and SWAP gates, respectively. A detailed study of the logical Hadamard gate can be found in [FMMC12], or in a more schematic way in Appendix 25.2 of [WSL+20].

15.3.3 S and T gate: Magic state distillation

The T gate, which brings the so far available set of gates out of the Clifford group, thus making computation universal and classical not simulable, is the most challenging one. The T gate, as well as the S gate (with $S = TT$) needs an ancilla qubit prepared in a so-called magic state (which is not an eigenstate of X, Y or Z) and logical Hadamard + CNOT operations between the ancilla and the targeted qubit. The S gate can be done deterministic with one logical Hadamard and two logical CNOTs. The T gate, which requires only one logical CNOT, however, only works in 50% of the attempts and performs the logical operator $T^\dagger$ in the other case. This can be detected by measurement of the non-used qubit (the desired state is on the ancilla qubit in the end - the initial targeted qubit can be measured) and compensated for by a subsequent S gate. Both the S and T gate implementations are described in Figure 15.5 as a general circuit diagram—in the surface code implementation, everything will be on a logical level.

The hardest part is the fault-tolerant preparation of the magic state ancilla. There exists no logical gate or initialization protocol to directly create the desired states for a distance d qubit when $d > 1$. Thus, the only way is to use a distance 1 qubit for the time of initialization (for which a physical operation on the data

[17]The ring can be placed directly next to the surrounding qubits without the need to include additional physical qubits anywhere. This is no problem in terms of fault tolerance if the surrounding logical qubits are all of the same type since the boundary of the ring is set to be a different one.

qubit between the two cuts is equivalent to a logical operation on that short qubit) and enlarging it immediately to the desired distance. This procedure will inevitably lead to a reduction of fidelity for this qubit given by the actual physical error rate of the qubit between the cuts, but the states can be made much more precise through distillation, for example with the Steane or Reed-Muller encoding [BK05] or the more recent Bravyi-Haah protocol [BH12]. These codes use multiple faulty (but in our case still logical) qubits to create one or several more precise qubits, a process which can be repeated until the desired fidelity is reached. In the first round, the logical magic states from the distance-1 creation process are used, subsequent rounds use the former purified output states to generate an even more precise state. The distillation codes need only—eventually multi-target—(logical) CNOT operations, (logical) state preparations and (logical) measurements in Pauli eigenstates, so the overhead is mostly due to the high number of logical ancillae and repetitions needed. The exact distillation circuits can be found for example in [FMMC12, Section XVI].

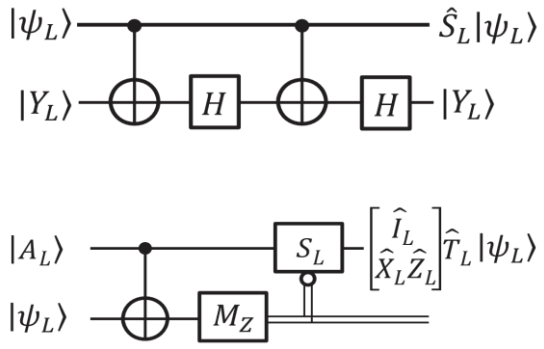

Figure 15.5: Implementation of S (top) and T (bottom) gate on the input state |ψ⟩ with magic states |Y⟩ and |A⟩, respectively. In a more recent version, the S gate can also be performed without the final Hadamard gate, carrying a byproduct operator in the classical control [GF17]. The T gate additionally needs a conditional S gate to correct its non-deterministic nature. The classical process of deciding whether to perform the additional S gate after measuring MZ is represented by double lines. When the S gate is needed, the final state will be XZT|ψ⟩, but the X and Z byproducts can be carried in the classical control. Reprinted figure with permission from [FMMC12] Copyright (2012) by the American Physical Society.

The Steane code [Ste96], distilling the (accurate) ancilla required for an *S* gate needs 7 (faulty but logical) ancilla qubits with an error rate p plus one logical qubit in the state $|+\rangle$(which can be created transversal and therefore fault-tolerant) and creates an output state with error rate $7p^3$, with a probability of $1\text{-}7p$. The process is probabilistic, but the measurement outcomes indicate whether the distillation was successful or not - in which case it has to be repeated with new ancillae. A second repetition will lead to an error rate of $7 \times (7p^3)^3 = 7^4p^9$, though requiring $7 \times (7+1) = 56$ ancillae[18]. This process can be extended to arbitrary length, the error rate scales with the number of repetitions as $P_l \sim p\text{^}(3^n)$, requiring $\sim 7^n$ (faulty) ancillae. One round of distillation can be fit into a space-time volume of $18 \times (5d/4)^3$ (surface code cycles × physical qubits) when implemented on distance d logical qubits [**FD12**].

The Reed-Muller code [BK05] used for the *T* gate ancillae works similar: It creates an output state with error rate $35p^3$ with a success probability of $1\text{-}15p$ from 15 initial ancillae with error rate p and one $|+\rangle$ state. The (physical) space-time volume of one distillation round within a distance d code is $192 \times (5d/4)^3$[FD12]. Additionally, recall that in 50% of the cases an additional high-fidelity *S* gate is required to complete the *T* gate. The volume for the creation of an accurate *S* ancilla is low compared to *T* ancilla, and it can therefore be neglected in overhead calculations.

In typical applications, two distillation cycles are enough to reach the desired error rate. With that, the creation of one magic state ancilla for the T gate requires $15 \times 16 = 240$ logical ancillae. In the first round of distillation, the overhead can be reduced by using lower distance qubits that match the achievable error rate of the ancillae after only one distillation round.

[18] 7 sets of 7 magic state ancillae and one $|+\rangle$ state per set.

Alternatives Instead of distilling ancilla states for performing T gates, it is also possible to distill some (not all) other states that might be required, depending on the algorithm to be performed. One possibility is the creation of ancilla states for Toffoli gates, which are for example required in factoring algorithms. A Toffoli gate can be constructed from several T gates + Clifford gates, however, instead of creating an ancilla for each of those T gates, one can also distill a state with which one can perform the whole Toffoli gate. This is more efficient in many cases [OC17, see for example Table I], but can just lead to a constant factor improvement. The main advantage is time, since the Toffoli gate then only needs one time-step with feed-forward, instead of 3 or four steps for each sequential T gate [AMMR13].

15.3.4 Ancilla factories

For algorithms using bigger amounts of T gates, the creation can be further optimized by creating the ancillae in parallel (for example using the qubits of the first round already for a new distillation in the second round) and offline (if all magic states created in a separate part of the code to be readily available when needed, state distillation does not necessarily introduce any time overhead to the calculation process). Depending on which distillation protocol is used, one [n,k] ancilla factory will produce k high fidelity states from n input states in one round, with a ratio n/k that can be significantly better than 15. One example is block code state distillation: The Bravyi-Haah code [BH12] distills $n = 3k + 8$ input qubits into k outputs with error reduction $p \rightarrow (3k + 1)p^2$ and a success probability of $1 - (3k + 8)p$. The corresponding space-time volume is $(96k + 216)(5d/4)^3$ [FDJ13]. This code only offers a moderate overhead reduction by a constant factor, compared to Reed-Muller. For bigger systems, the worse scaling of error reduction (quadratic instead of cubic) suggests even less benefit. There are optimization approaches improving the efficiency of block-code state distillation, for example via module-checking [OC17]. However, any improvement can only lead to a constant factor reduction of space time costs.

Since the ancillae required for state distillation all need to be logical qubits (except at the time of creation), non-Clifford gates are the ones that consume the majority of physical qubits in a computation process, according to an estimation [FMMC12] for a 2000-bit factoring algorithm, state distillation occupies around 90% of the total number of qubits. Furthermore, also the application of all distillation gates embedded in the surface code will introduce an additional error to the final states, depending on the distance that was used.

15.3.5 Magic state injection

It has been shown in [Li15] that the fidelity of a raw logical magic state can be higher than that of the unprotected (physical) qubit operations creating it. By increasing the distance of the magic state qubit step by step, the final error rate can be made $p_l = 2/5p_2+2p_I + 2/3p_1 + O(p^2)$, with $p_{1(2)}$ being the single (two) - qubit gate error and p_I the initialization error. In typical setups, two-qubit gate errors are by far the largest ones, so the injection error can be approximated by $\approx 0.4p_2$.

15.4 Lattice surgery

An alternative to the described encoding of logical qubits with defects and braids, i.e., in a topologically planar way, is lattice surgery. Lattice surgery here refers to performing operations by cutting and stitching of respective logical qubits as described in [HFDvM12] showing that the storage overhead can be reduced significantly.

The preprint [FG18] reviews how to perform *all* necessary operations for universal fault tolerant quantum computing as well as state distillation using a lattice surgery style qubit encoding. Further they include a section where they talk about state distillation and how to realize it with planar logical qubits using lattice surgery. The main message here is that it is possible to perform state distillation using lattice surgery in a very intuitive way and again save overhead compared to the usually used two defect logical qubits (mostly because of the intrinsic rotation property of planar qubits).

The authors show for one specific dataset (10^8 T gates and 100 logical qubits on a hardware with gate error rate 10^{-3} and surface code error correction time of 1μs) a defect and braiding algorithm needs 4.5 h and 1.8

million physical qubits, whereas using lattice surgery the same algorithm would use 5.4 h but only 0.37 million physical qubits. This is a promising development, yet, in order to become part of our evaluation scheme, a scaling analysis beyond this one dataset needs to be performed by the community

Reference documentation

[AAA+22] R. Acharya et al. Suppressing quantum errors by scaling a surface code logical qubit, 2022, arXiv:2207.06431

[AA13] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9(4):143–252, 2013.

[AAB+19] F.Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R.Biswas, S.Boixom, F. G. Brandao, et. al. Quantum supremacy using a programmable superconducting processor. Nature, 574(7779):505-510, 2019.

[Aar23] S. Aaronson. Of course Grover's algorithm offers a quantum advantage!, The Blog of Scott Aaronson, https://scottaaronson.blog/?p=7143, 2023.

[AB16a] S. Aaronson and D. J. Brod. Boson sampling with lost photons. *Phys. Rev. A*, 93(1):012335, 2016.

[AB16b] A. Auer and G. Burkard. Long-range photon-mediated gate scheme between nuclear spin qubits in diamond. *Phys. Rev. B*, 93:035402, Jan 2016.

[ABB17] J. M. Auger, S. Bergamini, and D. E. Browne. A blueprint for fault-tolerant quantum computation with Rydberg atoms, Phys. Rev. A 96, 052320, 2017.

[ABE58] E. R. Andrew, A. Bradbury, and R. G. Eades. Nuclear magnetic resonance spectra from a crystal rotated at high speed. *Nature*, 182(4650):1659–1659, 1958.

[ABO99] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, STOC '97, pages 176–188, New York, NY, USA, May 4, 1997. ISBN: 978-0-89791-888-6.

[ABL+23] M. Akhtar et al. A high-fidelity quantum matter-link between ion-trap microchip modules. Nature Communications, 14(1):531, February 8, 2023.

[Abr61] A. Abragam. *The Principles of nuclear Magnetism*. Oxford University Press, London, 1961.

[Ach22] R. Acharya et al. Suppressing quantum errors by scaling a surface codelogical qubit, 2022.

[ADL+16] S. Asaad, C. Dickel, N. K. Langford, S. Poletto, A. Bruno, M. A. Rol, D. Deurloo, and L. DiCarlo. Independent, extensible control of same-frequency superconducting qubits by selective broadcasting. *Nat. Partn. J. Quantum Inf.*, 2:16029, 2016.

[AGD+22] M. Ahmad, C. Giagkoulovits, S. Danilin, M. Weides, and H. Heidari. Scalable cryoelectronics for superconducting qubit control and readout. Advanced Intelligent Systems, page 2200079, 2022.

[AGP08] P. Aliferis, D. Gottesman, and J. Preskill. Accuracy threshold for postselected quantum computation. *Quantum Inf. Comput.*, 8:181–244, 2008.

[AGL+18] B. Amento-Adelmann, M. Grassl, B. Langenberg, Y.-K. Liu, E. Schoute, and R Steinwandt. *Quantum Cryptanalysis of Block Ciphers: A Case Study*. Poster at Quantum Information Processing QIP 2018, 2018.

[AHM+16a] D. Aasen, M. Hell, R. V. Mishmash, A. Higginbotham, J. Danon, M. Leijnse, T. S. Jespersen, J. A. Folk, C. M. Marcus, K. Flensberg, and J. Alicea. Milestones toward majorana-based quantum computing. *Phys. Rev. X*, 6(3):031016, 2016.

[AHM+16b] S. M. Albrecht, A. P. Higginbotham, M. Madsen, F. Kuemmeth, T. S. Jespersen, J. Nygård, P. Krogstrup, and C. M. Marcus. Exponential protection of zero modes in majorana islands. *Nature*, 531(7593):206–209, 2016.

[AHWZ18] David D. Awschalom, Ronald Hanson, Jörg Wrachtrup, and Brian B. Zhou. Quantum technologies with optically interfaced solid-state spins. Nature Photonics, 12(9):516–527, 2018.

[AKR10] B. Altshuler, H. Krovi, and J. Roland. Anderson localization makes adiabatic quantum optimization fail. *Proc. Natl. Acad. Sci. U.S.A.*, 107(28):12446–12450, 2010.

[AL06] P. Aliferis and D. W. Leung. Simple proof of fault tolerance in the graph-state model. *Phys. Rev. A*, 73(3):032308, 2006.

[AL07] R. Alicki and K. Lendi. *Quantum dynamical semigroups and applications*. Lectures Notes in Physics. Springer, Berlin, 2007.

[AL17] T. Albash and D. A. Lidar. Evidence for a limited quantum speedup on a quantum annealer, 2017, arXiv:1705.07452.

[AL18] T. Albash and D. A. Lidar. Demonstration of a Scaling Advantage for a Quantum Annealer over Simulated Annealing, Phys. Rev. X 8, 031016, 2018.

[AL18b] T. Albash and D. A. Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, *90(1), 015002*, 2018.

[AL22] D. An and L. Lin. Quantum Linear System Solver Based on Time-optimal Adiabatic Quantum Computing and Quantum Approximate Optimization Algorithm, *ACM Transactions on Quantum Computing* 3(2), Article 5, June 2022.[ALB+07] M. Anderlini, P. J. Lee, B. L. Brown, J. Sebby-Strabley, W. D. Phillips, and J. V. Porto. Controlled exchange interaction between pairs of neutral atoms in an optical lattice. *Nature*, 448(7152):452–456, 2007.

[Ali07] P. Aliferis. Level reduction and the quantum threshold theorem. arXiv preprint quant-ph/0703230, 2007.

[ALK+22] T. I. Andersen et al. Non-Abelian braiding of graph vertices in a superconducting processor, 2022, arXiv:2210.10255.

[ALS10] U. Andersen, G. Leuchs, and C. Silberhorn. Continuous-variable quantum information processing. Laser & Photonics Reviews, 4(3):337–354, 2010.

[APSW23] M. R. Albrecht, M. Prokop, Y. Shen, and P. Wallden. Variational quantum solutions to the Shortest Vector Problem. Quantum, 7:933, 2023

[Amb10] A. Ambainis. *Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations*. arXiv:1010.4458, 2010.

[AMG+16a] M. Amy, O. D. Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck. Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3. In Selected Areas in Cryptography - SAC 2016, Springer LNCS vol. 10532, pp. 317-337, 2016.

[Ami15] M. H. Amin. Searching for quantum speedup in quasistatic quantum annealers. *Rev. A*, 92(5):052323, 2015. *Phys.*

[AMM14] M. Amy, D. Maslov, and M. Mosca. Polynomial-time T-depth Optimization of Clifford+T Circuits via Matroid Partitioning. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33(10): 1476-1489, 2014.

[AMMR13] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 32(6):818–830, 2013.

[AND+17] V. V. Albert, K. Noh, K. Duivenvoorden, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang. Performance and structure of bosonic codes, 2017, arXiv:1708.05010.

[ANP+17] T. Astner, S. Nevlacsil, N. Peterschofsky, A. Angerer, S. Rotter, S. Putz, J. Schmiedmayer, and J. Majer. Coherent coupling of remote spin ensembles via a cavity bus. *Phys. Rev. Lett.*, 118(14):140502, 2017.

[AOGC19] E. R. Anschuetz, J. P. Olson, A. Aspuru-Guzik, and Y. Cao. Variational Quantum Factoring. In *International Workshop on Quantum Technology and Optimization Problems*, pages 74–85. Springer, 2019.

[ARL+17] C. K. Andersen, et al., Repeated Quantum Error Detection in a Surface Code, arxiv:1912.09410

[ARS13] B. Amento, M. Rötteler, and R. Steinwandt. Efficient quantum circuits for binary elliptic curve arithmetic: reducing *T*-gate complexity. *Quantum Inf. Comput.*, 13:631–644, 2013.

[ASA+18] M. Almazrooie, A. Samsudin, R. Abdullah, and K. N. Mutter. Quantum reversible circuit of AES-128. Quantum Information Processing, 5, 2018.

[ASB+13] S. M. Anton, I. A. B. Sognnaes, J. S. Birenbaum, S. R. O'Kelley, C. J. Fourie, and J. Clarke. Mean square flux noise in squids and qubits: numerical calculations. *Supercond. Sci. Technol.*, 26(7):075022, 2013.

[Ash97] A. Ashkin. Optical trapping and manipulation of neutral particles using lasers. Proceedings of the National Academy of Sciences, 94(10):4853–4860, 1997.

[ASK+16] V. V. Albert et al. Holonomic quantum control with continuous variable systems. Physical review letters, 116(14):140502, 2016.

[ATB16] R. N. Alexander, P. S. Turner, and S. D. Bartlett. Randomized benchmarking in measurement-based quantum computing. *Phys. Rev. A*, 94(3):032303, 2016.

[AvDK+07] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation. *SIAM J. Comput.*, 37(1):166–194, 2007, http://dx.doi.org/10.1137/S0097539705447323.

[AWR+22] M. H. Abobeih, Y. Wang, J. Randall, S. J. H. Loenen, C. E.Bradley, M. Markham, D. J. Twitchen, B. M. Terhal, and T. H.Taminiau. Fault-tolerant operation of a logical qubit in a diamond quantum processor. *Nature*, 606(7916):884–889, May 2022

[Bar22] J. Bardin. Beyond-classical computing using superconducting quantum processors. In 2022 IEEE International Solid-State Circuits Conference (ISSCC), volume 65, pages 422–424. IEEE, 2022.

[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *J Stat Phys* **22**, 563–591, 1980, https://doi.org/10.1007/BF01011339

[Bac06] D. Bacon. Operator quantum error-correcting subsystems for self-correcting quantum memories. *Physical Review* A, 73(1):012340, 2006.

[Bac13] D. Bacon. *Quantum Error Correction*, chapter Introduction to quantum error correction, pages 46–76. Cambridge University Press, 2013.

[Bak24] A. Baksi. Post in pqc-forum (pqc-forum@list.nist.gov), available at https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/EKoI0u_PuOw/m/wIXdlwZ8AwAJ Mar 1, 2024.

[BB17] G. Banegas and D. J. Bernstein. Low-communication parallel quantum multi-target preimage search. In *Selected Areas in Cryptography – SAC 2017*, 2017.

[BBB+21] S. Bartolucci et al. Fusion-based quantum computation. arXiv:2101.09310, 2021.

[BBC+17] L. S. Bishop, S. Bravyi, A. Cross, J. M. Gambetta, and J. Smolin. Quantum volume, 2017, https://dal.objectstorage.open.softlayer.com/v1/AUTH_039c3bf6e6e54d76b8e66152e2f87877/community-documents/quatnum-volumehp08co1vbo0cc8fr.pdf.

[BBC+22] J. FF. Bulmer et al. The boundary for quantum advantage in gaussian boson sampling. Science advances, 8(4):eabl9236, 2022

[BBC+24] K.Blekos et al. A review on Quantum Approxiamtive Optimization Algorithm and its variants. *Physics Reports* 1068, 2024.

[BDG+22] S. Bravyi, O. Dial, J. M. Gambetta, D. Gil, and Z. Nazario. The future of quantum computing with superconducting qubits, 2022, arXiv:2209.06841.

[BBHT98] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46:493–506, 1998.

[BBL16] A. Browaeys, D. Barredo, and T. Lahaye. Experimental investigations of dipole-dipole interactions between a few rydberg atoms. *J. Phys. B: At., Mol. Opt. Phys.*, 49(15):152001, 2016.

[BBM17] D. Bernstein, J.-F. Biasse, and M. Mosca. A Low-Resource Quantum Factoring Algorithm. Post-Quantum Cryptography – PQCrypto 2017, Springer LNCS vol. 10346, pp. 330-346, 2017.

[BBV+16] V. B. Braginsky, I. A. Bilenko, S. P. Vyatchanin, M. L. Gorodetsky, V. P. Mitrofanov, L. G. Prokhorov, S. E. Strigin, and F. Y. Khalili. The road to the discovery of gravitational waves. *Phys. Usp*, 59(9):879–885, 2016.

[BBvHL20] G. Banegas, D. J. Bernstein, I. van Hoof, and T. Lange. Concrete quantum cryptanalysis of binary elliptic curves. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(1):451–472, Dec. 2020.

[BBS+19] J. J. Burnett, A. Bengtsson, M. Scigliuzzo, D. Niepce, M. Kudra, P. Delsing, and J. Bylander. Decoherence benchmarking of superconducting qubits. npj Quantum Information, 5(1):54, 2019.

[BC15] S. Bravyi and A. Cross. Doubled color codes, 2015, arXiv:1509.03239.

[BC23] T. Begušić and G. K.-L. Chan, Fast Classical Simulation of Evidence for the Utility of Quantum Computing before Fault Tolerance, 2023, arXiv:2306.16372.

