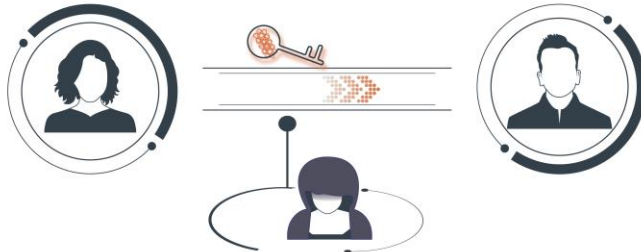


QKD INTEGRATION & EAVESDROPPING



IQBN



SQuaD
Schlüssel Quantenkommunikation Deutschland

Tackling Challenges in QKD Integration and Eavesdropping: Insights and Recommendations from the SQuaD Workshop

Quantum communication has the potential to play a pivotal role in securing critical infrastructure, transforming the way we send, store, and secure data. From a technological standpoint, it has achieved significant advancements but still encounters hurdles, particularly in integrating QKD systems to accelerate industry adoption. Additionally, in the context of deploying QKD systems, it is essential to address potential vulnerabilities and threats to ensure the robustness of the security framework.

This article delves into the rich discussions and findings of the recent SQuaD workshop organized by QBN, with the local hosts [QTI](#) and CNR-INO, which took place on February 28th, 2024, in the historic home of Galileo Galilei – Villa il Gioiello in Florence, Italy.

The insights and recommendations from the workshop will be further explored in upcoming SQuaD workshops and the QBN Working Group on Quantum Communications & Cybersecurity, ensuring continued progress and collaborative solutions in this critical area.

Integration Challenges

QKD: From Niche to Network – When discussing the protection of personal data, the focus is usually on the secure transmission and storage of this data. Currently, complex mathematical algorithms have efficiently fulfilled this protective function. However, with the advent of quantum computing, new solutions need to be explored, with QKD and PQC leading the way in efforts to establish a quantum safe network.

It is crucial to understand that a quantum-safe network does not necessarily rely on quantum technology for protection. Instead, it must safeguard against the potential threats

posed by quantum technologies. QKD has demonstrated its effectiveness and maturity through real implementations around the world, such as the China-quantum-network, QCI in Europe, and others, as well as through test links. The real challenge, however, arises in integrating this technology into existing infrastructures to develop a quantum-safe network that is:

- robust,
- scalable,
- cost-effective,
- flexible,
- operating without the need for trusted nodes.

As of now, only a few telecom operators have deployed QKD systems.



We need to encourage telecom operators to pilot QKD systems, supported by long-term government incentives.

Looking forward, fiber-based QKD systems are expected to be among the first to be deployed (indeed they are already deployed), with mobile and satellite-based systems following in a subsequent phase.

To foster a vital market and deliver value to end-users, it is essential to speed up standardization and certification efforts. Standardization will also allow smaller startups to remain competitive by focusing on their core expertise without worrying about interoperability with other systems or the need to develop the full stack.



Standardization and certification need to be pushed forward to create a vital market and common language.


Additionally, the broader adoption of QKD will benefit from services such as Quantum-as-a-Service and Entanglement-as-a-Service. These innovative offerings will lower the entry barrier for organizations looking to harness QKD, enabling them to experiment with QKD solutions without the substantial upfront investment. By providing access to quantum resources on-demand, these services have the potential to accelerate the development and deployment across various industries.

Eavesdropping and Security

Theoretically Secure, Practically to Be Confirmed – Although QKD is inherently secure according to the laws of physics and often described as unbreakable, this is a common misconception. As soon as the theory becomes technology, several backdoors can appear, and these vulnerabilities could negate the advantage. QKD systems are not unbreakable in an absolute sense but rather any eavesdropping attempt will disturb the transmitted quantum states which can be detected.

In practice, the implementation, including the physical devices, protocols, and key management, determines the level of security. When considering the overall security of

the system, it is also important to ensure that the supply chain is not compromised and that the classic system, including trusted nodes and computers, is secure.

 **Not all QKD systems offer the same level of security.**

To classify the attacks, we can divide the whole system into source, channel, and receiver. Figure 1 depicts prominent attacks and possible countermeasures.






