

Whitepaper

Quantum Key Distribution: Evolution and Perspectives

Authors: Mira Stephan, Dr. Rene Kirrbach

Introduction

The Q-Day, the day when quantum computers can break the encryption methods used today, is approaching. To protect against store-now-decrypt-later attacks, the transition to quantum-safe encryption must begin immediately. Quantum key distribution (QKD) is an approach for secure key distribution in the post-quantum age.

In contrast to post-quantum cryptography (PQC), which relies on hard-to-solve mathematical problems, QKD offers security based on the laws of quantum physics. QKD therefore offers true security.

PQC and QKD are no competing approaches. Rather, they address different layers of the quantum-safe security stack: PQC provides a software-based solution for broad deployment, while QKD can harden the most critical links by providing physics-based key establishment.

How QKD works

QKD enables two parties to establish a shared secret key in such a way that eavesdropping attempts become detectable. Put simply, QKD can be compared to a security seal. Anyone trying to intercept the transmission leaves traces behind. The reason is that measuring an unknown quantum state changes it. As a result, an attacker cannot observe the quantum transmission without disturbing it. QKD can be realized through different protocol families, most notably prepare-and-measure and entanglement-based schemes. In prepare-and-measure protocols, one party encodes information into quantum states of light, such as the polarization states of single photons, and transmits them to the other party through a quantum channel. In entanglement-based protocols, correlated keys are established from measurements on entangled photon pairs distributed between the communicating parties. Depending on the implementation, QKD may use discrete

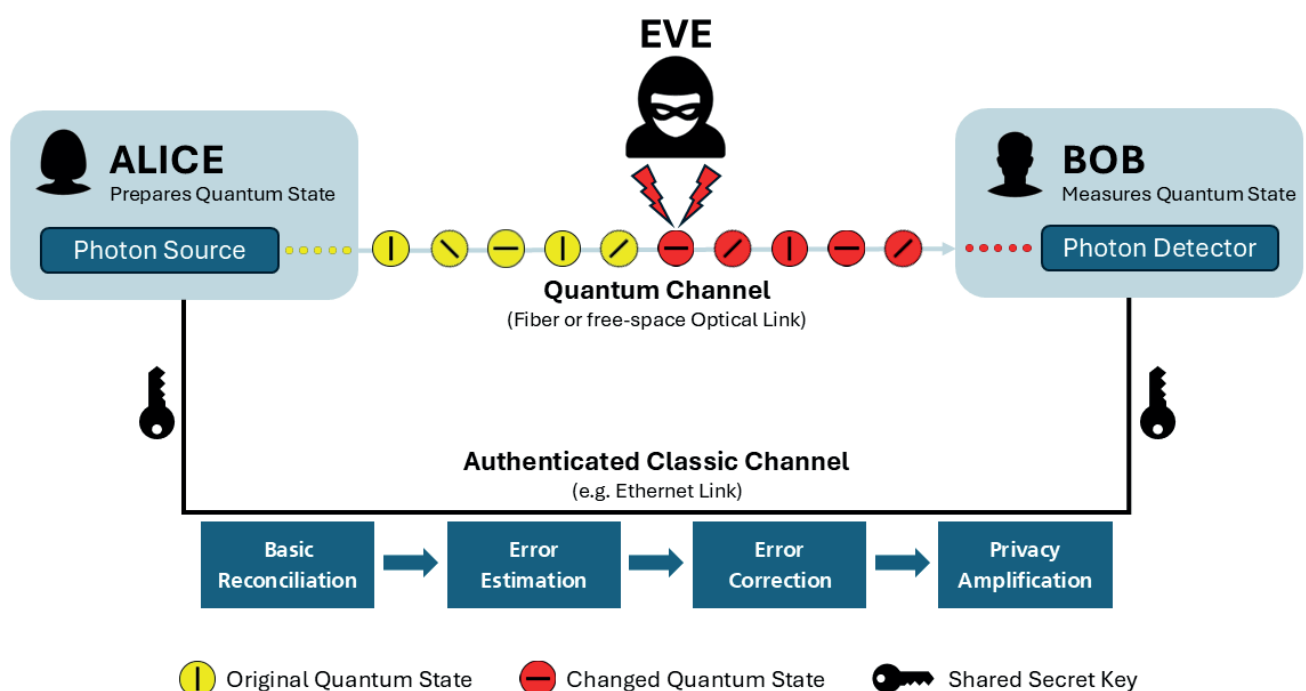


Figure 1. Basic principle of QKD: secure key establishment and eavesdropping detection through induced transmission errors.