[BCC+07] J. Baugh et al., Quantum information processing using nuclear and electron magnetic resonance: review and prospects. 2007, arXiv:0710.1447.

[BCFNP22] R. Bhaumik, A. Chailloux, P. Frixons, and M. Naya Plasencia. Safely doubling your block ciphers for a post-quantum world. *Cryptology ePrint Archive, Paper 2022/1342, 2022*. https://eprint.iacr.org/2022/1342. Presented at FRISIACRYPT 2022, Terschelling, The Netherlands, September 25-28, 2022.

[BCG+24] S. Bravyi et al. High-threshold and low-overhead fault-tolerant quantum memory. Nature, 627(8005):778–782, March 2024.

[BCK22] S. Baek, S. Cho, and J. Jim. Quantum cryptanalysis of the full AES-256-based Davies–Meyer, Hirose and MJH hash functions, Quantum Information Processing 21: 163, 2022.

[BCI+16] Z. Bian, F. Chudak, R. Israel, B. Lackey, W. G. Macready, and A. Roy. Mapping constrained optimization problems to quantum annealing with application to fault diagnosis, 2016, arXiv:1603.03111.

[BCMS19] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M Sage. Trapped-ion quantum computing: Progress and challenges. Applied Physics Reviews, 6(2):021314, 2019.

[BCM+20] F. Borjans, X. Croot, X. Mi, M. Gullans, and J. Petta. Resonant microwave-mediated interactions between distant electron spins. Nature, 577(7789):195–198, 2020.

[BCOR09] S. Blanes, F. Casas, J. Oteo, and J. Ros. The Magnus expansion and some of its applications. *Phys. Rep.*, 470(5-6):151–238, 2009.

[BCP+20] F. Borjans et al. Split-gate cavity coupler for silicon circuit quantum electrodynamics. Applied Physics Letters, 116(23):234001, 2020.

[BDGD05] K. Bladh, T. Duty, D. Gunnarsson, and P. Delsing. The single cooper-pair box as a charge qubit. *New J. Phys.*, 7(1):180, 2005.

[BdLL+16] D. Barredo, S. de Léséleuc, V. Lienhard, T. Lahaye, and A. Browaeys. An atom-by-atom assembler of defect-free arbitrary two-dimensional atomic arrays. *Science*, 354(6315):1021–1023, 2016.

[BDG+22] S. Bravyi, O. Dial, J. M. Gambetta, D. Gil, and Z. Nazario. The future of quantum computing with superconducting qubits, 2022, arXiv:2209.06841.

[Bea03] S. Beauregard. Circuit for Shor's algorithm using 2*n* + 3 qubits. *Quantum Inf. Comput.*, 3(2):175–185, 2003.

[BEG+24] D. Bluvstein et al. Logical quantum processor based on reconfigurable atom arrays. *Nature* **626** (2024)

.BEKP18] S. Bravyi, M. Englbrecht, R. König, and N. Peard. Correcting coherent errors with surface codes. NPJ Quant. Inf.,4:55, 2018.

[BEL+21] K. Boothby, C. Enderud, T. Lanting, R. Molavi, N. Tsai, M. H. Volkmann, F. Altomare, M. H. Amin, M. Babcock, A. J. Berkley, et al. Architectural considerations in the design of a third-generation superconducting quantum annealing processor. arXiv preprint arXiv:2108.02322, 2021.

[BE21] N. P. Breuckmann and J. N. Eberhardt. Quantum low-density parity-check codes. PRX Quantum, 2(4):040101, 2021.

[Ber09] D. Bernstein. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? SHARC '09 Workshop Record, pp. 105-116, 2009, http://www.hyperelliptic.org/tanja/SHARCS/record2.pdf#page=113 .

[Ber17] D. Bernstein. 2017.10.17: Quantum algorithms to find collisions: Analysis of several algorithms for the collision problem, and for the related multi-target preimage problem., The cr.yp.to blog, 2017. https://blog.cr.yp.to/20171017-collisions.html

[BFBA10] B. B. Buckley, G. D. Fuchs, L. C. Bassett, and D. D. Awschalom. Spin-light coherence for single-spin measurement and control in diamond. *Science*, 330(6008):1212–1215, 2010, http://science.sciencemag.org/content/330/6008/1212.full.pdf.

[BFN+11] H. Bluhm, S. Foletti, I. Neder, M. Rudner, D. Mahalu, V. Umansky, and A. Yacoby. Dephasing time of gaas electron-spin qubits coupled to a nuclear bath exceeding 200[thinsp][mu]s. *Nat Phys*, 7(2):109–113, February 2011.

[BGN20] E. Bourgeois, M. Gulka, and M. Nesladek. Photoelectric detection and quantum readout of nitrogen-vacancy center spin states in diamond. Advanced Optical Materials, 8(12):1902132, 2020.

[BGW+07] A. Blais, J. Gambetta, A. Wallraff, D. I. Schuster, S. M. Girvin, M. H. Devoret, and R. J. Schoelkopf. Quantum-information processing with circuit quantum electrodynamics. *Phys. Rev. A*, 75(3):032329, 2007.

[BGW+15] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola. Microwave quantum illumination. *Phys. Rev. Lett.*, 114(8):080503, 2015.

[BGY+11] J. Bylander, S. Gustavsson, F. Yan, F. Yoshihara, K. Harrabi, G. Fitch, D. G. Cory, Y. Nakamura, J.-S. Tsai, and W. D. Oliver. Noise spectroscopy through dynamical decoupling with a superconducting flux qubit. *Nat. Phys.*, 7(7):565–570, 2011.

[BH12] S. Bravyi and J. Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86(5):052329, 2012.

[BHJ+14] P. I. Bunyk, E. M. Hoskinson, M. W. Johnson, E. Tolkacheva, F. Altomare, A. J. Berkley, R. Harris, J. P. Hilton, T. Lanting, A. J. Przybysz, and J. Whittaker. Architectural considerations in the design of a superconducting quantum annealing processor. *IEEE Transactions on Applied Superconductivity*, 24(4):1–10, Aug 2014.

[BHL+16] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas. High-fidelity quantum logic gates using trapped-ion hyperfine qubits. *Phys. Rev. Lett.*, 117(6):060504, 2016.

[BHP+14] C. W. Berry, M. R. Hashemi, S. Preu, H. Lu, A. C. Gossard, and M. Jarrahi. High power terahertz generation from eras: Ingaas plasmonic photomixers. In *2014 39th International Conference on Infrared, Millimeter, and Terahertz waves (IRMMW-THz)*, pages 1–2, 2014.

[BHNP+19] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher, *Quantum Attacks Without Superposition Queries: The Offline Simon's Algorithm*. In Advances in Cryptology – ASIACRYPT 2019, vol. 11921 of LNCS, pp. 552 – 583, Springer, 2019.

[BHS+22] D. Bluvstein, H. Levine, G. Semeghini, T. T. Wang, S. Ebadi, M. Kali-nowski, A. Keesling, N. Maskara, H. Pichler, M. Greiner, et al. A quantumprocessor based on coherent transport of entangled atom arrays. *Nature*, 604(7906):451–456, 2022.

[BHT98] G. Brassard, P. Høyer, and A. Tapp. Quantum Algorithm for the Collision Problem. In *Third Latin American Symposium on Theoretical Informatics (LATIN '98)*, volume 1380 of *Lecture Notes in Computer Science*, pages 163–169. Springer, 1998.

[Bia08] J. D. Biamonte. Nonperturbative *k*-body to two-body commuting conversion hamiltonians and embedding problem instances into ising spins. *Phys. Rev. A*, 77(5):052331, 2008.

[BIS+16] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, J. M. Martinis, and H. Neven. Characterizing quantum supremacy in near-term devices, 2016, arXiv:1608.00263.

[BK98] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary, 1998, arXiv:quant-ph/9811052.

[BK05] S. Bravyi and A. Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Phys. Rev. A*, 71(2):022316, 2005.

[BK13] S. Bravyi and R. König. Classification of topologically protected gates for local stabilizer codes. *Phys. Rev. Lett.*, 110(17):170503, 2013.

[BKCD02] R. Blume-Kohout, C. Caves, and I. Deutsch. Climbing mount scalable: Physical resource requirements for a scalable quantum computer. *Found. Phys.*, 32(11):1641–1670, 2002.

[BKGN+13] R. Blume-Kohout, J. K. Gamble, E. Nielsen, J. Mizrahi, J. D. Sterk, and P. Maunz. Robust, self-consistent, closed-form tomography of quantum logic gates on a trapped ion qubit, 2013, arXiv:1310.4492.

[BKGN+17] R. Blume-Kohout, J. K. Gamble, E. Nielsen, K. Rudinger, J. Mizrahi, K. Fortier, and P. Maunz. Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography. *Nat. Commun.*, 8, 2017.

[BKH+17] J. Benedikter, H. Kaupp, T. Hümmer, Y. Liang, A. Bommer, C. Becher, A. Krueger, J. M. Smith, T. W. Hänsch, and D. Hunger. Cavity-enhanced single-photon source based on the silicon-vacancy center in diamond. *Phys. Rev. Applied*, 7:024031, Feb 2017.

[BKLW00] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley. Universal fault-tolerant quantum computation on decoherence-free subspaces. *Phys. Rev. Lett.*, 85(8):1758–1761, 2000.

[BKM+13] R. Barends, J. Kelly, A. Megrant, D. Sank, E. Jeffrey, Y. Chen, Y. Yin, B. Chiaro, J. Mutus, et al. Coherent josephson qubit suitable for scalable quantum integrated circuits. *Phys. Rev. Lett.*, 111(8):080502, 2013.

[BKM+14] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler et al. Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature*, 508(7497):500–503, 2014.

[BKM16] K. R. Brown, J. Kim, and C. Monroe. Co-designing a scalable quantum computer with trapped atomic ions. *Nat. Partn. J. Quantum Inf.*, 2:16034, 2016.

[BKM18] A. Botea, A. Kishimoto, and Radu Marinescu. On the Complexity of Quantum Circuit Compilation. 11th Annual Symposium on Combinatorial Search (SoCS 2018), AAAI Publications, 2018, https://aaai.org/ocs/index.php/SOCS/SOCS18/paper/view/17959.

[BKP13] P. Brooks, A. Kitaev, and J. Preskill. Protected gates for superconducting qubits.Physical Review A, 87(5):052306, 2013.

[BKRB15] M. Brownnutt, M. Kumph, P. Rabl, and R. Blatt. Ion-trap measurements of electric-field noise near surfaces. *Rev. Mod. Phys.*, 87(4):1419–1482, 2015.

[BLAG14] R. Babbush, P. J. Love, and A. Aspuru-Guzik. Adiabatic quantum simulation of quantum chemistry. *Sci. Rep.*, 4:6603 EP, 2014.

[BLK+15] R. Barends, L. Lamata, J. Kelly, L. García-Álvarez, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, et al. Digital quantum simulation of fermionic models with a superconducting circuit. *Nat. Commun.*, 6:7654, 2015.

[BLNPS21] X. Bonnetain, G. Leurent, M. Naya-Plasencia, and A. Schrottenloher. Quantum Linearization Attacks. In MehdiTibouchi and Huaxiong Wang, editors, *Advances in Cryptology –ASIACRYPT 2021*, pages 422–452, Cham, 2021. Springer International Publishing.

[BLS+22] D. Bluvstein, H. Levine, G. Semeghini, TT. Wang, S. Ebadi, M. Kalinowski et al. A quantum processor based on coherent transport of entangled atom arrays. Nature 604 (2022).

[BLPV16] H.-P. Breuer, E.-M. Laine, J. Piilo, and B. Vacchini. Colloquium. *Rev. Mod. Phys.*, 88(2):021002, 2016.

[BLP+23] G. Burkard, T. D. Ladd, A. Pan, J. M. Nichol, and J. R. Petta, *Semiconductor Spin Qubits*, Rev. Mod. Phys. **95**, 025003 (2023).

[BMD07] H. Bombin and M. A. Martin-Delgado. Topological computation without braiding. *Phys. Rev. Lett.*, 98(16):160502, 2007.

[BMR+06] J. Baugh, O. Moussa, C. A. Ryan, R. Laflamme, C. Ramanathan, T. F. Havel, and D. G. Cory. Solid-state nmr three-qubit homonuclear system for quantum-information processing: Control and characterization. *Phys. Rev. A*, 73(2):022305, 2006.

[BNB16] B. J. Brown, N. H. Nickerson, and D. E. Browne. Fault-tolerant error correction with the gauge color code. *Nat. Commun.*, 7:12302, 2016.

[BNP18] X. Bonnetain and M. Naya-Plasencia. Hidden Shift Quantum Cryptanalysis and Implications. Advances in Cryptology - ASIACRYPT 2018, Lecture Notes in Computer Science vol. 11272, pp. 560–592, Springer, 2018.

[BNPS19] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, *Quantum Security Analysis of AES*. IACR Transactions on Symmetric Cryptology, 2019(2), 55-93, 2019.

[BOV+09] R. B. Blakestad, C. Ospelkaus, A. P. VanDevender, J. M. Amini, J. Britton, D. Leibfried, and D. J. Wineland. High-fidelity transport of trapped-ion qubits through an **X**-junction trap array. *Phys. Rev. Lett.*, 102(15):153002, 2009.

[Boy03] R. W. Boyd. *Nonlinear Optics (Second Edition)*. Academic Press, 2003.

[Bon21] X. Bonnetain. Tight Bounds for Simon's Algorithm. In P. Longa and C. Ràfols, editors, Progress in Cryptology – LATINCRYPT 2021, pages 3–23, Cham, 2021. Springer International Publishing.

[BP02] H. P. Breuer and F. Petruccione. *The theory of open quantum systems*. Oxford University Press, 2002.

[BPIG14] M. T. Bell, J. Paramanandam, L. B. Ioffe, and M. E. Gershenson. Protected josephson rhombus chains. *Phys. Rev. Lett.*, 112(16):167001, 2014.

[BPK+22] J. Z. Blumoff et al. Fast and high-fidelity state preparation and measurement in triple-quantum-dot spin qubits. PRX Quantum, 3(1):010352, March 29, 2022.

[BR05] D. E. Browne and T. Rudolph. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.*, 95(1):010501, 2005.

[BR12] R. Blatt and C. F. Roos. Quantum simulations with trapped ions. *Nat. Phys.*, 8(4):277–284, 2012.

[Bra98] S. L. Braunstein. Error correction for continuous quantum variables. *Phys. Rev. Lett.*, 80(18):4084–4087, 1998.

[Bra17] M. F. Brandl. A quantum von Neumann architecture for large-scale quantum computing in systems with long coherence times, such as trapped ions, 2017, arxiv:1702.02583v1.

[BRA+19] C. E. Bradley et al. A ten-qubit solid-state spin register with quantum memory up to one minute. Physical ReviewX, 9(3):031045, 2019.

[BS15] P. Budhathoki and R. Steinwandt. Automatic synthesis of quantum circuits for point addition on ordinary binary elliptic curves. *Quantum Inf. Process.*, 14(1):201–216, 2015.

[BSA17] G. Burkard, V. O. Shkolnikov, and D. D. Awschalom. Designing a cavity-mediated quantum cphase gate between nv spin qubits in diamond. *Phys. Rev. B*, 95:205420, May 2017.

[BSBN02] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto. Efficient classical simulation of continuous variable quantum information processes. *Phys. Rev. Lett.*, 88(9):097904, 2002.

[BSE+24] B. L. Brock et al. Quantum Error Correction of Qudits Beyond Break-even. October 8, 2024. arXiv: 2409 .15065 [quant-ph]. url: http://arxiv.org/abs/2409.15065. Pre-published.

[BSK+12] J. W. Britton et al. Engineered two-dimensional ising interactions in a trapped-ion quantum simulator with hundreds of spins. *Nature*, 484(7395):489–492, 2012.

[BSK+17] H. Bernien et al. Probing many-body dynamics on a 51-atom quantum simulator, 2017, arXiv:1707.04344.

[BSL+16] R. Barends et al. Digitized adiabatic quantum computing with a superconducting circuit. *Nature*, 534(7606):222–226, 2016.

[BSM+10] N. Bergeal et al. Phase-preserving amplification near the quantum limit with a josephson ring modulator. *Nature*, 465(7294):64–68, 2010.

[BSS22] X. Bonnetain, A. Schrottenloher, and F. Sibleyras. Beyond Quadratic Speedups in Quantum Attacks on SymmetricSchemes. In O. Dunkelman and S. Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 315–344, Cham, 2022. Springer International Publishing.

[BSV01] V. Braginsky, S. Strigin, and S. Vyatchanin. Parametric oscillatory instability in fabry-perot interferometer. *Phys. Lett. A*, 287(5):331 – 338, 2001.

[BSV14] S. Bravyi, M. Suchara, and A. Vargo. Efficient algorithms for maximum likelihood decoding in the surface code. *Phys. Rev. A*, 90(3):032326, 2014.

[Bur02] C. J. Burges. Factoring as optimization. Microsoft Research MSR-TR-200, 2002

[BVAC13] J. Bochmann, A. Vainsencher, D. D. Awschalom, and A. N. Cleland. Nanomechanical coupling between microwave and optical photons. *Nat. Phys.*, 9(11):712–716, 2013.

[BVJ+98] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, and M. H. Devoret. Quantum coherence with a single cooper pair. *Phys. Scr.*, 1998(T76):165, 1998.

[BvL05] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77(2):513–577, 2005.

[BvL16] M. Bergmann and P. van Loock. Quantum error correction against photon loss using multicomponent cat states. *Physical Review A*, 94(4):042332, October 2016.

[BW08a] R. Blatt and D. Wineland. Entangled states of trapped atomic ions. *Nature*, 453(7198):1008–1015, 2008.

[BW08b] L. Bogani and W. Wernsdorfer. Molecular spintronics using single-molecule magnets. *Nat. Mater.*, 7(3):179–186, 2008.

[BWC+11] K. R. Brown, A. C. Wilson, Y. Colombe, C. Ospelkaus, A. M. Meier, E. Knill, D. Leibfried, and D. J. Wineland. Single-qubit-gate error below $\mathbf{10^{-4}}$ in a trapped ion. *Phys. Rev. A*, 84(3):030303, 2011.

[BWG+18] S.J. Beale, J.J. Wallmann, M. Gutierrez, K.R. Brown, and R. Laflamme, Quantum error correction decoheres noise, Physical review letters, 121(19), 190501, 2018.

[BWM+16] B. Bauer, D. Wecker, A. J. Millis, M. B. Hastings, and M. Troyer. Hybrid quantum-classical approach to correlated materials. *Phys. Rev. X*, 6(3):031045, 2016.

[BWMM22] E. Burek, M. Wrónski, K. Mańk, and M. Misztal. Algebraic attacks on block ciphers using quantum annealing. *IEEE Transactions on Emerging Topics in Computing*, 10(2):678–689, 2022.

[BXN+17] A. Bermudez et al. Assessing the progress of trapped-ion processors towards fault-tolerant quantum computation, 2017, arXiv:1705.02771.

[CAB+21] M. Cerezo et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021.

[CAS+21] P. C. S. Costa, D. An, Y. R. Sanders, Y. Su, R. Babbush, and D. W. Berry. Optimal scaling quantum linear systems solver via discrete adiabatic theorem, arXiv:2111.08152, 2021.

[CB06] J. Clarke and A. Braginski. *The SQUID Handbook: Fundamentals and Technology of SQUIDs and SQUID Systems*. Wiley, 2006.

[CB18] C. Chamberland and M. E. Beverland. Flag fault-tolerant error correction with arbitrary distance codes. Quantum, 2:53, 2018.

[CC19] C. Chamberland and A. W. Cross. Fault-tolerant magic state preparation with flag qubits. Quantum, 3:143, 2019.

[CBDB14] P. Cerfontaine, T. Botzem, D. P. DiVincenzo, and H. Bluhm. High-fidelity single-qubit gates for two-electron spin qubits in gaas. *Phys. Rev. Lett.*, 113:150501, Oct 2014.

[CBIH+08] M. A. Castellanos-Beltran, K. D. Irwin, G. C. Hilton, L. R. Vale, and K. W. Lehnert. Amplification and squeezing of quantum noise with a tunable josephson metamaterial. *Nat. Phys.*, 4(12):929–931, 2008.

[CBS+04] I. Chiorescu et al. Coherent dynamics of a flux qubit coupled to a harmonic oscillator. *Nature*, 431(7005):159–162, 2004.

[CBSG17] A. W. Cross, L. S. Bishop, J. A. Smolin, and J. M. Gambetta. Open quantum assembly language, 2017, arXiv:1707.03429.

[CCG+11] J. M. Chow et al. Simple all-microwave entangling gate for fixed-frequency superconducting qubits. *Phys. Rev. Lett.*, 107(8):080502, 2011.

[CDG+10] A. A. Clerk, M. H. Devoret, S. M. Girvin, F. Marquardt, and R. J. Schoelkopf. Introduction to quantum noise, measurement, and amplification. *Rev. Mod. Phys.*, 82(2):1155–1208, 2010.

[CDR+17] S. Caldwell et al. Parametrically-activated entangling gates using transmon qubits, 2017, arXiv:1706.06562.

[CET+20] P. Campagne-Ibarcq et al. Quantum error correction of a qubit encoded in grid states of an oscillator. *Nature*, 584(7821):368–372, 2020.

[CFLLS14] E. Crosson, E. Farhi, C. Y. Lin, H. Lin, P. Shor, Different Strategies for Optimization Using the Quantum Adiabatic Algorithm,, https://arxiv.org/abs/1401.7320

[CFGR+13] H. O. H. Churchill et al. Superconductor-nanowire devices from tunneling to the multichannel regime: Zero-bias oscillations and magnetoconductance crossover. *Phys. Rev. B*, 87(24):241401, 2013.

[CFS24] C. Chevignard, P.-A. Fouque, and A. Schrottenloher. Reducing the Number of Qubits in Quantum Factoring, *Cryptology ePrint Archive, Paper 2024/222,* https://eprint.iacr.org/2024/222, 2024.