	 Source	 Channel	 Receiver
 Attacker	<ul style="list-style-type: none"> • Trojan-horse attack • Laser seeding / Injection locking • Laser damage • Intersymbol interference • Induced photorefracton 	<ul style="list-style-type: none"> • Photon number splitting attack • Compromising calibration routines • QKD protocol without a full security proof • Denial of service • Intercept and resend 	<ul style="list-style-type: none"> • Detector control • Trojan-horse attack • Laser damage • Detector backflash • Induced photorefracton
 Countermeasures	<ul style="list-style-type: none"> • Decoy state • Optical isolation • Watchdog detectors • Active phase randomization • Passive transmitter • Continuous monitoring of the functionality of the implemented measures 	<ul style="list-style-type: none"> • Decoy state protocol • Calibration methods localized in detector (Bob) or source (Alice), four-state protocol • SDN-enabled QKD-Networks (Software Defined Network Applications for routing) • Photocurrent monitoring 	<ul style="list-style-type: none"> • Monitoring detector parameters / Statistical analyses • Optical isolation • Watchdog detectors • Semi-device independent solutions such as MDI, Twin field • Continuous monitoring of the functionality of the implemented measures

Figure 1: Attacks and countermeasures on source, channel, and receiver.

Although there is a good understanding of attacks and how to possibly prevent them, what is lacking is an official rating system and unified security proof. When defining an attack rating system, the following considerations need to be taken into account:

- Theoretical or practical risk.
 - Can it be exploited today, or does it need further technological development?
- What is the level of breach, e.g., what amount of the secret key material gets leaked?
- Required knowledge of the system.
- Cost of equipment to execute attack.
- Where did the attack happen?

 **We need an official rating system.**

 **We need a unified security proof.**

If you look at the long list of attacks, you may wonder how you are supposed to settle them all and how to develop systems that are intrinsically more secure. It is important to understand that not all countermeasures need to be implemented as some make others redundant.

 **Plan the implemented countermeasures well and prioritize them since some are more effective and prevent from multiple attacks.**

Furthermore, countermeasures can be categorized as those primarily preventing the attack and those primarily monitoring to detect and alert when an attack is happening. Based on the above list of attacks, we can categorize them as follows:

Countermeasures primarily for preventing attacks or rendering them ineffective:

- Optical isolation
- Active phase randomization
- Passive transmitter
- Semi-device independent solutions such as MDI, Twin field

Countermeasures primarily for monitoring and detecting attacks:

- Decoy state
- Monitoring detector parameters / Statistical analyses
- Watchdog detectors
- Continuous monitoring of the functionality of the implemented measures

Future Directions and Collaborative Efforts

The challenges of QKD integration and eavesdropping will be pivotal topics in future SQuaD workshops. These workshops will provide a platform for experts to delve deeper into specific issues such as developing robust countermeasures, advancing standardization efforts, and exploring innovative services like Quantum-as-a-Service.

Moreover, the QBN Working Group on Quantum Communications & Cybersecurity will take a systematic approach to address these challenges. The WG's mission is to spearhead the transition into the era of quantum-safe cybersecurity by fostering partnerships, promoting rigorous technical innovation, and guiding policy and standards both in Europe and globally. Regular meetings and collaborative projects within the QBN WG will ensure a continuous exchange of knowledge and innovative ideas, facilitating the development of more secure and scalable quantum communication networks.

By bringing together a diverse group of stakeholders, including industry leaders, academic researchers, and government representatives, these efforts aim to create a cohesive and comprehensive approach to overcoming the current hurdles in QKD implementation. This collaborative environment will foster the development of practical solutions and accelerate the adoption of QKD technologies across various sectors.

About SQuaD

The SQuaD project (Schirmprojekt Quantenkommunikation Deutschland) aims to accelerate the commercialization of Quantum Communication in Germany by bridging the gap between scientific research and industrial application. Funded by the Federal Ministry of Education and Research (BMBF), the project lifts synergies and brings together expertise of different stakeholders improving the infrastructure by testbeds, supporting standardization and certification, and enhancing Germany's competitive position in the global market.

QBN's Role in SQuaD

QBN plays a pivotal role in SQuaD and leads the project's efforts in networking, innovation promotion, and technology transfer. It develops methods, tools, and formats to foster innovation, supports entrepreneurs and SMEs in Quantum Communication, and connects stakeholders across industry, science, and politics to enhance collaboration and ecosystem development. This significantly contributes to the acceleration of Quantum Communication commercialization in Germany and Europe.

More on the SQuaD project and QBN's role in SQuaD: [Link](#)

Acknowledgement

We would like to express our sincere gratitude to the esteemed speakers of the Quantum Communication Workshop for their invaluable expertise and fruitful discussions, which contributed significantly to the formulation of the recommendations presented in this article. In particular, we would like to thank Mihaila Luminita (BSI), Nitin Jain (DTU, Alea Quantum Technologies), Davide Bacco ([QTI](#)), Tara Liebisch (PTB), and Vadim Makarov (VQCC) for their exceptional contributions.

Contact



Haissam Hanafi
Quantum Technology Manager
QBN

[Contact us.](#)