variables, such as photon polarization, or continuous variables, such as the amplitude and phase quadratures of light. A schematic overview of this process is shown in Figure 1. Its security is derived from fundamental principles of quantum mechanics. Measuring an unknown quantum state disturbs it, and the no-cloning theorem prohibits perfect copying of unknown quantum states. As a consequence, any eavesdropping attempt introduces detectable disturbances in the transmission. In practical operation, the communicating parties monitor the error rate of the quantum exchange and discard compromised key material if the disturbance exceeds an acceptable threshold. The quantum channel itself is physically implemented over conventional transmission media, such as optical fiber or free-space optical links, while the exchanged key is subsequently used in classical cryptographic systems to encrypt user data.

QKD Development

From Idea to First Systems

Major milestones for QKD are shown in Figure 2. The idea of QKD traces back to Stephen Wiesner, whose work on “conjugate coding” was written in the early 1970s and eventually published in 1983 [1]. Shortly afterwards, in

1984, Charles H. Bennett and Gilles Brassard introduced the first explicit QKD protocol in their paper “Quantum cryptography: Public key distribution and coin tossing” [2], a scheme that later became known as BB84. Laboratory proof-of-concept demonstrations were realized shortly thereafter.

Since the earliest 32 cm experiment, major effort has gone into increasing the achievable distances and key rates of QKD systems. Fiber-based CV-QKD has been demonstrated over distances on the order of 100 km [3], while state-of-the-art discrete-variable implementations have reached several hundred kilometers in both fiber and free-space configurations. Commercialization started in the early 2000s. Since then, governmental and commercial QKD networks have been deployed, including a government QKD network in South Korea and the Quantum-Secure Metro Network for financial institutions in London, and China’s wide-area quantum communication network. A recent example is Singtel’s Quantum-Safe Network (QSN) [4], deployed in Singapore that offers QKD commercially as a managed service. These milestones mark the transition of QKD from laboratory experiments to operational systems. Most of today’s practical QKD products allow for maximum ranges of tens of kilometers to over 100 km depending on the secret key rate.