[CG18] Y.-A. Chen, X.-S. Gao. *Quantum algorithms for Boolean equation solving and quantum algebraic attack on cryptosystems*. arXiv:1712.06239v3, 2018.

[CG21] Y.-A. Chen and X.-S. Gao. Quantum Algorithm for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems. *J Syst Sci Complex* 35: 373–412, 2022, https://doi.org/10.1007/s11424-020-0028-6. Preprint available as [CG18].

[CGFF17] J. Combes, C. Granade, C. Ferrie, and S. T. Flammia. Logical randomized benchmarking, 2017, arXiv:1702.03688.

[Chi09] A. M. Childs. Universal computation by quantum walk. Physical review letters, 102(18):180501, 2009.

[CHLS20] C. Cid, A. Hosoyamada, Y. Liu, and S. M. Sim. Quantum Cryptanalysis on Contracting Feistel Structures and Observation on Related-Key Settings. In K. Bhargavan, E. Oswald, and M. Prabhakaran, editors, *Progress in Cryptology – INDOCRYPT 2020*, pages 373–394, Cham, 2020. Springer International Publishing.

[CHS+15] J. Carolan et al. Universal linear optics. *Science*, 349(6249):711–716, 2015.

[CJS13] B. D. Clader, B. C. Jacobs, and C. R. Sprouse. Preconditioned Quantum Linear System Algorithm. Phys. Rev. Lett., 110(250504), 2013.

[CKS17] A. M. Childs, R. Kothari, and R. D. Somma. *Quantum Algorithm for Systems of Linear Equations with Exponentially Improved Dependence on Precision*. SIAM Journal on Computing 46.6, pp. 1920–1950, 2017.

[CLCL22] D. Chung, S. Lee, D. Choi, and J. Lee. Alternative Tower Field Construction for Quantum Implementation of the AES S-Box. *IEEE Transactions on Computers*, 71(10): 2553–2564, October 2022.

[Cle10] A. Cleland. Nanoelectromechanical resonators. In K. Sattler, editor, *Handbook of Nanophysics: Functional Nanomaterials*, chapter 37, pages 266–290. CRC Press (Taylor & Francis), 2010.

[CLGM+23] M. Cerezo et al. Does provable absence of barren plateaus imply classical simulability? Or, why we need to rethink variational quantum computing. *ArXiv:*2312.09121, 2023.

[CLK+00] D. Cory et al. Nmr based quantum information processing: Achievements and prospects. *Fortschr. Phys.*, 48(9-11):875–907, 2000.

[CMB+10] J. H. Cole et al. Quantitative evaluation of defect-models in superconducting phase qubits. *Appl. Phys. Lett.*, 97(25):252501, 2010.

[CMB+16] A. W. Cross, E. Magesan, L. S. Bishop, J. A. Smolin, and J. M. Gambetta. Scalable randomised benchmarking of non-clifford gates. *Nat. Partn. J. Quantum Inf.*, 2:16012 EP, 2016.

[CMM99] P. T. Cochrane, G. J. Milburn, and W. J. Munro. Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping. *Phys. Rev. A*, 59(4):2631–2634, 1999.

[CMP14] M. Chen, N. C. Menicucci, and O. Pfister. Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb. *Phys. Rev. Lett.*, 112(12):120505, 2014.

[CMQ+10] W. C. Campbell et al. ultra-fast gates for single atomic qubits. *Phys. Rev. Lett.*, 105(9):090502, 2010.

[CMR+16] B. J. Chapman, B. A. Moores, E. I. Rosenthal, J. Kerckhoff, and K. W. Lehnert. General purpose multiplexing device for cryogenic microwave systems. *Appl. Phys. Lett.*, 108(22):222602, 2016.

[CNHM03] I. Chiorescu, Y. Nakamura, C. J. P. M. Harmans, and J. E. Mooij. Coherent quantum dynamics of a superconducting flux qubit. *Science*, 299(5614):1869–1871, 2003.

[CNPS17] A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher. *An efficient quantum collision search algorithm and implications on symmetric cryptography*. In ASIACRYPT (2), vol. 10625 of LNCS, pp. 211–240. Springer, 2017.

[CNR+14] Y. Chen et al. Qubit architecture with high coherence and fast tunable coupling. *Phys. Rev. Lett.*, 113(22):220502, 2014.

[Cop94] D. Coppersmith. An Approximate Fourier Transform Useful in Quantum Factoring, 1994.

[CR14] J. I. Colless and D. J. Reilly. Modular cryogenic interconnects for multi-qubit devices. *Rev. Sci. Instrum.*, 85(11):114706, 2014.

[CR18] R. Chao and B. W. Reichardt. Fault-tolerant quantum computation with few qubits. npj Quantum Information, 4(1):1–8, 2018.

[CR20] R. Chao and B. W. Reichardt. Flag fault-tolerant error correction for any stabilizer code. PRX Quantum, 1(1):010302, 2020.

[CRFG17] D. S. A. Coden, R. H. Romero, A. Ferrón, and S. S. Gomez. Optimal control of a charge qubit in a double quantum dot with a coulomb impurity. *Physica E: Low-dimensional Systems and Nanostructures*, 86:36–43, 2017.

[CRKW17] T. Chasseur, D. M. Reich, C. P. Koch, and F. K. Wilhelm. Hybrid benchmarking of arbitrary quantum gates. *Phys. Rev. A*, 95(6), 2017.

[CSA+21] Z. Chen et al. Exponential suppression of bit or phase errors with cyclic error correction. Nature, 595(7867):383–387, 2021.

[CSDS17] D. J. Clarke, J. D. Sau, and S. Das Sarma. Probability and braiding statistics in majorana nanowires. *Phys. Rev. B*, 95(15):155451, 2017.

[CSF+21] A. Chatterjee et al. Semiconductor qubits in practice. Nature Reviews Physics, 3(3):157–177, 2021.

[CTS+21] Craig R Clark et al. High-fidelity bell-state preparation with ca+ 40 optical qubits. PhysicalReview Letters, 127(13):130505, 2021

[CTV17] E. T. Campbell, B. M. Terhal, and C. Vuillot. Roads towards fault-tolerant universal quantum computation. Nature, 549(7671):172–179, 2017.

[CW00] R. Cleve and J. Watrous. Fast parallel circuits for the quantum Fourier transform. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 526–536, 2000.

[CW08] J. Clarke and F. K. Wilhelm. Superconducting quantum bits. *Nature*, 453(7198):1031–1042, 2008.

[CW15] T. Chasseur and F. K. Wilhelm. Complete randomized benchmarking protocol accounting for leakage errors. *Phys. Rev. A*, 92(4), 2015.

[CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74(20):4091–4094, 1995.

[CZW16] N. Chancellor, S. Zohren, and P. A. Warburton. Circuit design for multi-body interactions in superconducting quantum annealing system with applications to a scalable architecture, 2016, arXiv:1603.09521.

[DA17] R. Dridi and H. Alghassi. Prime factorization using quantum annealing and computational algebraic geometry. Scientific Reports, 7(43048), 2017, https://doi.org/10.1038/srep43048.

[Deu89] D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, *425*, pages 73-90, 1989.

[DB14] N. S. Dattani and N. Bryans. Quantum factorization of 56153 with only 4 qubits. arXiv:1411.6758, 2014.

[DBI+16] V. S. Denchev et al. What is the computational value of finite-range tunneling? *Phys. Rev. X*, 6(3):031015, 2016.

[DBK+00] D. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K. Whaley. Universal quantum computation with the exchange interaction. *Nature*, 408(6810):339–342, 2000.

[DC24] Sarah D. and Peter C. On the practical cost of Grover for AES key recovery. *Fifth PQC Standardization Conference*, 2024, https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf.

[DCJ+07] M. V. G. Dutt et al. Quantum register based on individual electronic and nuclear spin qubits in diamond. *Science*, 316(5829):1312–1316, 2007, http://science.sciencemag.org/content/316/5829/1312.full.pdf.

[DDBA13] I. Diniz, E. Dumur, O. Buisson, and A. Auffèves. ultra-fast quantum nondemolition measurements based on a diamond-shaped artificial atom. *Phys. Rev. A*, 87(3):033837, 2013.

[DDW16] P.-L. Dallaire-Demers and F. K. Wilhelm. Quantum gates and architecture for the quantum simulation of the fermi-hubbard model. *Phys. Rev. A*, 94(6):062304, 2016.

[DFII05] B. Douçot, M. V. Feigel'man, L. B. Ioffe, and A. S. Ioselevich. Protected qubits and chern-simons theories in Josephson junction arrays. *Phys. Rev. B*, 71(2):024505, 2005.

[DFZC+21] Y. Dong, C. Feng, Y. Zheng, X.-D. Chen, G.-C. Guo, and F.-W. Sun. Fast high-fidelity geometric quantum control with quantum brachistochrones. Physical Review Research, 3(4):043177, 2021.

[DGGHL23] J. Ding, V. Gheorghiu , A. Gilyén, S. Hallgren, and J. Li, Limitations of the Macaulay matrix approach for using the HHL algorithm to solve multivariate polynomial systems. Quantum 7, 1069, 2023. https://doi.org/10.22331/q-2023-07-26-1069

[DH81] P. Dutta and P. M. Horn. Low-frequency fluctuations in solids: 1/f noise. *Rev. Mod. Phys.*, 53(3):497–516, 1981.

[DHMS+18] D. Dervovic, M. Herbster, P. Mountney, S. Severini, N. Usher, and L. Wossnig. *Quantum linear systems algorithms: a primer*. arXiv:1802.08227v1, 2018.

[DHN06a] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen. Noise thresholds for optical cluster-state quantum computation. *Phys. Rev. A*, 73(5):052306, 2006.

[DHN06b] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen. Noise thresholds for optical quantum computers. *Phys. Rev. Lett.*, 96(2):020501, 2006.

[DiV00] D. P. DiVincenzo. The physical implementation of quantum computation, 2000, arXiv:quant-ph/0002077v3, http://arXiv.org/abs/quant-ph/0002077v3.

[DJA+13] N. G. Dickson et al. Thermally assisted quantum annealing of a 16-qubit problem. *Nat. Commun.*, 4:1903, 2013.

[DK12] S. L. Danilishin and F. Y. Khalili. Quantum measurement theory in gravitational-wave detectors. *Living Rev. Relativ.*, 15(1):5, 2012.

[DKRS23] O. Dunkelman, N. Keller, E. Ronen, and A. Shamir. Quantum/time/memory/data tradeoff attacks. *Designs, Codes and Cryptography* 92: 159-177, 2024.

[dLvHB+15] G. de Lange et al. Realization of microwave quantum circuits using hybrid superconducting-semiconducting nanowire josephson elements. *Phys. Rev. Lett.*, 115(12):127002, 2015.

[DM12] S. Ding and D. N. Matsukevich. Quantum logic for the control and manipulation of molecular ions using a frequency comb. *New J. Phys.*, 14(2):023028, 2012.

[DMBK+16] J. P. Dehollain et al. Optimization of a solid-state electron spin qubit using gate set tomography. *New J. Phys.*, 18(10):103018, 2016.

[DMC85] M. H. Devoret, J. M. Martinis, and J. Clarke. Measurements of macroscopic quantum tunneling out of the zero-voltage state of a current-biased josephson junction. *Phys. Rev. Lett.*, 55(18):1908–1911, 1985.

[DMT+14] J. P. Dehollain et al. Single-shot readout and relaxation of singlet and triplet states in exchange-coupled ^{31}P electron spins in silicon. *Phys. Rev. Lett.*, 112(23):236801, 2014.

[DOS+15] C. Deng, J.-L. Orgiazzi, F. Shen, S. Ashhab, and A. Lupascu. Observation of floquet states in a strongly driven artificial atom. *Phys. Rev. Lett.*, 115(13):133601, 2015.

[DR99] J. Daemen and V. Rijmen. The Rijndael Block Cipher, 1999.

[Dra00] T.G. Draper. Addition on a Quantum Computer, arXiv:quant-ph/0008033, 2000.

[DRJ+19] H. De Raedt et al. Massively parallel quantum computer simulator, eleven years later. Computer Physics Communications, 237:47–61, 2019.

[DRM+12] A. Das et al. Zero-bias peaks and splitting in an al–InAs nanowire topological superconductor as a signature of majorana fermions. *Nat. Phys.*, 8(12):887–895, 2012.

[DSFN06] S. Das Sarma, M. Freedman, and C. Nayak. Topological quantum computation. *Phys. Today*, 2006.

[DSH+13] O. E. Dial et al. Charge noise spectroscopy using coherent exchange oscillations in a singlet-triplet qubit. *Phys. Rev. Lett.*, 110:146804, Apr 2013.

[DSMN16] S. J. Devitt, A. M. Stephens, W. J. Munro, and K. Nemoto. *Analysis of an Atom-Optical Architecture for Quantum Computation*, pages 407–437. Springer Japan, Tokyo, 2016.

[DSNT06] S. Das Sarma, C. Nayak, and S. Tewari. Proposal to stabilize and detect half-quantum vortices in strontium ruthenate thin films: Non-abelian braiding statistics of vortices in a $p_x + ip_y$ superconductor. *Phys. Rev. B*, 73(22):220502, 2006.

[DSS+20] X. Dong et al. Quantum Collision Attacks on AES-Like Hashing with Low Quantum Random Access Memories. In S. Moriai and H. Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 727–757, Cham, 2020. Springer International Publishing.

[dVRT02] R. de Vivie-Riedle and C. Tesch. Molecular quantum computing: Implementation of global quantum gates applying optimal control theory. In *The Thirteenth International Conference on ultra-fast Phenomena*, page FB2. Optical Society of America, 2002.

[DZS+21] X. Dong et al. Automatic Classical and Quantum Rebound Attacks on AES-Like Hashing by Exploiting Related-Key Differentials. In M. Tibouchi and H. Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 241–271, Cham, 2021. Springer International Publishing.

[EAÅ05] J. Emerson, R. Alicki, and K. Å»yczkowski. Scalable noise estimation with random unitary operators. *J. Opt. B: Quantum Semiclassical Opt.*, 7(10):S347, 2005.

[EBK+23] S.J. Evered *et al*. High-fidelity parallel entangling gates on a neutral atom quantum computer. *Nature* 622 (2023).

[ECMG14] J. M. Epstein, A. W. Cross, E. Magesan, and J. M. Gambetta. Investigating the limits of randomized benchmarking protocols. *Phys. Rev. A*, 89(6):062321, 2014.

[Edm65] J. Edmonds. Paths, trees, and flowers. *Canad. J. Math.*, 17(0):449–467, 1965.

[EGMW11] Y. Elias, H. Gilboa, T. Mor, and Y. Weinstein. Heat-bath cooling of spins in two amino acids. *Chem. Phys. Lett.*, 517(4-6):126 – 131, 2011.

[EG24] M. Ekerå and J. Gärtner. Extending Regev's Factoring Algorithm to Compute Discrete Logarithms. In: Saarinen, MJ., Smith-Tone, D. (eds), *Post-Quantum Cryptography. PQCrypto 2024, pages 211*–242, Lecture Notes in Computer Science, vol 14772. Springer, Cham, 2024.

[EG24b] M. Ekerå and J. Gärtner. A high-level comparison of state-of-the-art quantum algorithms for breaking asymmetric cryptography. arXiv:2405.14381, 2024.[EG24c] M. Ekerå and J. Gärtner: Simulating Regev's quantum factoring algorithm. GitHub repository ekera/regevnum, 2024.

[EH17] M. Ekerå and J. Håstad. Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers. Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Lecture Notes in Computer Science vol. 10346, pp. 347–363, Springer, 2017.

[EHWvB+04] J. M. Elzerman, R. Hanson, L. H. Willems van Beveren, B. Witkamp, L. M. K. Vandersypen, and L. P. Kouwenhoven. Single-shot read-out of an individual electron spin in a quantum dot. *Nature*, 430(6998):431–435, 2004.

[EHWR+19] J. Eisert et al. Quantum certification and benchmarking. Nature Reviews Physics, 2(7):382–390, July 2020. doi: 10.1038/s42254-020-0186-4.

[Eke16] M. Ekerå. Modifying Shor's algorithm to compute short discrete logarithms. Cryptology ePrint Archive, Report 2016/1128, 2016.

[Eke21] M. Ekerå. On completely factoring any integer efficiently in a single run of an order-finding algorithm. *Quantum Information Processing*, 20(205), 2021.

[Eke21b] M. Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. *Journal of Mathematical Cryptology*, 15(1):359–407, 2021.

[Eke21c] M. Ekerå. Revisiting Shor's quantum algorithm for computing general discrete logarithms. *arXiv:1905.09084v2*, 2021.

[Eke22] M. Ekerå. On the success probability of quantum order finding. arXiv:2201.07791 [quant-ph], 2022. https://doi.org/10.48550/arXiv.2201.07791

[ELR10] S. E. Economou, N. Lindner, and T. Rudolph. Optically generated 2-dimensional photonic cluster state from coupled quantum dots. *Phys. Rev. Lett.*, 105(9):093601, 2010.

[EWL+21] S. Ebadi et al. Quantum phases of matter on a 256-atom programmable quantum simulator. Nature, 595(7866):227–232, 2021.

[EWP+19] A. Erhard et al. Characterizing large-scale quantum computers via cycle benchmarking. Nature communications, 10(1):5347, 2019

[FBS+15] T. Feldker et al. Rydberg excitation of a single trapped ion. *Phys. Rev. Lett.*, 115(17):173001, 2015.

[FCH+17] M. A. Fogarty et al. Integrated silicon qubit platform with single-spin addressability, exchange control and robust single-shot singlet-triplet readout, 2017, arXiv:1708.03445.

[FD12] A. G. Fowler and S. J. Devitt. A bridge to lower overhead quantum computation, 2012, arXiv:1209.0510.

[FDJ13] A. G. Fowler, S. J. Devitt, and C. Jones. Surface code implementation of block code state distillation. *Sci. Rep.*, 3(1), 2013.

[FEF+08] I. Fushman et al. Controlled phase shifts with a single quantum dot. *Science*, 320(5877):769–772, 2008, http://science.sciencemag.org/content/320/5877/769.full.pdf.

[FFE+08] A. Faraon et al. Coherent generation of non-classical light on a chip via photon-induced tunnelling and blockade. *Nat. Phys.*, 4(11):859–863, 2008.

[FFSG09] A. G. Fowler, A. G. Fowler, A. M. Stephens, and P. Groszkowski. High threshold universal quantum computation on the surface code. *Phys. Rev. A*, 80:052312, 2009.

[FG09] A. G. Fowler and K. Goyal. Topological cluster state quantum computing. *Quantum Inf. Comput.*, 9(9):721–738, 2009.

[FG18] A.G. Fowler and C. Gidney. Low overhead quantum computation using lattice surgery. arXiv:1808.06709.

[FGG14] E. Farhi, J. Goldstone, and S. Gutmann. A Quantum Approximate Optimization Algorithm. ArXiv:1411.4028, 2014.

[FGG15] E. Farhi, J. Goldstone, and S. Gutmann. A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem. ArXiv:1412.6262, 2015.

[FHZ14] D. Fangwei, W. Hong, and M. Zhi. Quantum Collision Search Algorithm Against New FORK-256. *J. Electron.*, 31, 2014.

[FM14] A. G. Fowler and J. M. Martinis. Quantifying the effects of local many-qubit errors and nonlocal two-qubit errors on the surface code. *Phys. Rev. A*, 89(3):032316, 2014.

[FML+17] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe. Complete 3-qubit Grover search on a programmable quantum computer. Nat. Comm. 8:1918 (2017).

[FMMC12] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86(3):032324, 2012.

[FMP09] S. T. Flammia, N. C. Menicucci, and O. Pfister. The optical frequency comb as a one-way quantum computer. *J. Phys. B: At., Mol. Opt. Phys.*, 42(11):114009, 2009.

[FNS+21] Q. Ficheux et al. Fast logic with slow qubits: microwave-activated controlled-z gate on low-frequency fluxoniums. Physical Review X, 11(2):021026, 2021.

[Föl14] S. Fölling. Quantum noise correlation experiments with ultracold atoms, 2014, arXiv:1403.6842.

[Fow12] A. G. Fowler. Time-optimal quantum computation, 2012, arXiv:1210.4626.

[Fow13a] A. G. Fowler. Analytic asymptotic performance of topological codes. *Phys. Rev. A*, 87(4):040301, 2013.

[Fow13b] A. G. Fowler. Polyestimate: instantaneous open source surface code analysis, 2013, arXiv:1307.0689.

[Fow15] A. G. Fowler. Minimum weight perfect matching of fault-tolerant topological quantum error correction in average o(1) parallel time. *Quantum Inf. Comput.*, 15:145–158, 2015.

[Fox06] M. Fox. *Quantum Optics: An Introduction (Oxford Master Series in Physics, 6)*. Oxford University Press, USA, 2006.

[FPC+00] J. R. Friedman, V. Patel, W. Chen, S. K. Tolpygo, and J. E. Lukens. Quantum superposition of distinct macroscopic states. *Nature*, 406(6791):43–46, 2000.

[FRP+21] K. G Fedorov et al. Experimental quantum teleportation of propagating microwaves.Scienceadvances, 7(52):eabk0891, 2021

[FSG09] A. G. Fowler, A. M. Stephens, and P. Groszkowski. High-threshold universal quantum computation on the surface code. *Phys. Rev. A*, 80(5):052312, 2009.

[FSL+17] S. Freer et al. A single-atom quantum memory in silicon. *Quantum Sci. Technol.*, 2(1):015009, 2017.

[FSLC97] P. Fisk, M. Sellars, M. Lawn, and G. Coles. Accurate measurement of the 12.6 GHz "clock" transition in trapped $^{171}Yb^{+}$ ions. *IEEE Trans. Ultrason., Ferroelect., Freq. Control*, 44(2):344–354, 1997.

