Chapter 3
QKD

QKD (Quantum Key Distribution) promises information-theoretical security by using quantum states to generate shared cryptographic key material and to reveal eavesdropping attempts through unavoidable physical disturbances. The practical value of this promise depends not only on quantum technologies such as DV-QKD, CV-QKD, entanglement-based QKD, MDI-QKD, and Twin-Field QKD, but also on authentication, post-processing, implementation quality, and operational architecture. Fiber-optic, satellite, and free-space QKD each impose distinct limits on distance, key rate, trusted nodes, costs, and resistance to side-channel attacks.

3.1 What is QKD?

QKD [WP–QKD][1] is a communication method that allows Alice and Bob to generate a shared cryptographic key that can later be used by both parties for symmetric encryption methods. A significant part of the communication takes place via a quantum channel whose physical characteristics can only be described by the theories of quantum physics.

QKD offers perfect information-theoretical security under the following conditions:

- There is a classical accompanying channel (e.g., a normal Internet connection). All QKD methods and protocols assume that Eve can completely eavesdrop on or read everything that happens on this classical accompanying channel. Everything sent via this channel is therefore considered public knowledge.
- Alice and Bob authenticate each other on this classical channel by adding a MAC (Message Authentication Code) [WP–MAC][2] to each message.

[1] https://en.wikipedia.org/wiki/Quantum_key_distribution.

[2] https://en.wikipedia.org/wiki/Message_authentication_code.

E. Piller and H. Schölnast, *Data Encryption at the Intersection of Mathematics and Physics*, SpringerBriefs in Information Security and Cryptography,
https://doi.org/10.1007/978-3-032-24764-3_3

- The devices used by Alice and Bob are optimally configured and perfectly secured against classic eavesdropping attacks such as side-channel attacks.

It is expressly not a requirement that Eve be prevented from eavesdropping on the quantum channel in addition to the classical channel.

Perfect information-theoretical security specifically means that Eve, who is eavesdropping on both the quantum channel and the classical channel, has no way of extracting useful information about the key that Alice and Bob are currently trying to generate on both sides from the intercepted data. This circumstance is often referred to as "eavesdropping security of quantum communication." However, this term does not mean that eavesdropping is impossible, but rather that Eve can eavesdrop on both channels without being able to derive any benefit from what she intercepts. The reason for this is not any special mathematical procedures, but rather the physical nature of the quantum channel used.

In this consideration, the entire mathematical processing (see Chap. 8) required to generate a final cryptographic key is ignored or assumed to be perfectly secure, and possible side-channel attacks are also disregarded (see Chap. 3.8). This means that the security of QKD requires a much more comprehensive consideration than presented above and is usually undertaken in scientific QKD publications or manufacturer presentations.

3.1.1 Eavesdropping on the Classical Side Channel

Alice and Bob consider the classical side channel to be public and do not concern themselves with whether anyone is eavesdropping on the data traffic on this channel. Alice and Bob do not even know if anyone is eavesdropping on this classical side channel. They do not care.

3.1.2 Eavesdropping on the Quantum Channel

The quantum channel is designed in such a way that any attempt to eavesdrop on it will result in the falsification of a large proportion of the transmitted information units (bits [WP–Bit][3] or qubits [WP–Qbit][4]). This falsification is purely random and, due to the laws of physics, cannot be prevented or actively influenced by Eve. Alice and Bob use mathematical and statistical methods to detect these distortions retrospectively and then respond in such a way that Eve cannot obtain any useful information about the key from what she may have picked up on the quantum channel.

[3] https://en.wikipedia.org/wiki/Bit.

[4] https://en.wikipedia.org/wiki/Qubit.

More specifically, if Eve eavesdrops on the quantum channel and thereby obtains information that could potentially be useful to her, she will inevitably be noticed by Alice and Bob. Based on the extent of the perceived interference, the two can estimate the maximum amount of data traffic Eve could have intercepted. Alice and Bob then use appropriate mathematical methods to reduce the length of the shared key, with the result that Eve cannot gain any useful information about the key from what she has learned. The more information Eve intercepts on the quantum channel, the shorter becomes the key generated by Alice and Bob. If Eve exceeds a certain amount of intercepted information, Alice and Bob terminate the key exchange altogether. This means that Eve is effectively carrying out a denial-of-service attack, but in most cases she could do this more easily and cheaply by simply cutting the transmission medium (very often a fiber optic cable, see Chap. 3.4). Apart from that, the damage to Alice and Bob is minor, because the two were not trying to transmit important or urgent information, but only wanted to replenish their shared key stock. So the two have time to find the physical location where Eve carried out her eavesdropping attack. They then secure this location and repeat the key exchange.

3.1.3 Quantum Physics Paradigms

The special type of eavesdropping security offered by the quantum channel is based on physical principles that can only be described by quantum physics theories. In particular, these are the following quantum physics paradigms:

- **Measurement disturbance principle**: Every measurement of a quantum state changes this state with a high degree of probability [WP–MQM].[5]
- **No-cloning theorem**: Unknown quantum states cannot be duplicated. [WP–NCT].[6]
- **Monogamy of entanglement**: Maximum entanglement is only possible between two particles. It is possible to extend entanglement to three or more particles, but then there is no completely shared information between all particles. If you measure the state of one particle in a three-particle entanglement, you do not obtain complete knowledge about the states of the other two particles [WP–QEnt].[7]
- **Superposition**: Quantum states can consist of superpositions of several basis states [WP–QSup].[8]
- **Uncertainty principle**: Complementary observables cannot exist simultaneously with arbitrary precision, but are subject to a fundamental common uncertainty (indeterminacy) that is distributed unevenly between the two observables. This

[5] https://en.wikipedia.org/wiki/Measurement_in_quantum_mechanics.