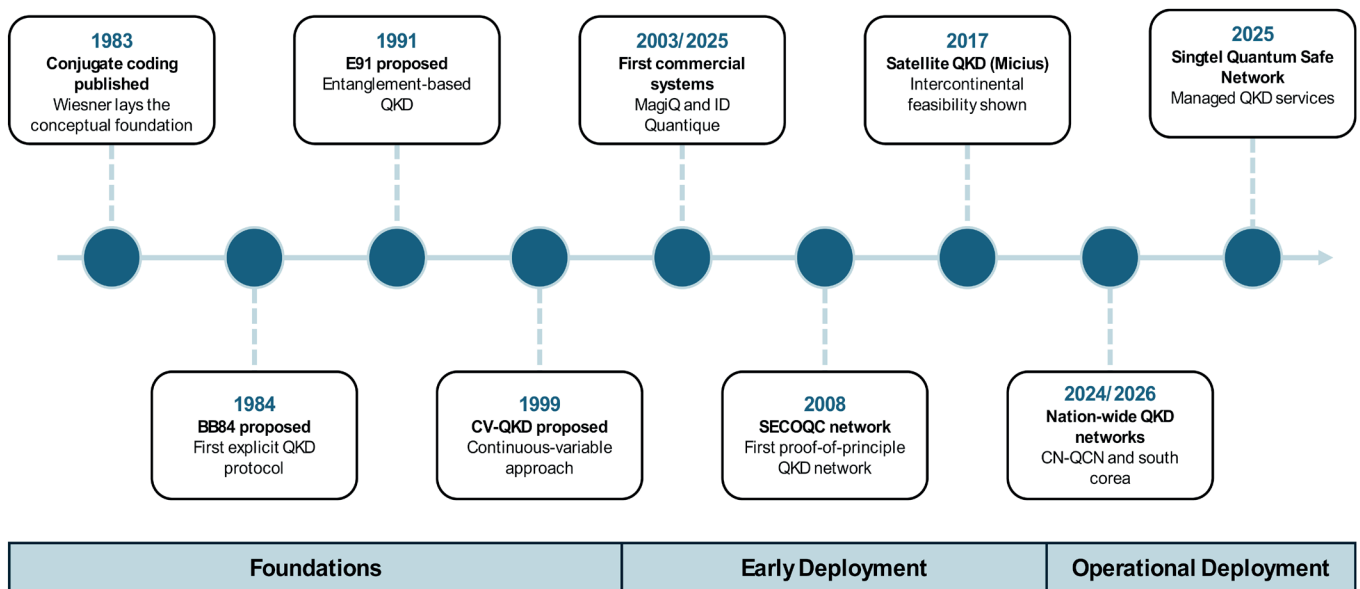


Figure 2. QKD Milestones.

Early Implementers and Emerging Markets for QKD

Building on these technological and commercial milestones, a first wave of QKD adopters has emerged. These early users are predominantly organizations operating in highly security-sensitive and regulated environments:

- **Government, defense, and critical infrastructure operators:** National security agencies, defense command networks, and operators of critical infrastructure are among the first users. Early QKD testbeds have been deployed for this group, demonstrating secure inter-governmental and inter-agency communication links.
- **Telecom operators and network providers:** Communication service providers are integrating QKD into their backbone and metro networks to offer quantum-secured connectivity as a premium service for large enterprise and public-sector customers.
- **Financial institutions:** Banks and other financial organizations are running pilot projects that use QKD to secure data-center interconnects, trading platforms, and transaction backbones, where confidentiality and integrity are business-critical.
- **Universities and research institutions:** Academic and research organizations deploy commercial QKD devices as experimental platforms for advancing quantum communication technologies and exploring new applications.

This combination of critical security needs and strong regulatory drivers makes these sectors natural first movers in QKD adoption.

As QKD technology matures and becomes standardized, its adoption is expected to broaden.

Likely later adopters include:

- **Cloud and data center operators,** securing high-value inter-data-center links and offering “quantum-secured” connectivity as part of their service portfolio.
- **IP-intensive industries** where protection of trade secrets and R&D data is critical.
- **Healthcare and public sector organizations,** driven by data-protection regulations and long-term confidentiality requirements.
- **Energy, transport, and industrial IoT operators,** protecting control networks, sensor backbones, and smart grid infrastructures.
- **Managed security service providers,** who will integrate QKD into turnkey security offerings for enterprises that cannot operate such systems themselves.

In these segments, QKD is expected to be adopted not as a stand-alone technology, but as part of broader, hybrid security architectures combining QKD with PQC and conventional key management systems.

Advantages of QKD

- **Security based on physics:** Robust even against future algorithmic breakthroughs.
- **Resilience against quantum computers:** QKD does not rely on mathematically hard problems that can be broken by quantum algorithms.
- **Intrinsic eavesdropper detection:** Any attempt to intercept the quantum signal disturbs it.
- **Information-theoretic key security:** Possible when combined with a one-time pad.
- **High key-refresh rates:** QKD systems can generate new keys continuously.
- **Complementary to PQC:** QKD can be used complementary to PQC and conventional encryption. QKD can harden the most critical links.

Disadvantages of QKD

- **Infrastructure and cost:** Requires specialized hardware; still not very widespread today.
- **Distance and key-rate limits:** Key rate decreases with distance and classical repeaters cannot be used.
- **Trusted intermediates:** Today's practical QKD networks rely on trusted nodes.
- **Implementation and side channel risks:** Security proofs assume ideal devices.
- **Need for classical authentication:** A quantum-safe authentication mechanism is required.