[FTCL09] J. Fischer, M. Trif, W. Coish, and D. Loss. Spin interactions, relaxation and decoherence in quantum dots. *Solid State Commun.*, 149(35):1443 – 1450, 2009.

[FW11] B. H. Fong and S. M. Wandzura. Universal quantum computation and leakage reduction in the 3-qubit decoherence free subsystem. Quantum Information & Computation, 11(11-12):1003–1018, 2011.

[FWMR12] A. G. Fowler, A. C. Whiteside, A. L. McInnes, and A. Rabbani. Topological code Autotune. *Phys. Rev. X*, 2(4):041003, 2012.

[FWS+18] A. Fornieri et al. Evidence of topological superconductivity in planar Josephson junctions. arXiv:1809.03037

[FZ01] Rosario Fazio, Herre van der Zant, Quantum phase transitions and vortex dynamics in superconducting networks, Physics Report, Volume 355, Issue 4, December 2001, Pages 235-334.

[GBC+15] S. J. Glaser et al. Training Schrödinger's cat: quantum optimal control. *Eur. Phys. J. D*, 69(12):279, 2015.

[GBKJ+19] Karin Groot-Berning et al. Deterministic single-ion implantation of rare-earth ions for nanometer-resolution color-center generation. *Physical Review Letters* 123(10):106802, 2019.

[GBY+11] S. Gustavsson et al. Noise correlations in a flux qubit with tunable tunnel coupling. *Phys. Rev. B*, 84:014525, Jul 2011.

[GCB20] A. L. Grimsmo, J. Combes, B. Q. Baragiola. Quantum computing with rotation-symmetric bosonic codes. *Phys. Rev. X* 2020; 10:011058.

[GCZ+17] S. Gazibegovic et al. Epitaxy of advanced nanowire quantum devices. *Nature*, 548(7668):434–438, 2017.

[GCZ+22] S. Gazibegovic et al. Retraction note: Epitaxy of advanced nanowire quantum devices. Nature, 604(7907):786–786,2022.

[GD16] D. Greenbaum and Z. Dutton. Modeling coherent errors in quantum error correction. ArXiv:1612.03908

[GE21] C. Gidney and M. Ekerå. *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. Quantum, 5: 433, April 2021.

[GF15] J. Ghosh and A. G. Fowler. Leakage-resilient approach to fault-tolerant quantum computing with superconducting elements. *Phys. Rev. A*, 91(2):020302, 2015.

[GF17] C. Gidney and A. Fowler. A slightly smaller surface code s gate, 2017, arXiv:1708.00054.

[GFM10] O. Golubitsky, S. M. Falconer, and D. Maslov. Synthesis of the Optimal 4-bit Reversible Circuits. In Proc. Of the 47th Design Automation Conference DAC '10, pp. 653-656, ACM, 2010.

[GGK+11] L. Gaudreau, G. Granger, A. Kam, G. C. Aers, S. A. Studenikin, P. Zawadzki, M. Pioro-Ladrière, Z. R. Wasilewski, and A. S. Sachrajda. Coherent control of three-spin states in a triple quantum dot. *Nat. Phys.*, 8(1):54–58, 2011.

[GGRV+23] R. García Gutierrez, C. Recio Valcarce, R. Radanyi, S. Gago Huertao. *Are the RSA and Diffie-Hellman cryptosystems under threat sooner than previously thought?*, Moody's Analytics, January 2023. Available at https://www.linkedin.com/posts/sergiogh_are-rsa-cryptosystems-under-threat-by-quantum-activity-7016810521219715074-D5ol

[GGZ+13] J. Ghosh, A. Galiautdinov, Z. Zhou, A. N. Korotkov, J. M. Martinis, and M. R. Geller. High-fidelity controlled-σ^Z gate for resonator-based superconducting quantum computers. *Phys. Rev. A*, 87(2):022309, 2013.

[Gid18] C. Gidney: *Halving the cost of quantum addition*. Quantum 2, 74 (2018).

[Gir20] D. Giry. BlueKrypt | Cryptographic Key Length Recommendation, 2020. https://www.keylength.com

[GJKPS06] W. Geiselmann, F. Januszewski, H. Köpfer, J. Pelzl, and R. Steinwandt. A Simpler Sieving Device: Combining ECM and TWIRL. In: Rhee, M.S., Lee, B. (eds) *Information Security and Cryptology – ICISC 2006*. Lecture Notes in Computer Science, vol 4296. Springer, Berlin, Heidelberg, 2006.

[GKP01] D. Gottesman, A. Kitaev, and J. Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A*, 64(1):012310, 2001.

[GKV06] S. Glancy, E. Knill, and H. M. Vasconcelos. Entanglement purification of any stabilizer state. *Phys. Rev. A*, 74(3):032319, 2006.

[GLF+10] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.*, 105(15):150401, 2010.

[GLRS16] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt. Applying Grover's Algorithm to AES: Quantum Resource Estimates. In *Post-Quantum Cryptography*, volume 9606 of *Lecture Notes in Computer Science*. Springer, 2016.

[GM19] J. Guillaud and M. Mirrahimi. Repetition Cat Qubits for Fault-Tolerant Quantum Computation. Physical Review X, 9(4):041053, December 2019. doi: 10.1103/PhysRevX.9.041053.

[GMdP+21] A. Gyenis et al. Experimental realizationof a protected superconducting circuit derived from the 0–πqubit.PRXQuantum, 2(1):010339, 2021.

[GMT+12] J. P. Gaebler et al. Randomized benchmarking of multiqubit gates. *Phys. Rev. Lett.*, 108(26):260503, 2012.

[Goo+24] Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. *ArXiv*:2408.13687, 2024.

[Got98] D. Gottesman. The heisenberg representation of quantum computers. 1998, arXiv:quant-ph/9807006.

[Got14] D. Gottesman. Fault-tolerant quantum computation with constant over-head.Quantum Information & Computation, 14(15-16):1338–1372, 2014.

[GPP+15] L. C. G. Govia, E. J. Pritchett, B. L. T. Plourde, M. G. Vavilov, R. McDermott, and F. K. Wilhelm. Scalable two- and four-qubit parity measurement with a threshold photon counter. *Phys. Rev. A*, 92(2):022335, 2015.

[GPX+14] L. C. G. Govia et al. High-fidelity qubit measurement with a microwave-photon counter. *Phys. Rev. A*, 90(6):062307, 2014.

[Gre15] D. Greenbaum. Introduction to quantum gate set tomography, 2015, arXiv:1509.02921.

[Gri11] W. P. Grice. Arbitrarily complete bell-state measurement using only linear optical elements. *Phys. Rev. A*, 84(4):042331, 2011.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 212–219, 1996.

[GRR+23] E. Gouzien, D. Ruiz, F.-M. L. R´egent, J. Guillaud, and N. Sangouard. Performance analysis of a repetition cat code architecture: computing 256-bit elliptic curve logarithm in 9 hours with 126133 cat qubits. arXiv preprint arXiv:2302.06639, 2023.

[GS21] E. Gouzien and N. Sangouard. Factoring 2048-bit RSA Integers in 177 Days with 13 436 qubits and a Multimode Memory. *Phys. Rev. Lett.*, 127:140503, Sep 2021.

[GSS+22] T. Graham et al. Multi-qubit entanglement and algorithms on a neutral-atom quantum computer. Nature,
604(7906):457–462, 2022.

[GSV+22] M. de Goede et al. High fidelity 12-mode quantum photonic processor operating at InGaAs quantum dot wavelength. In Integrated Photonics Research, Silicon and Nanophotonics, pages ITu4B–3. Optica Publishing Group, 2022.

[GSVB13] M. Gutiérrez, L. Svec, A. Vargo, and K. R. Brown. Approximation of realistic errors by clifford channels and pauli measurements. *Phys. Rev. A*, 87(3), 2013.

[GTL+16] J. P. Gaebler, T. R. Tan, Y. Lin, Y. Wan, R. Bowler, A. C. Keith, S. Glancy, K. Coakley, E. Knill, D. Leibfried, and D. J. Wineland. High-fidelity universal gate set for $^{9}Be^{+}$ ion qubits. *Phys. Rev. Lett.*, 117(6):060505, 2016.

[GZ13] M. R. Geller and Z. Zhou. Efficient error models for fault-tolerant architectures and the pauli twirling approximation. *Phys. Rev. A*, 88(1):012314, 2013.

[HAB+14] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas. High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit. *Phys. Rev. Lett.*, 113(22):220501, 2014.

[Hal13] B. C. Hall. Lie groups, lie algebras, and representations. In *Quantum Theory for Mathematicians*, pages 333–366. Springer, 2013

[Har13] S. Haroche. Nobel lecture: Controlling photons in a box and exploring the quantum to classical boundary. *Rev. Mod. Phys.*, 85(3):1083–1102, 2013.

[Has19] M. B. Hastings. Classical and Quantum Bounded Depth Approximation Algorithms. *ArXiv:*1905.07047, 2019.

[HBD+15] B. Hensen et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[HBR+16] A. Holleczek et al. Quantum logic with cavity photons from single atoms. *Phys. Rev. Lett.*, 117(2):023602, 2016.

[HCS+06] D. Hong, D. Chang, J. Sung, S. Lee, S. Hong, J. Lee, D. Moon, and S. Chee. A New Dedicated 256-Bit Hash Function: FORK-256. In *Fast Software Encryption 2006 (FSE 2006)*, volume 4047 of *Lecture Notes in Computer Science*, pages 195–209. Springer, 2006.

[HCW+12] D. A. Hite et al. 100-fold reduction of electric-field noise in an ion trap cleaned with in situ argon-ion-beam bombardment. *Phys. Rev. Lett.*, 109(10):103001, 2012.

[HDF18] E. Huang, A.C. Doherty, and S. Fllammia, Performance of quantum error correction with coherent errors, 2019, arXiv:1805.08227

[HDM+16] N. C. Harris et al. *nanoph*, volume 5, chapter Large-scale quantum photonic circuits in silicon, page 456. 2017 2016.

[Hei03] T. Heinzel. *Mesoscopic Electronics in Solid State Nanostructures*. Wiley, 2003.

[HF18] R. Harper and S. Flammia. Fault tolerance in the IBM Q Experience. ArXiv:1806.02359.

[HFC+03] T. Hayashi, T. Fujisawa, H. D. Cheong, Y. H. Jeong, and Y. Hirayama. Coherent manipulation of electronic states in a double quantum dot. *Phys. Rev. Lett.*, 91(22):226804, 2003.

[HFDvM12] C. Horsman, A.G. Fowler, S. Devitt, and R. van Meter. Surface code quantum computing by lattice surgery. *New. J. Phys.*, 14(12):123011, 2012.

[HFJ+17] T. Hensgens et al. Quantum simulation of a fermi-hubbard model using a semiconductor quantum dot array. *Nature*, 548(7665):70–73, August 2017.

[HFS+20] N. Hendrickx, D. Franke, A. Sammak, G. Scappucci, and M. Veldhorst. Fast two-qubit logic with holes in germanium. Nature, 577(7791):487–491, 2020.

[HFZ20] H.-L. Huang, D. Wu, D. Fan, and X. Zhu. Superconducting quantum computing: a review. Science China Information Sciences, 63(8):1–32,2020.

[HG14] S.-Y. Huang and H.-S. Goan. Optimal control for fast and high-fidelity quantum gates in coupled superconducting flux qubits. *Phys. Rev. A*, 90(1):012318, Jul 2014.

[HGL+98] M. Haake, B. M. Goodson, D. D. Laws, E. Brunner, M. C. Cyrier, R. H. Havlin, and A. Pines. Nmr of supercritical laser-polarized xenon. *Chem. Phys. Lett.*, 292(4–6):686 – 690, 1998.

[HHJ+09] J. P. Home et al. Complete methods set for scalable ion trap quantum information processing. *Science*, 325(5945):1227–1230, 2009.

[HHL09] A. W. Harrow, A. Hassidim, and S. Lloyd. "Quantum algorithm for linear systems of equations". In: Physical review letters 103.15 (2009), p. 150502.

[HJNRS20] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, and M. Soeken. *Improved Quantum Circuits for Elliptic Curve Discrete Logarithms*. In Post-Quantum Cryptography – PQCrypto 2020, Springer LNCS vol. 12100, pp. 425–444, 2020.

[HKD+09] A. A. Houck, J. Koch, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Life after charge noise: recent results with transmon qubits. *Quantum Inf. Process.*, 8(2):105–115, 2009.

[HKEG19] D. Hangleiter, M. Kliesch, J. Eisert, and C. Gogolin, Sample Complexity of Device-Independently Certified "Quantum Supremacy", Phys. Rev. Lett. 122, 210502

[HLBH11] M. D. Hughes, B. Lekitsch, J. A. Broersma, and W. K. Hensinger. Microfabricated ion traps. *Contemp. Phys.*, 52(6):505–529, 2011.

[HMB+15] T. Huang et al. Suppression of dispersive effects in algan/gan high-electron-mobility transistors using bilayer sinx grown by low pressure chemical vapor deposition. *IEEE Electron Device Lett.*, 36(6):537–539, 2015.

[HNG+24] A. Hashim et al. A Practical Introduction to Benchmarking and Characterization of Quantum Computers. August 22, 2024. doi: 10.48550/arXiv.2408.12064. arXiv: 2408.12064. Pre-published.

[HPAA+21] N. N. Hegade, K. Paul, F. Albarrán-Arriagada, X. Chen, and E. Solano. Digitized adiabatic quantum factorization. *Physical Review A*, 104(5):L050403, 2021.

[HPS+17] Qing Lin He et al. Chiral majorana fermion modes in a quantum anomalous hallinsula

[HPZ+17] G. Higgins, F. Pokorny, C. Zhang, Q. Bodart, and M. Hennrich. Coherent control of a single trapped Rydberg ion, 2017, arXiv:1708.06387.

[HR06] S. Haroche and J. Raimond. *Exploring the Quantum: Atoms, Cavities, and Photons*. Oxford Graduate Texts. OUP Oxford, 2006.

[HRC02] A. W. Harrow, B. Recht, and I. L. Chuang. Efficient discrete approximations of quantum gates. *J. Math. Phys.*, 43(9):4445–4451, 2002.

[HRO+16] R. W. Heeres et al. Implementing a universal gate set on a logical qubit encoded in an oscillator, 2016, arXiv:1608.02430.

[HRP+06] T. Hime et al. Solid-state qubits with current-controlled coupling. *Science*, 314(5804):1427–1429, 2006.

[HJNRS20] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, and M. Soeken. *Improved Quantum Circuits for Elliptic Curve Discrete Logarithms*, Cryptology ePrint Archive: Report 2020/077, 2020.

[HRS17] T. Häner, M. Roetteler, and K. M. Svore. Factoring using 2n + 2 qubits with Toffoli-based modular multiplication, Quantum Information & Computation 17 (7&8), pp. 673-684, 2017.

[HS17a] T. Häner and D. S. Steiger. 0.5 petabyte simulation of a 45-qubit quantum circuit, 2017, Proc. of the International Conference for High Performance Computing, Networking, Storage and Analysis SC 2017: 33: 1-33: 10, 2017.

[HS20] A. Hosoyamada and Y. Sasaki. Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 249–279, Cham, 2020. Springer International Publishing.

[HS21] A. Hosoyamada and Y. Sasaki. Quantum Collision Attacks on Reduced SHA-256 and SHA-512. In T. Malkin and C. Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 616–646, Cham, 2021. Springer International Publishing.

[HS22] Z. Huang and S. Sun. Synthesizing Quantum Circuits of AES with Lower T-depth and Less qubits. Cryptology ePrint Archive, Paper 2022/620, 2022. A major revision of an IACR publication in ASIACRYPT 2022.

[HSA+16] T. P. Harty et al. High-fidelity trapped-ion quantum logic using near-field microwaves. *Phys. Rev. Lett.*, 117(14):140501, 2016.

[HSG+07] A. A. Houck et al. Generating single microwave photons in a circuit. *Nature*, 449(7160):328–331, Sep 2007.

[HSM06] J. Harrison, M. Sellars, and N. Manson. Measurement of the optically induced spin polarisation of n-v centres in diamond. *Diamond Relat. Mater.*, 15(4-8):586 – 588, 2006.

[HVS+11] M. Hatridge, R. Vijay, D. H. Slichter, J. Clarke, and I. Siddiqi. Dispersive magnetometry with a quantum limited squid parametric amplifier. *Phys. Rev. B*, 83(13):134501, 2011.

[HYC+18] W. Huang et al. Fidelity benchmarks for two-qubit gates in silicon. ArXiv:1805.05027.

[HZS22] S. S. Hegde, J. Zhang, and D. Suter. Toward the speed limit of high-fidelity two-qubit gates. Physical Review Letters, 128(23):230502, 2022.

[IBM18] IBM. Quantum Information Science Kit, 2018. https://qiskit.org/.

[IBM22] IBM. Quantum Road Map: https://www.ibm.com/quantum/roadmap

[ICJ+05] G. Ithier et al. Decoherence in a superconducting quantum bit circuit. *Phys. Rev. B*, 72(13):134519, 2005.

[IFI+02] L. B. Ioffe et al. Topologically protected quantum bits using josephson junction arrays. *Nature*, 415(6871):503–506, 2002.

[IIS+13] V. V. Ivanov et al. Atom trapping in a bottle beam created by a diffractive optical element, 2013, arXiv:1305.5309, https://arxiv.org/abs/1305.5309.

[Il'16] E. V. Il'ichev. A microwave photon detector. *Phys. Solid State*, 58(11):2160–2164, 2016.

[IONQ] IONQ.Algorithmic-Qubits. https://ionq.com/posts/february-23-2022-algorithmic-qubits. Accessed: 2022-10-30.

[JAG+11] M. W. Johnson et al. Quantum annealing with manufactured spins. *Nature*, 473(7346):194–198, 2011.

[JBM+18] S. Jiang, K. A. Britt, A. J. McCaskey, T. S. Humble, and S. Kais. Quantum Annealing for Prime Factorization. *Scientific reports*, 8(17667), 2018.

[JBS+22] K. Jang et al. Quantum Analysis of AES. Lowering Limit of Quantum Attack Complexity. Cryptology ePrint Archive, Paper 2022/683 (Revision from Nov 23,2023), 2022.

[JdSR+15] B. R. Johnson et al. Demonstration of robust quantum gate tomography via randomized benchmarking. *New J. Phys.*, 17(11):113019, 2015.

[JF08] S. P. Jordan and E. Farhi. Perturbative gadgets at arbitrary orders. *Phys. Rev. A*, 77(6):062329, 2008.

[JFV+11] J. Jang et al. Observation of Half-Height Magnetization Steps in Sr2RuO4. *Science*, 331(6014):186–188, 2011.

[JFS+06] S. P. Jordan, E. Farhi, and P. W. Shor. Error-correcting codes for adiabatic quantum computation. Phys. Rev. A, 74:052322, Nov 2006.

[JGBW+16] G. Jacob et al. Transmission microscopy with nanometer resolution using a deterministic single ion source. *Phys. Rev. Lett.*, 117(4):043001, 2016.

[JGLM19] D. Joseph, A. Ghionis, C. Ling, F. Mintert, Not-so-adiabatic quantum computation for the shortest vector problem, 23rd October, 2019

[JGP+04] F. Jelezko et al. Observation of coherent oscillation of a single nuclear spin and realization of a two-qubit conditional quantum gate. *Phys. Rev. Lett.*, 93(13):130501, 2004.

[JHK+16] Y.-Y. Jau, A. M. Hankin, T. Keating, I. H. Deutsch, and G. W. Biedermann. Entangling atomic spins with a rydberg-dressed spin-flip blockade. *Nat. Phys.*, 12(1):71–74, 2016.

[JJR+22] R. M. Jock, N. T. Jacobson, M. Rudolph, D. R. Ward, M. S. Carroll, and D. R. Luhman. A silicon singlet–triplet qubit driven by spin-valley coupling. Nature communications, 13(1):641, 2022.

[JKS+15] X. Y. Jin et al. Thermal and residual excited-state population in a 3d transmon qubit. *Phys. Rev. Lett.*, 114(24):240501, 2015.

[JLH+14] P. Jurcevic et al. Quasiparticle engineering and entanglement propagation in a quantum many-body system. *Nature*, 511(7508):202–205, 2014.

[JLO+24] K. Jang et al. Quantum Implementation and Analysis of SHA-2 and SHA-3. *Cryptology ePrint Archive, Paper 2024/513*, available at *https://ia.cr/2024/513*, 2024., 2024.

[JMB+18a] Jiang, K.A. Britt, A.J. McCaskey, T.S. Humble, and Sabre Kais. Quantum Annealing for Prime Factorization, Scientific Reports vol. 8, Article no. 17667, 2018.

[JNRV20] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia. *Implementing Grover oracles for quantum key search on AES and LowMC*. In Advances in Cryptology - EUROCRYPT 2020, Springer LNCS vol. 12106, pp. 280-310, 2020.

[JOB16] T. Jochym-O'Connor and S. D. Bartlett. Stacked codes: Universal fault-tolerant quantum computation in a two-dimensional layout. *Phys. Rev. A*, 93(2):022323, 2016.

[Joh28] J. B. Johnson. Thermal agitation of electricity in conductors. *Phys. Rev.*, 32(1):97–109, 1928.

[Joh17] A. M. Johnston. Shor's Algorithm and Factoring: Don't Throw Away the Odd Orders. Cryptology ePrint Archive: Report 2017/083, 2017, http://eprint.iacr.org/2017/083.

[Jon13] C. Jones. Low-overhead constructions for the fault-tolerant toffoli gate. *Phys. Rev. A*, 87:022328, Feb 2013.

[JSM+14] E. Jeffrey et al. Fast accurate state measurement with superconducting qubits. *Phys. Rev. Lett.*, 112(19):190504, 2014.