Technology	Security basis	Strength	Limitation	Role
Classical Cryptography	Mathematical hardness assumptions	Mature, universally deployed	Vulnerable to quantum computing QC	Standard but has to migrate (BSI recommendation 2032)
PQC	New mathematical problems believed to remain hard even for QC	Scalable, software-based	relies on assumptions & long-term confidence in new algorithms; some of today's devices are too slow	Primary and recommended quantum-safe path for standard systems
QKD	Laws of quantum physics	Detectable eavesdropping, strong long-term security	Specialized hardware, distance, cost and integration limits	Protection for the most critical links eventually complementary to PQC

QKD Implementation Concepts

In science, QKD-secured networks are often considered to provide end-to-end security between two trusted nodes, e.g. two computers. Each of the trusted nodes features a QKD device (Alice or Bob) that generate the keys by means of the quantum channel and an already existing classical channel. The generated keys are subsequently used by a certain application that runs within the trusted nodes. While this approach provides very high security, it requires access to the application and the possibility to import the QKD key into the encryption process. For users with common commercial third-party software this might not be an option and costly.

Another approach with lower implementation effort is the concept of the secure link: The QKD-devices not only feature the quantum channel, but also the classical link. The QKD devices can be seen as a switch with quantum channel for QKD. The switch uses for instance layer-2-encryption (MAC-Sec) to en- and decrypt all ingoing and outgoing data with the QKD key.

Generally, both implementation concepts allow the use of existing infrastructure: single-mode fibers for the quantum channels and wired- or unwired connections for the classical channel.

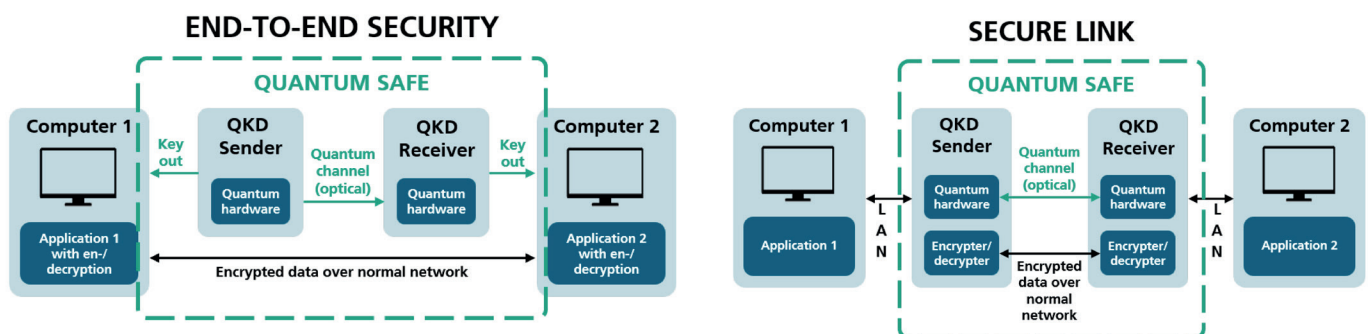


Figure 3. QKD-Implementation Concepts.

Outlook and future perspectives for QKD

Ongoing technological advances are expected to significantly improve the performance and practicality of QKD. Better photon sources, detectors and error-correction algorithms will enable higher key rates over longer distances. At the same time, substantial effort is going into implementing QKD on integrated photonic chips to reduce size, power consumption and cost, paving the way for large-scale deployment as well as mobile, field-deployable, and service-based QKD applications.

To overcome today's distance limitations, quantum repeaters are a central research topic. In the longer term, they are expected to enable end-to-end quantum-secured communication over very large distances. In addition, entanglement-based QKD schemes will support more flexible and larger-scale QKD networks. Twin-field QKD has also attracted particular attention because it significantly improves achievable distance scaling and has enabled record transmission distances in fiber-based experiments.