[KAHL22] M. Kowalsky, T. Albash, I. Hen, and D. A. Lidar. 3-regular three-xorsat planted solutions benchmark of classical and quantum heuristic optimizers. Quantum Science and Technology, 7(2):025008, 2022.

[Kal17] B. S. Kaliski Jr. *A Quantum "Magic Box" for the Discrete Logarithm Problem*, Cryptology ePrint Archive, Paper 2017/745, 2017.

[Kal17b] B. S. Kaliski Jr. Targeted Fibonacci exponentiation. arXiv:1711.02491, 2017.

[Kan98] B. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393(6681):133–137, 1998.

[Kas50] A. Kastler. Applications of polarimetry to infra-red and micro-wave spectroscopy. *Nature*, 166(4211):113–113, 1950.

[Kas67] A. Kastler. Optical methods for studying hertzian resonances. *Science*, 158(3798):214–221, 1967.

[Kat50] Tosio Kato. On the adiabatic theorem of quantum mechanics. *Journal of the Physical Society of Japan*, 5(6):435–439, 1950.

[LB99] S. Lloyd and S. L. Braunstein. Quantum computation over continuous variables. Physical Review Letters, 82(8):1784–1787, 1999.

[KBF+15] J. Kelly et al. State preservation by repetitive error detection in a superconducting quantum circuit. *Nature*, 519(7541):66–69, 2015.

[KBLW01] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley. Theory of decoherence-free fault-tolerant universal quantum computation. *Phys. Rev. A*, 63(4):042307, 2001.

[KC11] D. Kinion and J. Clarke. Superconducting quantum interference device as a near-quantum-limited amplifier for the axion dark-matter experiment. *Appl. Phys. Lett.*, 98(20):202503, 2011.

[KCK+10] K. Kim, M.-S. Chang, S. Korenblit, R. Islam, E. E. Edwards, J. K. Freericks, G.-D. Lin, L.-M. Duan, and C. Monroe. Quantum simulation of frustrated ising spins with trapped ions. *Nature*, 465(7298):590–593, 2010.

[KdSR+14] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki. Robust extraction of tomographic information via randomized benchmarking. *Phys. Rev. X*, 4(1), 2014.

[KEA+23] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. van den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme, and A. Kandala, Evidence for the Utility of Quantum Computing before Fault Tolerance, Nature 618, 500 (2023).

[Ken20] V. Kendon. Quantum computing using continuous-time evolution. Interface focus, 10(6):20190143, 2020.

[KGPUK16] F. Kaneda, K. Garay-Palmett, A. B. U'Ren, and P. G. Kwiat. Heralded single-photon source utilizing highly nondegenerate, spectrally factorable spontaneous parametric downconversion. *Opt. Express*, 24(10):10733–10747, May 2016.

[KHDS01] B. Koiller, X. Hu, and S. Das Sarma. Exchange in silicon-based quantum computer architecture. *Phys. Rev. Lett.*, 88(2):027903, 2001.

[KHJ18] P. Kim, D. Han, and K. C. Jeong. Time-space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2. Quantum Information Processing 17:339, 2018.

[Kie01] D. Kielpinski. A decoherence-free quantum memory using trapped ions. *Science*, 291(5506):1013–1015, 2001.

[Kim08] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[Kit97a] A. Y. Kitaev. Quantum error correction with imperfect gates. In O. Hirota, A. Holevo, and C. Caves, editors, *Proceedings of the Third International Conference on Quantum Communication, Computing and Measurement*. Plenum Press, New York, 1997.

[Kit97b] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Russ. Math. Surv.*, 52(6):1191–1249, 1997.

[Kit97c] A. Y. Kitaev. Quantum communication, computing, and measurement. In Proceedings of the 3rd International Conference of Quantum Communication and Measurement, New York: Plenum, 1997.

[Kit03] A. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003.

[Kit06] A. Kitaev. Protected qubit based on a superconducting current mirror, 2006, arXiv:cond-mat/0609441.

[KJS+16] E. Kawakami et al. Gate fidelity and coherence of an electron spin in an si/sige quantum dot with micromagnet. *Proc. Natl. Acad. Sci. U.S.A.*, 113(42):11738–11743, 2016.

[KKL+17] T. Karzig et al. Scalable designs for quasiparticle-poisoning-protected topological quantum computation with majorana zero modes. *Phys. Rev. B*, 95(23):235305, 2017.

[KKR06] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, 2006.

[KLC+15] J. Kerckhoff, K. Lalumière, B. J. Chapman, A. Blais, and K. W. Lehnert. On-chip superconducting microwave circulator from synthetic rotation. *Phys. Rev. Applied*, 4(3):034002, 2015.

[KLFF+15] A. M. Kaufman et al. Entangling two transportable neutral atoms via local spin exchange. *Nature*, 527(7577):208–211, 2015.

[KLH+04] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther. Continuous generation of single photons with controlled waveform in an ion-trap cavity system. *Nature*, 431(7012):1075–1078, Oct 2004.

[KLHM14] R. Kalra, A. Laucht, C. D. Hill, and A. Morello. Robust two-qubit gates for donors in silicon controlled by hyperfine interactions. *Phys. Rev. X*, 4(2):021044, 2014.

[Kli13] V. Kliuchnikov. Synthesis of unitaries with Clifford+T circuits. arXiv:1306.3200, 2013.

[KLLNP16] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Transactions on Symmetric Cryptology*, 2016(1), 2016.

[KLM01] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[KLNP16] M. Kaplan, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Advances in Cryptology – CRYPTO 2016*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016.

[KLR+08] E. Knill et al. Randomized benchmarking of quantum gates. *Phys. Rev. A*, 77(1):012307, 2008.

[KLR+22] S. Krinner et al. Realizing repeated quantum error correction in a distance-three surface code. Nature, 605(7911):669–674, 2022.

[KMBD06] C. Kruszynska, A. Miyake, H. J. Briegel, and W. Dür. Entanglement purification protocols for all graph states. *Phys. Rev. A*, 74(5):052316, 2006.

[KMW02] D. Kielpinski, C. Monroe, and D. J. Wineland. Architecture for a large-scale ion-trap quantum computer. *Nature*, 417(6890):709–711, 2002.

[KMY24] G. D. Kahanamoku-Meyer and N.Y. Yao. Fast quantum integer multiplication with zero ancillas, arXiv:2403.18006, 2024.

[KN98] T. Kadowaki and H. Nishimori. Quantum annealing in the transverse ising model. *Physical Review E*, 58(5):5355, 1998.

[Kni05] E. Knill. Quantum computing with realistically noisy devices. *Nature*, 434(7029):39–44, 2005.

[Kor08] A. N. Korotkov. Quantum efficiency of binary-outcome detectors of solid-state qubits. *Phys. Rev. B*, 78(17):174512, 2008.

[Kre22] Mario Krenn. Largest genuine Entanglement:Qubits in GHZ state. https://mariokrenn.wordpress.com/2021/01/29/reference-list-for-records-in-large-entanglement-generation-number-of-qubits-in-ghz-states/.Accessed: 2022-09-30

[KRG+23] L. Kranz, S. Roche, S. K. Gorman, J. G. Keizer, and M. Y. Simmons. High-fidelity cnot gate for donor electron spin qubits in silicon. Phys. Rev. Appl., 19:024068, Feb 2023.

[KRK+05] N. Khaneja, T. Reiss, C. Kehlet, T. Schulte-Herbrüggen, and S. J. Glaser. Optimal control of coupled spin dynamics: design of {NMR} pulse sequences by gradient ascent algorithms. *J. Magn. Reson.*, 172(2):296 – 305, 2005.

[KRS+17] H. Kaufmann et al. Scalable creation of long-lived multipartite entanglement. *Phys. Rev. Lett.*, 119:150503, Oct 2017.

[KSB+16] P. Kumar et al. Origin and reduction of 1/*f* magnetic flux noise in superconducting devices. *Phys. Rev. Applied*, 6(4):041001, 2016.

[KSK+21] A. H. Karamlou et al. Analyzing the performance of variational quantum factoring on a superconducting quantum processor. npj Quantum Information, 7(1):1–6, 2021.

[KSR+22] A. D. King et al. Coherent quantum annealing in a programmable 2,000 qubit ising chain. Nature Physics,18(11):1324–1328, 2022.

[KSS+14] D. Kim et al. Quantum control and process tomography of a semiconductor quantum dot hybrid qubit. *Nature*, 511(7507):70–74, July 2014.

[KWS+20] A. Kandala et al. Demonstration ofa high-fidelity cnot for fixed-frequency transmons with engineeredzz suppression.arXiv preprint arXiv:2011.07050, 2020.

[KTC+19] A. Kandala et al. Error Mitigation Extends the Computational Reach of a Noisy Quantum Processor, Nature 567, 491, 2019.

[KXB+16] D. Korenkevych et al. Benchmarking quantum hardware for training of fully visible boltzmann machines, 2016, arXiv:1611.04528.[KYG+07] J. Koch et al. Charge-insensitive qubit design derived from the Cooper pair box. *Phys. Rev. A*, 76:042319, 2007.

[KYP15] A. Kubica, B. Yoshida, and F. Pastawski. Unfolding the color code. *New J. Phys.*, 17(8):083026, 2015.

[KZ04] P. Kaye and C. Zalka. Optimized quantum implementation of elliptic curve arithmetic over binary fields, 2004.

[Lan95] R. Landauer. Is quantum mechanics useful? *Phil. Trans. R. Soc. A*, 353(1703):367–376, 1995.

[Law15] T. Lawson. Odd orders in Shor's factoring algorithm. *Quantum Information Processing*, 14:831–838, 2015.

[LB13] D. A. Lidar and T. A. Brun. *Quantum Error Correction*, chapter Introduction to decoherence and noise in open quantum systems, pages 3–45. Cambridge University Press, 2013.

[LBH+16] J. C. Loredo et al. Bosonsampling with single-photon fock states from a bright solid-state source, 2016, arXiv:1603.00054, PRL to appear, https://arxiv.org/abs/1603.00054v1.

[LBM+16] J. Lisenfeld et al. Decoherence spectroscopy with individual two-level tunneling defects. *Sci. Rep.*, 6:23786–, 2016.

[LCYY00] D. W. Leung, I. L. Chuang, F. Yamaguchi, and Y. Yamamoto. Efficient implementation of coupled logic gates for quantum computation. *Phys. Rev. A*, 61(4):042310, 2000.

[LCE+21] Y.-H. Luo et al. Quantum teleportation of physical qubits into logical code spaces. *Proceedings of the National Academy of Sciences*, 118(36):e2026250118, 2021.

[LD98] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57(1):120–126, 1998.

[LDP+17] X. Lin et al. Electrically-driven single-photon sources based on colloidal quantum dots with near-optimal antibunching at room temperature. *Nature Communications*, 8(1):1132, 2017.

[Leg80] A. J. Leggett. Macroscopic quantum systems and the quantum theory of measurement. *Progr. Theor. Phys.*, 69:80, 1980.

[Lev01] M. Levitt. *Spin Dynamics: Basics of Nuclear Magnetic Resonance*. Spin Dynamics: Basics of Nuclear Magnetic Resonance. Wiley, 2001.

[LGA+08] J. Labaziewicz et al. Suppression of heating rates in cryogenic surface-electrode ion traps. *Phys. Rev. Lett.*, 100(1):013001, 2008.

[LGB+19] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen. Deterministic generation of a two-dimensional cluster state. Science, 366(6463):369–372, 2019.

[LGL05] R. Lutchyn, L. Glazman, A. Larkin, Quasiparticle decay rate of Josephson charge qubit oscillations, *Phys. Rev. B,* 72, 014517 (2005)

[LGQW23] Z. Li, F. Gao, S. Qin, and Q. Wen, *New record in the number of qubits for a quantum implementation of AES*, Cryptology ePrint Archive, Paper 2023/018, 2023.

[LH10] M. Lieb, M. J. Hartmann, Bose–Hubbard dynamics of polaritons in a chain of circuit quantum electrodynamics cavities, New Journal of Physics, Volume 12, September 2010.

[LHA+08] E. Lucero et al. High-fidelity gates in a single josephson qubit. *Phys. Rev. Lett.*, 100(24):247001, 2008.

[LHZ15] W. Lechner, P. Hauke, and P. Zoller. A quantum annealing architecture with all-to-all connectivity from local interactions. *Sci. Adv.*, 1(9):e1500838–e1500838, 2015.

[Li15] Y. Li. A magic state's fidelity can be superior to the operations that created it. *New J. Phys.*, 17(2):023037, 2015.

[Lin76] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.*, 48:119–130, 1976.

[Lit23] D. Litinski. How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates, arXiv:2306.08585, 2023.

[LJH+13] E. J. H. Lee et al. Spin-resolved andreev levels and parity crossings in hybrid superconductor–semiconductor nanostructures. *Nat. Nanotechnol.*, 9(1):79–84, 2013.

[LJV+21] T. Lubinski et al. Application-oriented performance benchmarks for quantum computing. 2021, arXiv:2110.03137.

[LKB+10] E. Lucero et al. Reduced phase error through optimized control of a superconducting qubit. *Phys. Rev. A*, 82(4):042339, 2010.

[LKEH17] T. Lanting, A. D. King, B. Evert, and E. Hoskinson. Experimental demonstration of perturbative anticrossing mitigation using nonuniform driver hamiltonians. *Phys. Rev. A*, 96:042322, Oct 2017.

[LKF+22] V. Langrock et al. Blueprint of a scalable spin qubit shuttle device for coherent mid-range qubit transfer in disordered si/sige/sio 2. PRX Quantum, 4(2):020305, 2023.

[LKV+13] Z. Leghtas et al. Hardware-efficient autonomous quantum memory protection. *Phys. Rev. Lett.*, 111(12):120501, 2013.

[LKS+19] H. Levine et al. Parallel implementation of high-fidelity multiqubit gates with neutral atoms. Phys. Rev. Lett., 123:170503, Oct 2019.

[LL01] M. N. Leuenberger and D. Loss. Quantum computing in molecular magnets. *Nature*, 410(6830):789–793, 2001.

[LLF+18] P.H. Leung et al. Robust 2-qubit Gates in a Linear Ion Crystal Using a Frequency-Modulated Driving Force. *Phys. Rev. Lett.,* 120(02):02001, 2018.

[LmcHM05] A. Lupaşcu, C. J. P. M. Harmans, and J. E. Mooij. Quantum state detection of a superconducting flux qubit using a dc-SQUID in the inductive mode. *Phys. Rev. B*, 71(18):184506, May 2005.

[LMR+17] N. M. Linke et al. Experimental comparison of two quantum computing architectures. 2017, arXiv:1702.01852.

[LPK+15] T. W. Larsen et al. Semiconductor-nanowire-based superconducting qubit. *Phys. Rev. Lett.*, 115(12):127001, 2015.

[LPS+14] T. Lanting et al. Entanglement in a quantum annealing processor. *Phys. Rev. X*, 4(2):021041, 2014.

[LPS20] B. Langenberg, H. Pham, and R. Steinwandt. *Reducing the Cost of Implementing AES as a Quantum Circuit*. IEEE Transactions on Quantum Engineering, 2020. Preprint available as Cryptology ePrint Archive: Report 2019/854.

[LPZW23] Q. Liu, B. Preneel, Z. Zhao, and M. Wang. Improved Quantum Circuits for AES: Reducing the Depth and the Number of Qubits. In: Guo, J., Steinfeld, R. (eds) *Advances in Cryptology – ASIACRYPT 2023. ASIACRYPT 2023.* Lecture Notes in Computer Science, vol 14440. Springer, Singapore, 2023. Minor revision available at https://ia.cr/2023/1417.

[LSDS10] R. M. Lutchyn, J. D. Sau, and S. Das Sarma. Majorana fermions and a topological phase transition in semiconductor-superconductor heterostructures. *Phys. Rev. Lett.*, 105(7):077001, 2010.

[LT20] L. Lin and Y. Tong. Optimal polynomial based quantum eigenstate filtering with application to solving quantum linear systems. *Quantum* 4, 361, 2020.

[LTD+10] E. A. Laird et al. Coherent spin manipulation in an exchange-only qubit. *Phys. Rev. B*, 82(7):075403, 2010.

[LTW+24] M. Larocca et al. A review of Barren Plateaus in Variational Quantum Computing. *ArXiv:*2405.00781, 2024.

[LW03] D. A. Lidar and K. B. Whaley. *Irreversible Quantum Dynamics*, volume 622 of *Springer Lecture Notes in Physics*, chapter Decoherence-Free Subspaces and Subsystems, pages 83–120. Springer, 2003.

[LWF+17] B. Lekitsch et al. Blueprint for a microwave trapped ion quantum computer. *Sci. Adv.*, 3(2):e1601540, 2017.

[LWS+21] G. Li et al. On the co-design of quantum software and hardware. In Proceedings of the Eight Annual ACM International Conference on Nanoscale Computing and Communication, pages 1–7, 2021.

[LZA+17] L. Li et al. Cat Codes with Optimal Decoherence Suppression for a Lossy Bosonic Channel. Physical Review Letters, 119(3):030502, July 2017. doi: 10.1103/PhysRevLett.119.030502.

[LZG+07] C.-Y. Lu, X.-Q. Zhou et al. Experimental entanglement of six photons in graph states. 3:91–95, Jan 2007.

[Mak02] Y. Makhlin. Nonlocal properties of two-qubit gates and mixed states, and the optimization of quantum computations. *Quantum Inf. Process.*, 1(4):243–252, 2002.

[Mar15] J. M. Martinis. Qubit metrology for building a fault-tolerant quantum computer, 2015, arxiv:1510.01406v1, http://arxiv.org/abs/1510.01406v1.

[Mar17] J. M. Martinis, 2017, http://www.acm.org/articles/people-of-acm/2017/john-martinis.

[Mau07] P. Maunz. High-fidelity operations in microfabricated surface ion traps. 2007.

[MAY+22] M. T. Madzik et al. Precision tomography of a three-qubit donor quantum processor in silicon. Nature, 601(7893):348–353, 2022.

[MBA+23] S. A. Moses et al. A Race-Track Trapped-Ion Quantum Processor. Physical Review X, 13(4):041052, December 2023. Publisher: American Physical Society.

[MB23] J. Mielke and G. Burkard. Dispersive cavity-mediated quantum gate between driven dot-donor nuclear spins. Physical Review B, 107(15):155302, 2023.

[MBB+16] T. Meany et al. Engineering integrated photonics for heralded quantum gates. *Sci. Rep.*, 6:25126, 2016.

[MBB+18] N.Moll et al. Quantum optimization using variational algorithms on near-term quantum devices. *Quantum Science and Technology 3*, 030503, 2018.

[MBB+22] Menke et al. Demonstration of tunable three-body interactions between superconducting qubits. Physical Review Letters, 129(22):220501, 2022.

[MBV20] M. Mosca, J.M.V. Basso, and S.R. Verschoor. On speeding up factoring with quantum SAT solvers. *Sci Rep* 10, 15022 (2020). https://doi.org/10.1038/s41598-020-71654-y

[MCP+17] A. C. Mahoney et al. On-chip microwave quantum hall circulator. *Phys. Rev. X*, 7(1):011007, 2017.

[MdARC+14] R. Medeiros de Araújo et al. Full characterization of a highly multimode entangled state embedded in an optical frequency comb using pulse shaping. *Phys. Rev. A*, 89:053828, May 2014.

[McKWS+17] D.C. McKay, C.J.W Wood, S. Sheldon, J.M. Chow, and J.M. Gambetta. Efficient Z gates for quantum computing. *Phys. Rev. A.* 96(2):022330, 2017.

[MDL+14] J. T. Muhonen et al. Storing quantum information for 30 seconds in a nanoelectronic device. *Nat. Nano.*, 9(12):986–991, 2014.

[MEMA+24] M. McEwen et al. Resisting high-energy impact events through gap engineering in superconducting superconducting qubit arrays. *ArXiv*:2402.15644, 2024.

[Men14] N. C. Menicucci. Fault-tolerant measurement-based quantum computing with continuous-variable cluster states. *Phys. Rev. Lett.*, 112(12):120504, 2014.

[Mes67] A Messiah. Quantum mechanics. *Wiley, New York*, 1967.

[MFZP07] N. C. Menicucci, S. T. Flammia, H. Zaidi, and O. Pfister. Ultracompact generation of continuous-variable cluster states. *Phys. Rev. A*, 76:010302, Jul 2007.

[MGE11] E. Magesan, J. M. Gambetta, and J. Emerson. Scalable and robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.*, 106(18):180504, 2011.

[MGE12] E. Magesan, J. M. Gambetta, and J. Emerson. Characterizing quantum gates via randomized benchmarking. *Phys. Rev. A*, 85(4):042311, 2012.

[MGF+22] A. Mills et al. High-fidelity state preparation, quantum control, and readout of an isotopically enriched silicon spin qubit. Physical Review Applied, 18(6):064028, December 12, 2022.

[MGG+22] A. R. Mills et al. Two-qubit silicon quantum processor with operation fidelity exceeding 99%. Science Advances, 8(14):eabn5130, April 6, 2022.

[MGJ+12] E. Magesan et al. Efficient measurement of quantum gate error by interleaved randomized benchmarking. *Phys. Rev. Lett.*, 109(8):080505, 2012.

[MGRW09] F. Motzoi, J. M. Gambetta, P. Rebentrost, and F. K. Wilhelm. Simple pulses for elimination of leakage in weakly nonlinear qubits. *Phys. Rev. Lett.*, 103(11):110501, 2009.

[MGS+13] S. T. Merkel et al. Self-consistent quantum process tomography. *Phys. Rev. A*, 87(6), 2013.

[MGW+03] O. Mandel et al. Controlled collisions for multi-particle entanglement of optically trapped atoms. *Nature*, 425(6961):937–940, 2003.