Standardization and certification are both current bottlenecks and key drivers for wider adoption. International bodies such as ETSI, ITU-T and ISO/IEC are developing standards for QKD frameworks, interfaces and security requirements. These standards are essential for later certification of QKD devices, which is a requirement for deployment in regulated environments. They will also ensure interoperability between devices from different vendors and thus enable the construction of large networks.

In future deployments, QKD is expected to be embedded into existing security and networking infrastructures rather than operated as a stand-alone system. QKD will provide fresh symmetric keys to existing key-management systems, for example to update AES-256 keys, rather than replace them outright. Telecom and cloud providers are likely to

offer quantum-secured services by integrating QKD into their backbones and data-center interconnects. Hybrid architectures, combining QKD with post-quantum cryptography and classical symmetric encryption, can be expected to become the norm for high-value links with long-term confidentiality requirements.

To reach the full potential of QKD, further progress is needed in several areas. Real-world implementations must be hardened against side-channel and implementation attacks, and certification schemes have to be developed that link theoretical security proofs to specific hardware. Research on measurement-device-independent and device-independent QKD aims to reduce trust assumptions on the underlying devices. Finally, continued cost reduction and operational simplification will be essential to make large-scale QKD networks economically viable.

Fraunhofer IPMS Activities

Over the last years, the Fraunhofer IPMS focused on the development of affordable QKD technologies to make QKD scalable and to bring it into a broad spectrum of applications [5,6]. Today, the IPMS offers QKD Evaluation Kits that enable an easy start. The Evaluation Kits are ideally suited for first proof of concepts and subsequently for widespread deployments.

With broad competencies in electronic design, software design, cryptography physics and practical experiences, the IPMS is the ideal partner for research and development activities and deployments in the field of QKD.

References

- [1] S. Wiesner, »Conjugate coding,« SIGACT News, vol. 15, no. 1, pp. 78–88, 1983, doi: 10.1145/1008908.1008920.
- [2] Charles H. Bennett and Gilles Brassard: "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9.12-12.12. 1984, pages: 175–179
- [3] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, »Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator,« Science advances, vol. 10, no. 1, eadi9474, 2024, doi: 10.1126/sciadv.adi9474.
- [4] Accessed: Sep. 21, 2026. [Online]. Available: <https://www.singtel.com/about-us/media-centre/news-releases/singtel-launches-southeast-asias-first-hybrid-quantum-safe-network-to-deliver-flexible-scalable-security-for-enterprises>
- [5] F. Klingmann, K. Dutta, M. Stephan, M. Haymann-Pohl, L. Reuschel, A. Noack, R. Kirrbach, J. Yang, Fei Ding., »A Low-Cost, Off-The-Shelf Quantum Key Distribution System with kbit/s Key Generation Rates,« in IEEE Transactions on Quantum Engineering, doi: 10.1109/TQE.2026.3733725.
- [6] M. Stephan, T. Schneider, F. Klingmann and R. Kirrbach, »A Modular Pointing and Tracking System for Terrestrial Quantum Key Distribution,« MikroSystemTechnik KONGRESS 2025; Mikroelektronik/Mikrosystemtechnik und ihre Anwendungen – Nachhaltigkeit und Technologiesouveränität, Duisburg, Germany, 2025, pp. 283-285, doi: 10.30420/456614133.



About Fraunhofer IPMS

The Fraunhofer-Gesellschaft, based in Germany, is the world's leading organization for application-oriented research. With its focus on future-relevant key technologies and the utilization of the results in business and industry, it plays a central role in the innovation process. As one of 76 institutes, Fraunhofer IPMS deals with electronic, mechanical and optical components and their integration into miniaturized devices and systems. Our services range from conception and product development to pilot production in our own laboratories and clean rooms.

Contact

Stephan Kube
B2B Sales Marketing Manager
+49 351 88 23 - 1112
stephan.kube@ipms.fraunhofer.de

Fraunhofer IPMS
Maria-Reiche-Straße 2
01109 Dresden, Germany
www.ipms.fraunhofer.de/en