[MHP+23] D. C. McKay et al. Benchmarking Quantum Processor Performance at Scale. November 10, 2023. arXiv: 2311.05933

[Mic18] Microsoft. Quantum Development Kit, 2018, https://www.microsoft.com/en-us/quantum/development-kit.

[Mir16] M. Mirrahimi. Cat-qubits for quantum computation. *Comptes Rendus Physique*, 17(7):778 – 787, 2016.

[MJ22] A. Mahasinghe and Y.Jayasinghe. An initial step toward a quantum annealing approach to the discrete logarithm problem. *Security and Privacy,* 5(4):e234, 2022, doi:10.1002/spy2.234.

[MK13] C. Monroe and J. Kim. Scaling the ion trap quantum processor. *Science*, 339(6124):1164–1169, 2013.

[MKC+15] E. Mount et al. Error compensation of single-qubit gates in a surface-electrode ion trap using composite pulses. *Phys. Rev. A*, 92(6):060301, 2015.

[MKT+00] C. J. Myatt et al. Decoherence of quantum superpositions through coupling to engineered reservoirs. *Nature*, 403(6767):269–273, 2000.

[MLA+14] M. Mirrahimi et al. Dynamically protected cat-qubits: a new paradigm for universal quantum computation. *New J. Phys.*, 16(4):045014, 2014.

[MLA+22] L. S Madsen et al. Quantum computational advantage with a programmable, photonic processor. Nature, 606(7912):75–81, 2022

[MLS+15] J. Muhonen et al. Quantifying the quantum gate fidelity of single-atom spin qubits in silicon by randomized benchmarking. *J. Phys.: Condens. Matter*, 27(15):154205, 2015.

[MLX+15] K. M. Maller et al. Rydberg-blockade controlled-not gate and entanglement in a two-dimensional array of neutral-atom qubits. *Phys. Rev. A*, 92:022336, Aug 2015.

[MMCP09] D. Maslov, J. Mathew, D. Cheung, and D. K. Pradhan. An $O(m^2)$-depth quantum algorith for the elliptic curve discrete logarithm problem over GF(2^m). *Quantum Inf. Comput.*, 9(7):610–621, 2009.

[MMEA+23] K. C. Miao et al. Overcoming leakage in quantum error correction. *Nat. Phys.* 19, 1780-1786, 2023.

[MMK+95] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.*, 75(25):4714–4717, 1995.

[MMK+12] N. Mizuochi et al. Electrically driven single-photon source at room temperature in diamond. 6:299 EP –, Apr 2012.

[MMN+17a] F. K. Malinowski, F. Martins, P. D. Nissen, E. Barnes, C. Łukasz, M. S. Rudner, S. Fallahi, G. C. Gardner, M. J. Manfra, C. M. Marcus, and F. Kuemmeth. Notch filtering the nuclear environment of a spin qubit. *Nat. Nanotechnol.*, 12(1):16–20, 2017.

[MMN+17b] F. K. Malinowski et al. Symmetric operation of the resonant exchange qubit. *Phys. Rev. B*, 96:045443, Jul 2017.

[MOH+15] C. Macklin et al. A near–quantum-limited josephson traveling-wave parametric amplifier. *Science*, 2015.

[MOL+99] J. E. Mooij et al. Josephson persistent-current qubit. *Science*, 285(5430):1036–1039, 1999.

[MPB+15] R. Marx et al. Engineering of an all-heteronuclear 5-qubit nmr quantum computer. *Magn. Reson. Chem.*, 53(6):442–447, 2015.

[MPB21] J. Mielke, J. R. Petta, and G. Burkard. Nuclear spin readout in a cavity-coupled hybrid quantum dot-donor system. PRX Quantum, 2(2):020347, 2021.

[MPBJ20] A. Morello, J. J. Pla, P. Bertet, and D. N. Jamieson. Donor spins in silicon for quantum technologies. Advanced Quantum Technologies, 3(11):2000005, 2020.

[MPS+21] W.-L. Ma, S. Puri, R. J. Schoelkopf, M. H. Devoret, S. M. Girvin, and L. Jiang. Quantum control of bosonic modes with superconducting circuits. *Science Bulletin*, 66(17):1789–1805, 2021.

[MPZ+10] A. Morello et al. Single-shot readout of an electron spin in silicon. *Nature*, 467(7316):687–691, 2010.

[MRR+14] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim. Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects. *Phys. Rev. A*, 89(2):022317, 2014.

[MS04] Y. Makhlin and A. Shnirman. Dephasing of solid-state qubits at optimal points. *Phys. Rev. Lett.*, 92(17):178301, 2004.

[MSB+11] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt. 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.*, 106(13):130506, 2011.

[MSB+16] M. H. Michael et al. New Class of Quantum Error-Correcting Codes for a Bosonic Mode. Physical Review X, 6(3):031006, July 2016. Publisher: American Physical Society.

[MSBS+23] A. Misra-Spieldenner et al. Mean-Field Approximate Optimization Algorithm. *PRX Quantum* 4, 030335, 2023.

[MSK+20] P. Magnard et al. Microwave quantum link between super-conducting circuits housed in spatially separated cryogenic sys-tems.Physical Review Letters, 125(26):260502, 2020.

[MSS00a] Y. Makhlin, G. Schön, and A. Shnirman. Nano-electronic realizations of quantum bits. *J. Low Temp. Phys.*, 118(5):751–763, 2000.

[MSS00b] Y. Makhlin, G. Schön, G.n, and A. Shnirman. Josephson-junction qubits. *Fortschr. Phys.*, 48(9-11):1043–1054, 2000.

[MSW+08] A. H. Myerson, D. J. Szwer, S. C. Webster, D. T. C. Allcock, M. J. Curtis, G. Imreh, J. A. Sherman, D. N. Stacey, A. M. Steane, and D. M. Lucas. High-fidelity readout of trapped-ion qubits. *Phys. Rev. Lett.*, 100(20):200502, 2008.

[MV22] M. Mosca and S.R. Verschoor. Factoring semi-primes with (quantum) SAT-solvers. *Sci Rep* 12, 7982 (2022). https://doi.org/10.1038/s41598-022-11687-7

[MVP+17] R. McDermott, M. G. Vavilov, B. L. T. Plourde, F. K. Wilhelm, P. J. Liebermann, O. A. Mukhanov, and T. A. Ohki. Quantum–classical interface based on single flux quantum digital logic, 2017, arXiv:1710.04645.

[MvTA+07] G. W. Morley, J. van Tol, A. Ardavan, K. Porfyrakis, J. Zhang, and G. A. D. Briggs. Efficient dynamic nuclear polarization at high magnetic fields. *Phys. Rev. Lett.*, 98(22):220501, 2007.

[MW01] F. Mintert and C. Wunderlich. Ion-trap quantum logic using long-wavelength radiation. *Phys. Rev. Lett.*, 87(25):257904, 2001.

[MZ04] M. Mosca and C. Zalka. Exact Quantum Fourier Transforms and Discrete Logarithm Algorithms. *Int. J. Quantum Inf.*, 2(1):91–100, 2004.

[MZF+12] V. Mourik, K. Zuo, S. M. Frolov, S. R. Plissard, E. P. A. M. Bakkers, and L. P. Kouwenhoven. Signatures of majorana fermions in hybrid superconductor-semiconductor nanowire devices. *Science*, 336(6084):1003–1007, 2012, http://science.sciencemag.org/content/336/6084/1003.full.pdf.

[Nam17] Y. Nam. Running Shor's Algorithm on a complete, gate-by-gate implementation of a virtual, universal quantum computer, April 2017.

[NB15a] Y. S. Nam and R. Blümel. Analytical formulas for the performance scaling of quantum processors with a large number of defective gates. *Phys. Rev. A*, 92, 2015.

[NB15b] Y. Nam and R. Blümel. Performance scaling of the quantum Fourier transform with defective rotation gates. *Quantum Inf. Comput.*, 15(9 & 10):0721–0746, 2015.

[NB17] Y. S. Nam and R. Blümel. Optimal length of decomposition sequences composed of imperfect gates. *Quantum Inf. Process.*, 16(5), 2017.

[NBS+10] P. Neumann, J. Beck, M. Steiner, F. Rempp, H. Fedder, P. R. Hemmer, J. Wrachtrup, and F. Jelezko. Single-shot readout of a single nuclear spin. *Science*, 329(5991):542–544, 2010.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NEJ+22] D. J. Niegemann et al. Parity and singlet-triplet high-fidelity readout in a silicon double quantum dot at 0.5 k. PRX Quantum, 3:040335, Dec 2022

[NER16] G. J. K. Nielsen E, Rudinger K and B.-K. R. pygsti: A python implementation of gate set tomography. http://github.com/pygstio, 2016.

[NFC09] J. Niset, J. Fiurášek, and N. J. Cerf. No-go theorem for gaussian quantum error correction. *Phys. Rev. Lett.*, 102(12):120501, 2009.

[NIS99] NIST. Data Encryption Standard (DES). Federal Information Processing Standards Publication 46-3, 1999.

[NIS01] NIST. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.

[NIS15a] NIST. Secure Hash Standard (SHS). Federal Information Processing Standards Publication 180-4, 2015.

[NIS15b] NIST. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Federal Information Processing Standards Publication 202, 2015.

[NIS16] NIST. Advancing quantum information science: National challenges and opportunities, 2016.

[NMM+14] D. Nigg et al. Quantum computations on a topologically encoded qubit. *Science*, 345(6194):302–305, 2014.

[NMR+06] C. Negrevergne et al. Benchmarking quantum control methods on a 12-qubit system. *Phys. Rev. Lett.*, 96(17):170501, 2006.

[NMR+08] P. Neumann et al. Multipartite entanglement among single spins in diamond. *Science*, 320(5881):1326–1329, 2008, http://science.sciencemag.org/content/320/5881/1326.full.pdf.

[NPT99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooper-pair box. *Nature*, 398(6730):786–788, 1999.

[NRK+17] C. Neill et al. A blueprint for demonstrating quantum supremacy with superconducting qubits, 2017, arXiv:1709.06678.

[NSL+11] K. C. Nowack et al. Single-shot correlations and two-qubit gate of solid-state spins. *Science*, 333(6047):1269–1272, 2011, http://science.sciencemag.org/content/333/6047/1269.full.pdf.

[NSM20] Y. Nam, Y. Su, and D. Maslov. Approximate Quantum Fourier Transform with O(nlog(n)) T gates, npj Quantum Information vol. 6, Article no. 26, 2020.

[NSS+08] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma. Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80(3):1083–1159, 2008.

[NTC11] A. Negretti, P. Treutlein, and T. Calarco. Quantum computing implementations with neutral particles. *Quantum Inf. Process.*, 10(6):721, 2011.

[NTD+14] K. Nemoto et al. Photonic architecture for scalable quantum information processing in diamond. *Phys. Rev. X*, 4(3):031022, 2014.

[Nyq28] H. Nyquist. Thermal agitation of electric charge in conductors. *Phys. Rev.*, 32(1):110–113, 1928.

[NZW+24] S. Neyens et al. Probing single electrons across 300-mm spin qubit wafers. Nature, 629(8010):80–85, May 2024.

[OBK+16] P. J. J. O'Malley et al. Scalable quantum simulation of molecular energies. *Phys. Rev. X*, 6(3):031007, 2016.

[OC17] J. O'Gorman and E. T. Campbell. Quantum computation with realistic magic-state factories. *Phys. Rev. A*, 95(3):032338, 2017.

[OFV09] J. L. O'Brien, A. Furusawa, and J. Vuckovic. Photonic quantum technologies. *Nat. Photon.*, 3(12):687–695, 2009.

[OK91] W. Ogata and K. Kurosawa. On Claw Free Families. In *International Conference on the Theory and Applications of Cryptology (ASIACRYPT '91)*, pages 111–123, 1991.

[OMM+09] S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan, and C. Monroe. Quantum teleportation between distant matter qubits. *Science*, 323(5913):486–489, 2009.

[OMT+99] T. P. Orlando et al. Superconducting persistent-current qubit. *Phys. Rev. B*, 60(22):15398–15413, 1999.

[OOHT11] R. Okamoto, J. L. O'Brien, H. F. Hofmann, and S. Takeuchi. Realization of a knill-laflamme-milburn controlled-not photonic quantum circuit combining effective optical nonlinearities. *Proc. Natl. Acad. Sci. U.S.A.*, 108(25):10067–10071, 2011.

[OOT+17] T. Ono, R. Okamoto, M. Tanida, H. F. Hofmann, and S. Takeuchi. Implementation of a quantum controlled-swap gate with photonic circuits. 7:45353, Mar 2017.

[OPH+16] N. Ofek et al. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, 536(7617):441–445, 2016.

[OPLTT12] T. Obata, M. Pioro-Ladrière, Y. Tokura, and S. Tarucha. The photon-assisted dynamic nuclear polarization effect in a double quantum dot. *New J. Phys.*, 14(12):123013–, 2012.

[OPW+03] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning. Demonstration of an all-optical quantum controlled-not gate. *Nature*, 426(6964):264–267, 2003.

[ORvO10] Y. Oreg, G. Refael, and F. von Oppen. Helical liquids and majorana bound states in quantum wires. *Phys. Rev. Lett.*, 105(17):177002, 2010.

[OWC+11] C. Ospelkaus, U. Warring, Y. Colombe, K. R. Brown, J. M. Amini, D. Leibfried, and D. J. Wineland. Microwave quantum logic gates for trapped ions. *Nature*, 476(7359):181–184, 2011.

[Oxf17] Oxford Instruments, 2017, https://www.oxford-instruments.com/products/cryogenic-environments/dilution-refrigerator/cryogen-free-dilution-refrigerators/tritonxl.

[OYL+05] W. D. Oliver, Y. Yu, J. C. Lee, K. K. Berggren, L. S. Levitov, and T. P. Orlando. Mach-zehnder interferometry in a strongly driven superconducting qubit. *Science*, 310(5754):1653–1657, 2005.

[PAL14] K. L. Pudenz, T. Albash, and D. A. Lidar. Error-corrected quantum annealing with hundreds of qubits. *Nat. Commun.*, 5, 2014.

[PAS18] PASQuanS https://pasquans.eu/

[Pau90] W. Paul. Electromagnetic traps for charged and neutral particles. *Rev. Mod. Phys.*, 62(3):531–540, 1990.

[POB22] A. Paler, O. Oumarou, and R. Basmadjian. On the Realistic Worst-Case Analysis of Quantum Arithmetic Circuits. *IEEE Transactions on Quantum Engineering*, 3:1–11, 2022.

[PB22] A. Paler and R. Basmadjian. Energy Cost of Quantum Circuit Optimisation: Predicting That Optimising Shor's Algorithm Circuit Uses 1 GWh. *ACM Transactions on Quantum Computing*, 3(1), January 2022.

[PBA14] D. Paredes-Barato and C. S. Adams. All-optical quantum information processing using rydberg gates. *Phys. Rev. Lett.*, 112(4):040501, 2014.

[PBB17] S. Puri, S. Boutin, and A. Blais. Engineering the quantum states of light in a Kerr-nonlinear resonator by two-photon driving. en. npj Quantum Information, 3(1):1–7, April 2017. issn: 2056-6387. doi: 10.1038/s41534-017-0019-1.

[PBS+22] N. Piot et al. A single hole spin with enhanced coherence in natural silicon. Naturenanonotechnology, 17(10):1072–1077, 2022.

[PCR+08] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien. Silica-on-silicon waveguide quantum circuits. *Science*, 320(5876):646–649, 2008, http://science.sciencemag.org/content/320/5876/646.full.pdf.

[PdGHM07] J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij. Demonstration of controlled-not quantum gates on a pair of superconducting quantum bits. *Nature*, 447(7146):836–839, 2007.

[PF13] A. Paetznick and A. G. Fowler. Quantum circuit optimization by topological compaction in the surface code, 2013, arXiv:1304.2807.

[PFR+15] D. K. Park et al. Hyperfine spin qubits in irradiated malonic acid: heat-bath algorithmic cooling. *Quantum Inf. Process.*, 14(7):2435–2461, 2015.

[PGC+14] I. M. Pop et al. Coherent suppression of electromagnetic dissipation due to superconducting quasiparticles. *Nature*, 508(7496):369–372, 2014.

[PHP+22] L. Postler et al. Demonstration of fault-tolerant universal quantum gate operations. Nature, 605(7911):675–680, 2022.

[PGMG19] E Pednault, J Gunnels, D Maslov, J Gambetta. On Quantum Supremacy, IBM Blog, 2019

[Phi98] W. D. Phillips. Nobel lecture: Laser cooling and trapping of neutral atoms. *Rev. Mod. Phys.*, 70(3):721–741, 1998.

[Pil24] C. Pilatte. Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms. Cryptology ePrint Archive, Paper 2024/629, 2024.

[PJM+04] J. R. Petta, A. C. Johnson, C. M. Marcus, M. P. Hanson, and A. C. Gossard. Manipulation of a single charge in a double quantum dot. *Phys. Rev. Lett.*, 93:186802, Oct 2004.

[PJT+05] J. R. Petta et al. Coherent manipulation of coupled electron spins in semiconductor quantum dots. *Science*, 309(5744):2180–2184, 2005, http://science.sciencemag.org/content/309/5744/2180.full.pdf.

[PJY+05] J. R. Petta et al. Pulsed-gate measurements of the singlet-triplet relaxation time in a two-electron double quantum dot. *Phys. Rev. B*, 72(16):161301, 2005.

[PKS17] M. D. Penny, D. E. Koh, R. W. Spekkens, Quantum circuit dynamics via path integrals: Is there a classical action for discrete-time paths. New J. Phys. 19 (2017) 073006

[Pla19] R. Player. *On the condition number of Macaulay matrices*. Presentation at Dagstuhl Seminar 19421 Quantum Cryptanalysis, October 2019.

[PLOT+08] M. Pioro-Ladrière, T. Obata, Y. Tokura, Y.-S. Shin, T. Kubo, K. Yoshida, T. Taniyama, and S. Tarucha. Electrically driven single-electron spin resonance in a slanting zeeman field. *Nat. Phys.*, 4(10):776–779, 2008.

[PLP+11] A. Peruzzo, A. Laing, A. Politi, T. Rudolph, and J. L. O'Brien. Multimode quantum interference of photons in multiport integrated devices. *Nat. Commun.*, 2:224 EP –, 2011.

[PLX+08] Xinhua Peng et al. Quantum adiabatic algorithm for factorization and its experimental implementation.Physicalreview letters, 101(22):220405, 2008.

[PMS+16] H. Paik et al. Experimental demonstration of a resonator-induced phase gate in a multiqubit circuit-qed system. *Phys. Rev. Lett.*, 117(25):250502, 2016.

[PNH+24] H. Putterman et al. Hardware-efficient quantum error correction using concatenated bosonic qubits. September 19, 2024. doi: 10. 48550/arXiv.2409.13025. arXiv: 2409.13025. Pre-published.

[Pob96] F. Pobell. *Matter and Methods at Low Temperatures*. Springer-Verlag, 1996.

[Poz12] D. Pozar. *Microwave Engineering*. Wiley, 2012.

[Pre97a] J. Preskill. Fault-tolerant quantum computation, 1997, arXiv:quant-ph/9712048v1, https://arxiv.org/abs/quant-ph/9712048v1.

[Pre97b] J. Preskill. Reliable quantum computers. 1997, arXiv:quant-ph/9705031.

[Pre12] J. Preskill. Quantum computing and the entanglement frontier, 2012, arXiv:1203.5813.

[Pre18] J. Preskill, Quantum computing in the NISQ era and beyond, Quantum, 2:79, 2018.

[Pre22] R. Preston. Applying Grover's Algorithm to Hash Functions: A Software Perspective, 2022, arXiv:2202.10982.

[PREF17] S. Plugge, A. Rasmussen, R. Egger, and K. Flensberg. Majorana box qubits. *New J. Phys.*, 19(1):012001, 2017.

[PRM+21] P. Place et al. New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds. Nature communications, 12(1):1779, 2021.

[PRY+17] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout. What randomized benchmarking actually measures, 2017, arXiv:1702.01853.

[PS53] W. Paul and H. Steinwedel. Ein neues Massenspektrometer ohne Magnetfeld. *Z. Naturforsch. A*, 8:448–450, 1953.

[PS13] P. Pham and K. M. Svore. A 2D Nearest-Neighbor Quantum Architecture for Factoring in Polylogarithmic Depth. *Quantum Inf. Comput.*, 13(11 & 12):0937–0962, 2013.

[PS22] C. Piveteau and D. Sutter. Circuit knitting with classical communication. arXiv preprint arXiv:2205.00016, 2022.

[PSB+11] H. Paik et al. Observation of high coherence in josephson junction qubits measured in a three-dimensional circuit qed architecture. *Phys. Rev. Lett.*, 107(24):240501, 2011.

[PSG+20] S. Puri et al. Bias-preserving gates with stabilized cat qubits. eng. Science Advances, 6(34):eaay5901, August 2020. doi: 10.1126/sciadv.aay5901.

[PSL13] G. A. Paz-Silva and D. A. Lidar. Optimally combining dynamical decoupling and quantum error correction. *Sci. Rep.*, 3(1), 2013.

[PSS+12] J. R. Prance et al. Single-shot measurement of triplet-singlet relaxation in a Si/SiGe double quantum dot. *Phys. Rev. Lett.*, 108(4):046808, 2012.

[PSV+12] S. R. Plissard et al. From insb nanowires to nanocubes: Looking for the sweet spot. *Nano Lett.*, 12(4):1794–1798, 2012, http://dx.doi.org/10.1021/nl203846g.

[PTD+12] J. J. Pla et al. A single-atom electron spin qubit in silicon. *Nature*, 489(7417):541–545, 2012.

[PTD+13] J. J. Pla et al. High-fidelity readout and control of a nuclear spin qubit in silicon. *Nature*, 496(7445):334–338, 2013.

[PTR+17] S. Peters, L. Tiemann, C. Reichl, S. F. t, W. Dietsche, and W. Wegscheider. Improvement of the transport properties of a high-mobility electron system by intentional parallel conduction. *Appl. Phys. Lett.*, 110(4):042106, 2017, http://dx.doi.org/10.1063/1.4975055.

[PvHK+21] Dmitry I Pikulin et al. Protocol toidentify a topological superconducting phase in a three-terminaldevice.arXiv preprint arXiv:2103.12217, 2021

[PvWC+13] S. R. Plissard et al. Formation and electronic properties of InSb nanocrosses. *Nat. Nanotechnol.*, 8(11):859–864, 2013.

[PWW+05] L. N. Pfeiffer, K. W. West, R. L. Willett, H. Akiyama, and L. P. Rokhinson. Nanostructures in gas fabricated by molecular beam epitaxy. *Bell Labs Tech. J.*, 10(3):151–159, 2005.

[PYB+24] T. Proctor, K. Young, A. D. Baczewski, and R. Blume-Kohout. Benchmarking quantum computers. July 11, 2024. arXiv: 2407. 08828 [quant-ph]. url: http://arxiv.org/abs/2407.08828. Pre-published.

[PZ03] J. Proos and C. Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Inf. Comput.*, 3(4):317–344, 2003.

[QE16] QUTE-Europe. Qt roadmap 2016, 2016, http://qurope.eu/h2020/qtflagship/roadm016.

[QL12] G. Quiroz and D. A. Lidar. High-fidelity adiabatic quantum computation via dynamical decoupling. *Phys. Rev. A*, 86(4):042333, 2012.

[RAB+22] C. Ryan-Anderson et al. Implementing fault-tolerant entangling gates on the five-qubit code and the color code. arXiv preprint arXiv:2208.01863, 2022.

[RAC+24] B. W. Reichardt et al. Demonstration of quantum computation and error correction with a tesseract code. September 6, 2024. arXiv: 2409.04628 [quant-ph]. url: http://arxiv.org/abs/ 2409.04628. Pre-published

[Rag24] S. Ragavan. Regev Factoring Beyond Fibonacci: Optimizing Prefactors, Cryptology ePrint Archive , Paper 2024/636, 2024.

[RB01] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, 2001.

[RBB03] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(2):022312, 2003.

[RBLD12] D. Ristè, C. C. Bultink, K. W. Lehnert, and L. DiCarlo. Feedback control of a solid-state qubit using high-fidelity projective measurement. *Phys. Rev. Lett.*, 109(24):240502, 2012.

[RBS+24] M. Ragone et al. A Lie algebraic theroy of barren plateaus for deep parameterized quantum circuits, *Nature Communications* 15, 7172, 2024.

[RCB+11] L. Robledo et al. High-fidelity projective read-out of a solid-state spin quantum register. *Nature*, 477(7366):574–578, 2011.

[RD15] D. Ristè and L. DiCarlo. Digital feedback in superconducting quantum circuits, 2015, arXiv:1508.01385.

[Reg24] O. Regev. An Efficient Quantum Factoring Algorithm,arXiv: 2308.06572, 2024.

[Rei20] B. W. Reichardt. Fault-tolerant quantum error correction for Steane's seven-qubit color code with few or no extra qubits. Quantum Science and Technology, 6(1):015007, 2020.

[Res16] M. Research. Language-integrated quantum operations: Liq*Ui*|⟩. https://www.microsoft.com/en-us/research/project/language-integrated-quantum-operations-liqui/, 2016.

[RFB+10] S. Rihani et al. Enhanced terahertz emission from a multilayered low temperature grown gaas structure. *Appl. Phys. Lett.*, 96(9):091101, 2010, http://dx.doi.org/10.1063/1.3332587.

[RGM+03] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy. Quantum computation with optical coherent states. *Phys. Rev. A*, 68(4):042319, 2003.

[RGP+12] C. Rigetti et al. Superconducting qubit in a waveguide cavity with a coherence time approaching 0.1 ms. *Phys. Rev. B*, 86(10):100506, 2012.

[RGL+24] D. Ruiz, J. Guillaud, A. Leverrier, M. Mirrahimi, and C. Vuillot. LDPC-cat codes for low-overhead quantum computing in 2D, February 2024.

[RGR+17] S. Rosenblum et al. A cnot gate between multiphoton qubits encoded in two cavities, 2017, arXiv:1709.05425.

[RH07] R. Raussendorf and J. Harrington. Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.*, 98(19):190504, 2007.

[RHG06] R. Raussendorf, J. Harrington, and K. Goyal. A fault-tolerant one-way quantum computer. *Ann. Phys.*, 321(9):2242–2270, 2006.

[RKB+16] A. Reiserer et al. Robust quantum-network memory using decoherence-protected subspaces of nuclear spins. *Phys. Rev. X*, 6(2):021040, 2016.

[RLB+14] S. Ravets, H. Labuhn, D. Barredo, L. Beguin, T. Lahaye, and A. Browaeys. Coherent dipole-dipole coupling between two single rydberg atoms at an electrically-tuned forster resonance. *Nat. Phys.*, 10(12):914–917, 2014.

[RLF12] L. P. Rokhinson, X. Liu, and J. K. Furdyna. The fractional a.c. josephson effect in a semiconductor–superconductor nanowire as a signature of majorana particles. *Nat. Phys.*, 8(11):795–799, 2012.

[RLL09] C. A. Ryan, M. Laforest, and R. Laflamme. Randomized benchmarking of single- and multi-qubit control in liquid-state nmr quantum information processing. *New J. Phys.*, 11(1):013034, 2009.

[RMBL08] C. A. Ryan, O. Moussa, J. Baugh, and R. Laflamme. Spin based heat engine: Demonstration of multiple rounds of algorithmic cooling. *Phys. Rev. Lett.*, 100(14):140501, 2008.

[RMR+07] K. D. Raedt, K. Michielsen, H. D. Raedt, B. Trieu, G. Arnold, M. Richter, T. Lippert, H. Watanabe, and N. Ito. Massively parallel quantum computer simulator. *Comput. Phys. Commun.*, 176(2):121 – 136, 2007.

[RNSL17c] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter. Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms. In Advances in Cryptology - ASIACRYPT 2017 (Part 2), Springer LNCS 10625, pp. 241-270, 2017.

[Roe17] M. Roetteler. (private email communication), October 2017.

[ROT+17] M. Reagor et al. Demonstration of universal parametric entangling gates on a multi-qubit lattice, 2017, arXiv:1706.06570.

[RS14] M. Roetteler and R. Steinwandt. A quantum circuit to find discrete logarithms on ordinary binary elliptic curves in depth O(log ^2n). *Quantum Inf. Comput.*, 14:888–900, 2014.

[RS15] M. Roetteler and R. Steinwandt. A note on quantum related-key attacks. *Inf. Process. Lett.*, 115(1):40–44, 2015.

[RS16a] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations, Quantum Information and Computation 16(11-12):901-953, 2016.
[RvLK+12] D. Ristè, J. G. van Leeuwen, H.-S. Ku, K. W. Lehnert, and L. DiCarlo. Initialization by measurement of a superconducting quantum bit circuit. *Phys. Rev. Lett.*, 109(5):050507, 2012.

[RV24] S. Ragavan and V. Vaikuntanathan. Space-Efficient and Noise-Robust Quantum Factoring, arXiv:2310.00899, 2024

[RWC+20] D. Rosenberg et al. Solid-state qubits: 3D Integration and Packaging. IEEE Microwave Magazine, 21(8):72–85, August 2020. issn:1557-9581.

[RWJ+14] T. F. Ronnow et al. Defining and detecting quantum speedup. *Science*, 345(6195):420–424, 2014.

[RWL+18] J. Randall, A. M. Lawrence, S. C. Webster, S. Weidt, N. V. Vitanov, and W. K. Hensinger. Generation of high-fidelity quantum control methods for multilevel systems. Phys. Rev. A 98(4):043414, 2018.

[RWN+17] M. Radulaski et al. Scalable quantum photonics with single color centers in silicon carbide. *Nano Lett.*, 17(3):1782–1786, 2017, http://dx.doi.org/10.1021/acs.nanolett.6b05102.

[Saf16] M. Saffman. Quantum computing with atomic qubits and Rydberg interactions: progress and challenges. *J. Phys. B: At., Mol. Opt. Phys.*, 49(20):202001, 2016.

[SBK+21] R. Srinivas et al. High-fidelity laser-free universal control of trapped ion qubits. Nature, 597(7875):209–213, 2021.

[SBM+11] P. Schindler et al. Experimental repetitive quantum error correction. *Science*, 332(6033):1059–1061, 2011.

[SBM+16] S. Sheldon et al. Characterizing errors on qubit operations via iterative randomized benchmarking. *Phys. Rev. A*, 93(1):012301, 2016.

[SBT+17] V. M. Schäfer et al. Fast quantum logic gates with trapped-ion qubits, 2017, arXiv:1709.06952.

[SCB+13] A. Stute, B. Casabone, B. Brandstatter, K. Friebe, T. Northup, and R. Blatt. Quantum-state transfer from an ion to a photon. *Nat. Photon.*, 7(3):219–222, 2013.

[Sch23] A. Schrottenloher. Quantum Linear Key-Recovery Attacks Using the QFT. In H. Handschuh and A. Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, pages 258*–291, Springer, 2023.

[SCQWG23] H.-W. Sun, B.-B. Cai, S.-J. Qin, Q.-Y. Wen, and F. Gao. Quantum Attacks on Beyond-Birthday-Bound MACs. Cryptology ePrint Archive, Paper 2023/025, 2023.

[SCS+16] I. Schwartz et al. Deterministic generation of a cluster state of entangled photons. *Science*, 354(6311):434–437, 2016, http://science.sciencemag.org/content/354/6311/434.full.pdf.

[SDEW13] R. Schutjens, F. A. Dagga, D. J. Egger, and F. K. Wilhelm. Single-qubit gates in frequency-crowded transmon systems. *Phys. Rev. A*, 88:052330, 2013.

[SDH+12] M. D. Shulman, O. E. Dial, S. P. Harvey, H. Bluhm, V. Umansky, and A. Yacoby. Demonstration of entanglement of electrostatically coupled singlet-triplet qubits. *Science*, 336(6078):202–205, 2012, http://science.sciencemag.org/content/336/6078/202.full.pdf.

[SDP+12] J. Stehlik, Y. Dovzhenko, J. R. Petta, J. R. Johansson, F. Nori, H. Lu, and A. C. Gossard. Landau-Zener-Stückelberg interferometry of a single electron charge qubit. *Phys. Rev. B*, 86(12):121303, 2012.

[Sei00] J.-P. Seifert. Using fewer qubits in Shor's Factorization Algorithm via Simultaneous Diophantine Approximation. Electronic Colloquium on Computational Complexity, Report 78, 2000.

[Sel16] P. Selinger. The Quipper Language. http://www.mathstat.dal.ca/~selinger/quipper/, 2016.

[SF24] H. Shi and X. Feng. Quantum Circuits of AES with a Low-depth Linear Layer and a New Structure. *Cryptology ePrint Archive*, Paper 2024/381 2024, https://eprint.iacr.org/2024/381.

[SFD+10] D. I. Schuster, A. Fragner, M. I. Dykman, S. A. Lyon, and R. J. Schoelkopf. Proposal for manipulating and detecting spin and orbital states of trapped electrons on helium using cavity quantum electrodynamics. *Phys. Rev. Lett.*, 105(4):040503, 2010.

[SFV+02] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto. Indistinguishable photons from a single-photon device. *Nature*, 419(6907):594–597, 2002.

[SGJ+13] M. J. Schwarz et al. Gradiometric flux qubits with a tunable gap. *New Journal of Physics*, 15(4):045001, 2013.

[SHD+13] X. Su, S. Hao, X. Deng, L. Ma, M. Wang, X. Jia, C. Xie, and K. Peng. Gate sequence for continuous variable one-way quantum computation. *Nat. Commun.*, 4:2828, 2013.

[SHK+08] J. A. Schreier et al. Suppressing charge noise decoherence in superconducting charge qubits. *Phys. Rev. B*, 77(18):180502, 2008.

[SHKW05] M. J. Storcz, U. Hartmann, S. Kohler, and F. K. Wilhelm. Intrinsic phonon decoherence and quantum gates in coupled lateral quantum-dot charge qubits. *Phys. Rev. B*, 72(23):235321, 2005.

[Sho94] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press, 1994.

[SHT18a] D. S. Steiger, T. Häner, and M. Troyer. ProjectQ: An Open Source Software Framework for Quantum Computing, Quantum 2, 49, 2018.

[Sho95] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493, 1995.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing*, 26(5):1484–1509, 1997.

[SJ09] R. Stock and D. F. V. James. Scalable, high-speed measurement-based quantum computer using trapped ions. *Phys. Rev. Lett.*, 102:170501, Apr 2009.

[SJD06] L. C. H. Simon J. Devitt, Austin G. Fowler. Robustness of Shor's algorithm. *Quant. Inf. Comp.*, 6:616–629, 2006.

[SJS23] G. Song, K. Jang, and H. Seo. Improved Low-Depth SHA3 Quantum Circuit for Fault-Tolerant Quantum Computers. *Applied Sciences* 13(6):3558, 2023.[SKD+10] M. Steffen et al. High-coherence hybrid superconducting qubit. *Phys. Rev. Lett.*, 105(10):100502, 2010.

[SKI+22] Y. Sunada et al. Fast readout and reset of a superconducting qubit coupled to a resonator with an intrinsic Purcell filter. *Physical Review Applied*, 17(4):044016, 2022.

[SKS+14] P. Scarlino et al. Spin-relaxation anisotropy in a gaas quantum dot. *Phys. Rev. Lett.*, 113:256802, Dec 2014.

[SL22] P. Stano and D. Loss. Review of performance metrics of spin qubits in gated semiconducting nanostructures. Nature Reviews Physics, 4(10):672-688, 2022.

[SLH+04] R. W. Simmonds et al. Decoherence in Josephson phase qubits from junction resonators. *Phys. Rev. Lett.*, 93(7):077003, 2004.

[SLTDS10] J. D. Sau, R. M. Lutchyn, S. Tewari, and S. Das Sarma. Generic new platform for topological quantum computation using semiconductor heterostructures. *Phys. Rev. Lett.*, 104(4):040502, 2010.

[SM00] A. Sørensen and K. Mølmer. Entanglement and quantum computation with ions in thermal motion. *Phys. Rev. A*, 62(2):022311, 2000.

[SM85] D. Strickland and G. Mourou. Compression of amplified chirped optical pulses. Optics communications, 55(6):447–449, 1985.

[SMCG16] S. Sheldon, E. Magesan, J. M. Chow, and J. M. Gambetta. Procedure for systematically tuning up cross-talk in the cross-resonance gate. *Phys. Rev. A*, 93(6):060302, 2016.

[Smi16] G. Smith. Private communication, 2016.

[SMS02] A. Shnirman, Y. Makhlin, and G. Schön. Noise and decoherence in quantum two-level systems. *Phys. Scr.*, 2002(T102):147, 2002.

[SMS+19] M. Soeken, F. Mozafari, B. Schmitt, G. De Micheli. Compiling permutations for superconducting QPUs. Design, Automation and Test in Europe (DATE) 2019, IEEE, preprint available at https://msoeken.github.io/papers/2019_date_4.pdf.

[SMSS06] J. Schriefl, Y. Makhlin, A. Shnirman, and G. Schön. Decoherence from ensembles of two-level fluctuators. *New J. Phys.*, 8(1):1, 2006.

[SNS+13] V. Srinivasa, K. C. Nowack, M. Shafiei, L. M. K. Vandersypen, and J. M. Taylor. Simultaneous spin-charge relaxation in double quantum dots. *Phys. Rev. Lett.*, 110(19):196803, 2013.

[Sol00] R. Solovay. Lie groups and quantum circuits, 2000, http://www.msri.org/publications/ln/msri/2000/qcomputing/solovay/1/.

[dSRABR+ 24] M. P. da Silva et al. Demonstration of logical qubits and repeated error correction with better-than-physical error rates. April 2024. arXiv:2404.02280.

[SRDR17] E. A. Sete, M. J. Reagor, N. Didier, and C. T. Rigetti. Charge- and flux-insensitive tunable superconducting qubit. *Phys. Rev. Applied*, 8(2):024004, 2017.

[SRW+14] R. C. Sterling et al. Fabrication and operation of a two-dimensional ion-trap lattice on a high-voltage microchip. *Nat. Commun.*, 5:3637, 2014.

[SS07] G. Smith and J. A. Smolin. Degenerate quantum codes for pauli channels. *Phys. Rev. Lett.*, 98(3):030501, 2007.

[SS10] G. Schaller and R. Schützhold. The role of symmetries in adiabatic quantum algorithms. *Quantum Inf. Comput.*, 10:0109–0140, 2010.

[SS17] T. Santoli and C. Schaffner. Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives. *Quantum Inf. Comput.*, 17(1&2):65–78, 2017.

[SSA+15] A. Srivastava et al. Optically active quantum dots in monolayer wse2. *Nat. Nanotechnol.*, 10(6):491–496, 2015.

[SSAG16] M. Smelyanskiy, N. P. D. Sawaya, and A. Aspuru-Guzik. qhipster: The quantum high performance software testing environment, 2016, arXiv:1601.07195.

[SSK+18] A. Stockklauser et al. Strong Coupling Cavity QED with Gate-Defined Double Quantum Dots Enabled by a High Impedance Resonator. *Phys. Rev. X, 7(1):011030, 2018.*

[SSD08] K. Steinberg, M, Scheffer, M. Dressel, Quasiparticle response of superconducting aluminium to electromagnetic radiation, *Phys. Rev. B,* 77, 214517 (2008)

[SSN+21] K.-N. Schymik et al. Single atoms with 6000-second trapping lifetimes in optical-tweezer arrays at cryogenic temperatures. Physical Review Applied, 16(3):034013, 2021.

[SSO19] Y. Subaşı, R. D. Somma, and D. Orsucci. Quantum Algorithms for Systems of Linear Equations Inspired by Adiabatic Quantum Computing, *Phys. Rev. Lett.* 122, 060504, 2019.

[SSO92] A. Suarez, R. Silbey, and I. Oppenheim. Memory effects in the relaxation of quantum open systems. *J. Chem. Phys.*, 97(7):5101–5107, 1992, http://dx.doi.org/10.1063/1.463831.

[SSX+22] I. Seidler et al. Conveyor-mode single-electron shuttling in si/sige for a scalable quantum computing architecture. npj Quantum Information, 8(1):100, 2022.

[Ste96] A. Steane. Multiple-particle interference and quantum error correction. *Proc. Royal Soc. A*, 452(1954):2551–2577, 1996.

[Ste03] A. Steane. Overhead and noise threshold of fault-tolerant quantum error correction. *Phys. Rev. A*, 68:042322, 2003.

[SVE+20] R. Stricker et al. Experimental deterministic correction of qubit loss. Nature, 585(7824):207–210, 2020.

[SVMA+17] A. Scherer et al. Concrete resource analysis of the quantum linear system algorithm used to compute the electromagnetic scattering cross section of a 2D target, Quantum Inf. Process. (2017) 16: 60. Preprint available at arXiv:1505.06552v2.

[SW03] M. J. Storcz and F. K. Wilhelm. Decoherence and gate performance of coupled solid-state qubits. *Phys. Rev. A*, 67(4):042319, 2003.

[SW23] E.M. Stoudenmire, X. Waintal. Grover's Algorithm Offers No Quantum Advantage, arXiv:2303.11317, 2023.

[SWM10] M. Saffman, T. G. Walker, and K. Mølmer. Quantum information with Rydberg atoms. *Rev. Mod. Phys.*, 82(3):2313–2363, 2010.

[SWS16] Y. R. Sanders, J. J. Wallman, and B. C. Sanders. Bounding quantum gate error rate based on reported average fidelity. *New J. Phys.*, 18(1):012002, 2016.

[SXZ+22] S. Shi et al. High-fidelity photonic quantum logic gate based on near-optimal Rydberg single-photon source. Nature Communications, 13(1):4454, 2022.

[SZH+16] H.-H. Sunet al. Majorana zero mode detected with spin selective andreev reflection in the vortex of a topological superconductor. *Phys. Rev. Lett.*, 116(25):257003, 2016.

[SZK+18] N. Samkharadze et al. Strong spin-photon coupling in silicon. Science 359:1123, 2018.

[SZW93] R. I. Shekhter, A. M. Zagoskin, and G. Wendin. Oxygen diffusion and dynamical disorder in high-t_c superconductors: low frequency noise in superconducting tunnel junctions. *Z. Phys. B*, 91(3):277–284, 1993.

[TAG+22] C. Taballioneet al. 20-mode universal quantum photonic processor. arXiv preprint arXiv:2203.01801, 2022

[TB05] B. M. Terhal and G. Burkard. Fault-tolerant quantum computation for local non-markovian noise. *Phys. Rev. A*, 71(1):012336, 2005.

[TBF18] D.K. Tuckett, S.D. Bartlett, and S.T. Flammia. Ultrahigh Error Threshold for Surface Codes with Biased Noise. *Phys. Rev. Lett.* 120(5):050505, 2018.

[TBJ+11] N. Timoney et al. Quantum gates and memory using microwave-dressed states. *Nature*, 476(7359):185–188, 2011.

[TCT+10] E. Togan et al. Quantum entanglement between an optical photon and a solid-state spin qubit. *Nature*, 466(7307):730–734, 2010.

[TDL+11] A. Tipsmark et al. Experimental demonstration of a hadamard gate for coherent state qubits. *Phys. Rev. A*, 84(5):050301, 2011.

[TdVR02] C. M. Tesch and R. de Vivie-Riedle. Quantum computation with vibrationally excited molecules. *Phys. Rev. Lett.*, 89(15):157901, 2002.

[TED+05] J. M. Taylor et al. Fault-tolerant architecture for quantum computation using electrically controlled semiconductor spins. *Nat. Phys.*, 1(3):177–183, 2005.

[TFSS23] J. Tindall, M. Fishman, M. Stoudenmire, and D. Sels. Efficient Tensor Network Simulation of IBM's Kicked Ising Experiment, 2023, arXiv:2306.14887.

[TGA+05] F. Troiani et al. Molecular engineering of antiferromagnetic rings for quantum computation. *Phys. Rev. Lett.*, 94(20):207208, 2005.

[THWZ16] A. Tayebi, T. N. Hoatson, J. Wang, and V. Zelevinsky. Environment-protected solid-state-based distributed charge qubit. *Phys. Rev. B*, 94(23):235150, 2016.

[TKL+04] F. Tafuri et al. Flavours of intrinsic D-Wave induced effects in $YBa_2Cu_3O_{7-\delta}$ grain boundary josephson junctions. *Supercond. Sci. Technol.*, 17(5):S202, 2004.

[TKO+16] K. Takeda et al. A fault-tolerant addressable spin qubit in a natural silicon quantum dot. *Sci. Adv.*, 2(8):e1600694–e1600694, 2016.

[TLA+11] J. D. Teufel et al. Circuit cavity electromechanics in the strong-coupling regime. *Nature*, 471(7337):204–208, 2011.

[TM96] K. Takeo and I. Masatoshi. Macroscopic quantum tunneling of a fluxon in a long josephson junction. *J. Phys. Soc. Jpn.*, 65(9):2963–2975, 1996.

[TMS+15] G. Tosi et al. Silicon quantum processor with robust long-distance qubit couplings, 2015, arXiv:1509.08538v2, https://arxiv.org/abs/1509.08538v2.

[TMW16] L. S. Theis, F. Motzoi, and F. K. Wilhelm. Simultaneous gates in frequency-crowded multilevel systems using fast, robust, analytic control shapes. *Phys. Rev. A*, 93(1):012324, 2016.

[TMWS16] L. S. Theis, F. Motzoi, F. K. Wilhelm, and M. Saffman. High-fidelity rydberg-blockade entangling gate using shaped, analytic pulses. *Phys. Rev. A*, 94:032306, Sep 2016.

[TNN+22] K. Takeda, A. Noiri, T. Nakajima, T. Kobayashi, and S. Tarucha. Quantum error correction with silicon spin qubits. Nature, 608(7924):682–686, August 2022.

[TNY+20] K. Takeda, A. Noiri, J. Yoneda, T. Nakajima, and S. Tarucha. Resonantly driven singlet-triplet spin qubit in silicon. Physical Review Letters,124(11):117701, 2020.

[TPLO+10] T. Takakura, et al. Triple quantum dot device designed for three spin qubits. *Applied Physics Letters*, 97(21):212104, 2010, https://doi.org/10.1063/1.3518919.

[TPM+24] S. J. S. Tan, C. A. Pattison, M. McEwen, and J. Preskill. Resilience of the surface code to error bursts. June 27, 2024.

[TSD+20] I. Tsioutsios et al. Free-standing silicon shadow masks for transmon qubit fabrication. AIP Advances, 10(6):065120, June 15, 2020.

[TvdWOT06] Y. Tokura, W. G. van der Wiel, T. Obata, and S. Tarucha. Coherent single electron spin control in a slanting zeeman field. *Phys. Rev. Lett.*, 96(4):047202, 2006.

[VAC+02] D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, and M. H. Devoret. Manipulating the quantum state of an electrical circuit. *Science*, 296(5569):886–889, 2002.

[VAVD+22] J. Verjauw et al. Path toward manufacturable superconducting qubits with relaxation times exceeding 0.1 ms, 2022.

[VAPS+15] W. Vinci, T. Albash, G. Paz-Silva, I. Hen, and D. A. Lidar. Quantum annealing correction with minor embedding. *Phys. Rev. A*, 92(4):042310, 2015.

[VBC+17] L. Vandersypen, H. Bluhm, J. Clarke, A. Dzurak, R. Ishihara, A. Morello, D. Reilly, L. Schreiber, and M. Veldhorst. Interfacing spin qubits in quantum dots and donors—hot, dense, and coherent. npj Quantum Information, 3(1):1–10, 2017.

[VBR08] M. Varnava, D. E. Browne, and T. Rudolph. How good must single photon sources and detectors be for efficient linear optical quantum computation? *Phys. Rev. Lett.*, 100(6):060502, 2008.

[VAW+19] C. Vuillot, H. Asasi, Y. Wang, L. P. Pryadko, and B. M. Terhal. Quantum error correction with the toric Gottesman-Kitaev-Preskill code. *Physical Review A*, 99(3):032344, 2019.

[VC76] R. F. Voss and J. Clarke. 1/f noise from systems in thermal equilibrium. *Phys. Rev. Lett.*, 36(1):42–45, 1976.

[VC05] L. Vandersypen and I. Chuang. NMR techniques for quantum control and computation. *Rev. Mod. Phys.*, 76(4):1037–1069, 2005.

[VD14] G. Viola and D. P. DiVincenzo. Hall effect gyrators and circulators. *Phys. Rev. X*, 4(2):021019, 2014.

[vDMV01] W. van Dam, M. Mosca, and U. Vazirani. How Powerful is Adiabatic Quantum Computation? In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pages 279–287, 2001.

[VF17] S. Vijay and L. Fu. Quantum error correction for complex and majorana fermion qubits, 2017, arXiv:1703.00459.

[Vio01] L. Viola. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293(5537):2059–2063, 2001.

[VKL99] L. Viola, E. Knill, and S. Lloyd. Dynamical decoupling of open quantum systems. *Phys. Rev. Lett.*, 82(12):2417–2421, 1999.

[vL10] P. van Loock. A note on quantum error correction with continuous variables. *J. Mod. Opt.*, 57(19):1965–1971, 2010, http://dx.doi.org/10.1080/09500340.2010.499047.

[vMM+08] R. van Meter, W. Munro, K. Nemoto, and K. M. Itoh. Arithmetic on a distributed-memory quantum multicomputer. ACM Journal on Emerging Technologies in Computing Systems (JETC), 3(4):1–23, 2008.

[vRLR+22] F. van Riggelen et al. Phase flip code with semiconductor spin qubits. npj Quantum Information, 8(1):1–7, October 27, 2022.

[VPK+16] R. Versluis et al. Scalable quantum circuit and control for a superconducting surface code, 2016, arXiv:1612.08208.

[VPS+14] U. Vool et al. Non-poissonian quantum jumps of a fluxonium qubit due to quasiparticle excitations. *Phys. Rev. Lett.*, 113(24):247001, 2014.

[VSB+01] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, 2001.

[vWGK15] D. J. van Woerkom, A. Geresdi, and L. P. Kouwenhoven. One minute parity lifetime of a nbtin cooper-pair transistor. *Nat. Phys.*, 11(7):547–550, 2015.

[vWPB+13] I. van Weperen, S. R. Plissard, E. P. A. M. Bakkers, S. M. Frolov, and L. P. Kouwenhoven. Quantized conductance in an insb nanowire. *Nano Lett.*, 13(2):387–391, 2013.

[VWvH+20] S. Vaitiekenas et al. Flux-induced topological superconductivity in full-shell nanowires. Science, 367(6485):eaav3392, 2020

[VYH+15] M. Veldhorst, C. H. Yang, J. C. C. Hwang, W. Huang, J. P. Dehollain, J. T. Muhonen, S. Simmons, A. Laucht, F. E. Hudson, K. M. Itoh, A. Morello, and A. S. Dzurak. A two-qubit logic gate in silicon. *Nature*, 526(7573):410–414, 2015.

[WAB15] F. H. E. Watson, H. Anwar, and D. E. Browne. Fast fault-tolerant decoder for qubit and qudit surface codes. *Phys. Rev. A*, 92(3):032309, 2015.

[WBE16] J. J. Wallman, M. Barnhill, and J. Emerson. Robust characterization of leakage errors. *New J. Phys.*, 18(4):043021, 2016.

[WBC+21] Y. Wu et al. Strong quantum computational advantage using a superconducting quantum processor. Physical review letters, 127(18):180501, 2021.

[WCJ22] P Wang, X. Chen, and G. Jiang. Quantum Demiric-Selcuk Meet-in-the-Middle Attacks on Reduced-Round AES. *International Journal of Theoretical Physics*, 61(1):1–12, 2022.

[Wei88] M. B. Weissman. 1/f noise and other slow, nonexponential kinetics in condensed matter. *Rev. Mod. Phys.*, 60(2):537–571, 1988.

[WEWH22] M. Webber, V. Elfving, S. Weidt, and W.K. Hensinger. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. *AVS Quantum Science* 4: 013801, 2022.

[WF14a] J. J. Wallman and S. T. Flammia. Randomized benchmarking with confidence. *New J. Phys.*, 16(10):103032, 2014.

[WF14b] A. C. Whiteside and A. G. Fowler. Upper bound for loss in practical topological-cluster-state quantum computing. *Phys. Rev. A*, 90(5):052316, 2014.

[WFH11] D. S. Wang, A. G. Fowler, and L. C. L. Hollenberg. Surface code quantum computing with error rates over 1, *Phys. Rev. A*, 83(2):020302, 2011.

[WG17] C. J. Wood and J. M. Gambetta. Quantification and characterization of leakage errors, 2017, arXiv:1704.03081.

[WHD+18] S. Welte, B. Hacker, S. Daiss, S. Ritter, and G. Rempe. Photon-Mediated Quantum Gate between Two Neutral Atoms in an Optical Cavity, *Phys. Rev. X 8(1):*011018, 2018.

[WHYW20] B. Wang, F. Hu, H. Yao, and C. Wang. Prime factorization algorithm based on parameter optimization of Ising model. *Scientific Reports*, 10(7106), 2020.

[Wil08] F. K. Wilhelm. Quantum oscillations in the spin-boson model: reduced visibility from non-markovian effects and initial entanglement. *New J. Phys.*, 10(11):115011, 2008.

[Wil09] F. Wilczek. Majorana returns. *Nat. Phys.*, 5(9):614–618, 2009.

[Wil13] R. L. Willett. The quantum hall effect at 5/2 filling factor. *Rep. Prog. Phys.*, 76(7):076501, 2013.

[WKG+17] T. Walter et al. Rapid high-fidelity single-shot dispersive readout of superconducting qubits. *Phys. Rev. Applied*, 7(5):054020, 2017.

[WKMS11] C. Weitenberg, S. Kuhr, K. Mølmer, and J. F. Sherson. Quantum computation architecture using optical tweezers. *Phys. Rev. A*, 84(3):032322, 2011.

[WKS+16] D. R. Ward et al. State-conditional coherent charge qubit oscillations in a si/sige quadruple quantum dot. *Nat. Partn. J. Quantum Inf.*, 2(1):16032, 2016.

[WKWW16] Y. Wang, A. Kumar, T.-Y. Wu, and D. S. Weiss. Single-qubit gates based on targeted phase shifts in a 3d neutral atom array. *Science*, 352(6293):1562–1565, 2016, http://science.sciencemag.org/content/352/6293/1562.full.pdf.

[WL95] P. A. Willems and K. G. Libbrecht. Creating long-lived neutral-atom traps in a cryogenic environment. *Phys. Rev. A*, 51(2):1403–1406, 1995.

[WL02] L.-A. Wu and D. A. Lidar. Qubits as parafermions. *J. Math. Phys.*, 43(9):4506–4525, 2002, http://dx.doi.org/10.1063/1.1499208.

[WL17] J. R. Wootton and D. Loss. A repetition code of 15 qubits, 2017, arXiv:1709.00990.

[WLL+03] A. Wallraff et al. Quantum dynamics of a single vortex. *Nature*, 425(6954):155–158, 2003.

[WM11] H. M. Wiseman, G. J. Milburn, Quatum Measurement and Control, Cambridge University Press, 2011

[WMJM17] J.D. Wong-Campos, S.A. Moses, K.G. Johnson, and C. Monroe. Demonstration of Two-Atom Entanglement with ultra-fast Optical Pulses. *Phys. Rev. Lett.,* 119(23):230501, 2017.

[WPGP+12] C. Weedbrook et al. Gaussian quantum information. *Rev. Mod. Phys.*, 84(2):621–669, 2012.

[WPK+18] T. Watson et al. A programmable
two-qubit quantum processor in silicon. Nature, 555(7698):633–637, 2018.

[WPJA+21] A. Wack et al. Quality, speed,and scale: three key attributes to measure the performance of near-term quantum computers. 2021, arXiv:2110.14108.

[WPK+17] T. F. Watson et al. A programmable two-qubit quantum processor in silicon, 2017, *Nature* 555(2):633-677, 2018.

[WRJ+23] A. J. Weinstein et al. Universal logic with encoded spin qubits in silicon. Nature, pages 1–3, 2023.

[Wro21] M. Wrónski. Index Calculus Method for Solving Elliptic Curve Discrete Logarithm Problem Using Quantum Annealing. In M. Paszynski, D. Kranzlmüller, V. V. Krzhizhanovskaya, J. J. Dongarra, and P. M. A. Sloot, editors, *Computational Science – ICCS 2021*, pages 149–155, Cham, 2021. Springer International Publishing.

[Wro22] M. Wrónski. Practical Solving of Discrete Logarithm Problem over Prime Fields Using Quantum Annealing. In D. Groen, C. de Mulatier, M. Paszynski, V. V. Krzhizhanovskaya, J. J. Dongarra, and P. M. A. Sloot, editors, *Computational Science – ICCS 2022*, pages 93–106, Cham, 2022. Springer International Publishing. Preprint available at Cryptology ePrint Archive, Paper 2021/527, https://eprint.iacr.org/2021/527.

[WRR+05] P. Walther et al. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, 2005.

[WRW+21] F. Wang et al. Experimental demonstration of a quantum controlled-swap gate with multiple degrees of freedom of a single photon. Quantum Science and Technology, 6(3):035005, 2021.

[WSHG06] F. K. Wilhelm, M. J. Storcz, U. Hartmann, and M. R. Geller. Superconducting qubits ii: Decoherence, 2006, arXiv:cond-mat/0603637.

[WSL+20] F. K. Wilhelm et al. Status of quantum computer development, Version 1.2. *Bundesamt für Sicherheit in der Informationstechnik*, 2020.

[WWL22] Z. Wang, S. Wei, and G. Long. A quantum circuit design of AES requiring fewer quantum qubits and gate operations. *Frontiers of Physics*, 17(41501), 2022.

[WWZ+14] G. Waldherr et al. Quantum error correction in a solid-state hybrid spin register. *Nature*, 506(7487):204–207, February 2014.

[WXG+22] K. Wang et al. Ultrafast coherent control of a hole spin qubit in a germanium quantum dot. Nature communications, 13(1):1–6, 2022.

[WZP18] L. Wossnig], Z. Zhao, and A. Prakash. *Quantum Linear System Algorithm for Dense Matrices.* Phys. Rev. Lett. 120 (5 2018), p. 050502, 2018.

[XHL+17] T. Xin et al. Nmrcloudq: A quantum cloud experience on a nuclear magnetic resonance quantum computer, 2017, arXiv:1710.03646.

[XJH+21] C. Xiang et al. High-performance silicon photonics using heterogeneous integration. IEEE Journal of Selected Topics in Quantum Electronics, 28(3: Hybrid Integration for Silicon Photonics):1–15, 2021.

[XLM+15] T. Xia et al. Randomized benchmarking of single-qubit gates in a 2d array of neutral-atom qubits. *Phys. Rev. Lett.*, 114(10):100503, 2015.

[XMC+20] Y. Xu et al. Demonstration of controlled-phase gates between two error-correctable photonic qubits. Phys. Rev. Lett., 124:120501, Mar 2020.

[XPvD+21] X. Xue et al. CMOS-based cryogenic control of silicon quantum circuits. Nature, 593(7858):205–210, 2021.

[XQLM22] L. Xiao, D. Qiu, L. Luo, and P. Mateus. Distributed shor's algorithm. arXiv preprint arXiv:2207.05976, 2022.

[XRS+22] X. Xue et al. Quantum logic with spin qubits crossing the surface code threshold. Nature, 601(7893):343–347, 2022.

[XSE+21] X. Xu, J. Sun, S. Endo, Y. Li, S. C. Benjamin, and X. Yuan. Variational algorithms for linear algebra. Science Bulletin, 66(21):2181–2188, 2021.

[XWH+18] X. Xue et al. Benchmarking Gate Fidelities in a Si/SiGe Two-Qubit Device. ArXiv:1811.04002.

[XXL+17] K. Xu et al. Experimental adiabatic quantum factorization under ambientconditions based on a solid-state single spin system. *Physical review letters*, 118(13):130504, 2017.

[YC10] P. Y. Yu and M. Cardona. *Fundamentals of Semiconductors*. Graduate Texts in Physics. Springer Berlin Heidelberg, 2010.

[YFK+16] G. Yang, A. Fragner, G. Koolstra, L. Ocola, D. A. Czaplewski, R. J. Schoelkopf, and D. I. Schuster. Coupling an ensemble of electrons on superfluid helium to a superconducting circuit. *Phys. Rev. X*, 6(1):011031, 2016.

[YGK+16] F. Yan et al. The flux qubit revisited to enhance coherence and reproducibility. *Nat. Commun.*, 7:12964 EP –, 2016.

[YHO+08] T. Yamamoto, K. Hayashi, Ş. K. Özdemir, M. Koashi, and N. Imoto. Robust photonic entanglement distribution by state-independent encoding onto decoherence-free subspace. *Nat. Photon.*, 2(8):488–491, 2008.

[YJG+12] N. Y. Yao et al. Scalable architecture for a room temperature solid-state quantum information processor. *Nat. Commun.*, 3:800 EP –, 2012.

[YSBK13] K. C. Young, M. Sarovar, and R. Blume-Kohout. Error suppression and error correction in adiabatic quantum computation: Techniques and challenges. *Phys. Rev. X*, 3(4), 2013.

[YSP14] A. J. Young, B. D. Schultz, and C. J. Palmstrøm. Lattice distortion in single crystal rare-earth arsenide/gaas nanocomposites. *Appl. Phys. Lett.*, 104(7):073114, 2014, http://dx.doi.org/10.1063/1.4865905.

[YTO+18] J. Yoneda et al. A quantum-dot spin qubit with coherence limited by charge noise and fidelity higher than 99.9%, *Nat. Nano.* 13(2):102-107, 2018.

[YTWJ+22] B. Yanet al. Factoring integers with sublinear resources on a superconducting quantum processor. arXiv:2212.12372v1 [quant-ph], 2022.

[YUvLF08] M. Yukawa, R. Ukai, P. van Loock, and A. Furusawa. Experimental generation of four-mode continuous-variable cluster states. *Phys. Rev. A*, 78(1):012301, 2008.

[YYK+16] J.-i. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa. Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing. *APL Photonics*, 1(6):060801, 2016.

[Zag97] A. M. Zagoskin. The half-periodic josephson effect in an s-wave superconductor - normal-metal - D-Wave superconductor junction. *J. Phys.: Condens. Matter*, 9(31):L419, 1997.

[Zal99] C. Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A*, pages 2746–2751, 1999.

[Zal08] C. Zalka. Shor's algorithm with fewer (pure) qubits. arXiv:quant-ph/0601097, 2008.

[ZB16] D. Zeuch and N. Bonesteel. Simple derivation of the Fong-Wandzura pulse sequence. Physical Review A, 93(1):010303, 2016.

[ZBD14] M. Zwerger, H. J. Briegel, and W. Dür. Hybrid architecture for encoded measurement-based quantum computation. *Sci. Rep.*, 4(1), 2014.

[ZHL+16] C. Zhang, Y.-F. Huang, B.-H. Liu, C.-F. Li, and G.-C. Guo. Experimental generation of a high-fidelity four-photon linear cluster state. *Phys. Rev. A*, 93(6):062329, Jun 2016.

[ZHM+16] D. M. Zajac, T. M. Hazard, X. Mi, E. Nielsen, and J. R. Petta. Scalable gate architecture for a one-dimensional array of semiconductor spin qubits. *Phys. Rev. Applied*, 6:054013, Nov 2016.

[ZJHR21] D. Zhu, T. Jaako, Q. He, and P. Rabl. Quantum computing with superconducting circuits in the picosecond regime. Phys. Rev. Applied, 16:014024, Jul 2021.

[ZLG+18] H. Zhang et al. Retracted article: Quantized majorana conductance. Nature, 556(7699):74–79, 2018.

[ZLG+21] H. Zhang et al. Retraction note: Quantized majorana conductance. Nature, 591(7851):E30–E30, 2021

[ZPH+17] J. Zhang et al. Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator, 2017, arXiv:1708.01044.

[ZPL+20] C. Zhang et al. Submicrosecond entangling gate between trapped ions via rydberg interaction. Nature, 580(7803):345–349, 2020.

[ZSBS14] J. Zhang, A. M. Souza, F. D. Brandao, and D. Suter. Protected quantum computing: Interleaving gate operations with dynamical decoupling sequences. *Phys. Rev. Lett.*, 112(5):050502, 2014.

[ZSR+18] D. M. Zajac et al. Resonantly driven CNOT gate for electron spins. Science, 359(6374):439–442, 2018.

[ZVSW03] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley. Geometric theory of nonlocal two-qubit operations. *Phys. Rev. A*, 67(4):042313, 2003.

[ZWD+20] H. Zhong et al. Quantum computational advantage using photons. Science,370(6523):1460–1463, 2020.

[ZWS+20] J. Zou, Z. Wei, S. Sun, X. Liu, and W. Wu. Quantum Circuit Implementations of AES with Fewer Qubits. In S. Moriai and H. Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 697–726, Cham, 2020. Springer International Publishing.