[6] https://en.wikipedia.org/wiki/No-cloning_theorem.

[7] https://en.wikipedia.org/wiki/Quantum_entanglement.

[8] https://en.wikipedia.org/wiki/Quantum_superposition.

makes it impossible to measure both observables exactly at the same time. Location and momentum, or energy and time, are often cited as such observable pairs, but in the case of QKD, it is the pair of amplitude and phase of an electromagnetic wave that is always subject to such a common uncertainty [WP–Unc].[9]

In addition, there are QKD methods that are currently in the experimental stage or that exist only as ideas on paper, some of which are based on lesser-known paradigms. For the sake of completeness, these methods are briefly mentioned below, but they have not yet reached a level of maturity that would allow them to be used in security-critical applications.

3.2 How Does QKD Work?

3.2.1 Two Communication Channels

As already mentioned, QKD always uses two communication channels:

1. There is a quantum channel through which quantum states are transmitted. Who generates these states, who sends them, and who receives them varies depending on the type of QKD method. What all QKD methods have in common is that eavesdropping on a transmission of quantum states via a quantum channel leads to an increased quantum bit error rate (QBER) due to the measurement disturbance principle, which Alice and Bob can use to detect that the quantum channel is being eavesdropped on. However, a low error rate always occurs even without an actual eavesdropping attempt. Regardless of the true cause, it is always formally attributed to Eve. Correction procedures ensure that Eve cannot use the intercepted information. If the error rate exceeds a certain threshold, the procedure is aborted.

   In all existing QKD procedures, photons are used as carriers of the quantum states. This means that light (or another electromagnetic wave) is sent from a transmitter to a receiver. There are attempts to transfer the quantum states of photons to matter particles (e.g., individual atoms or electrons), for example, to store them there or to transfer them back to another photon in a quantum repeater [QRep],[10] but these technologies are still in the experimental stage and currently have a high error rate.
2. In addition, a classical communication channel is always required for the legitimate communication partners to exchange meta-information. This classical communication is necessary to enable the communication partners to interpret their secretly performed quantum measurements in agreement with the other party. In addition, information is transmitted via this channel that is later used

[9] https://en.wikipedia.org/wiki/Uncertainty_principle.

[10] https://qt.eu/quantum-principles/communication/quantum-repeaters.

for error correction. Nothing transmitted via the classical channel is secret. It is therefore permissible for a potential attacker to read this classical information in its entirety.

3.2.2 Authentication

However, it is of crucial importance that Alice and Bob authenticate each other. Without strict authentication, man-in-the-middle attacks are possible, in which the legitimate communication partners do not actually generate secret keys with the supposed counterpart, but with an unknown third party (with *Mallory,* see Sect. 2.7.2). This mutual authentication is no different from authentication in many other communication protocols, so it will only be discussed very briefly here.

Wegman-Carter authentication [Weg81][11] is commonly used. Alice and Bob must already have a shared secret key before the key exchange process begins (from a previous key exchange, which may have been performed by means other than QKD). From this key, the sender obtains a small subkey for each message packet it sends, which it uses to add a Message Authentication Code (MAC) to the packet before sending it to the recipient via the public channel. The recipient receives the message packet and, in the same way as the sender, has derived the same subkey from the shared key, which it uses to calculate a MAC from the message in the same way. The recipient only accepts the received packet if the MAC it has calculated itself matches the MAC that the sender sent with the message.

Since fresh random bits are used for MAC generation for each transmitted packet (which may not be reused afterwards) and because only Alice and Bob know the secret key, it is guaranteed that Alice and Bob only accept data packets that have actually been authenticated by the other party. Without knowledge of the secret key, a third party cannot manipulate the data traffic on the public channel unnoticed, nor can they impersonate the other party to Alice or Bob.

In practice, this authentication requires an initial key at the beginning, which must have been distributed securely, but once common key material has been generated through ongoing key exchange, a small portion of this fresh key pool is used for authentication. All implementations of key exchange protocols ensure that this happens automatically and that the bit sequences used for ongoing mutual authentication are not added to those bit sequences that are issued as key material.

Although authentication technically only affects the classical side channel, it also indirectly protects the quantum channel from targeted manipulation attempts. No separate authentication is required on the quantum channel itself, as manipulation there would only be useful if it were coordinated with the message traffic on the classical side channel, which is impossible due to the authentication of this channel.

The quantum channel can still be manipulated, but without simultaneous manipulation of the classical accompanying channel, this inevitably leads to an increased

[11] https://doi.org/10.1016/0022-0000(81)90033-7.

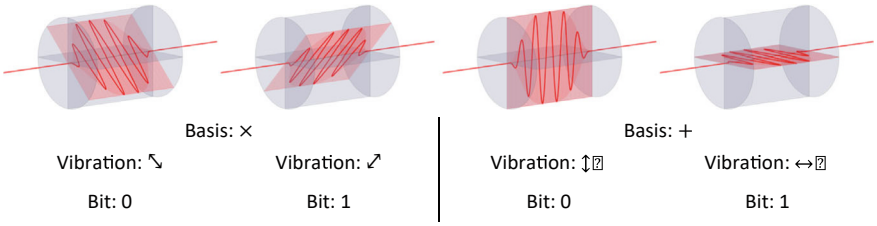

Fig. 3.1 The four oscillation planes in the BB84 protocol

quantum error rate. This reduces the actual key rate generated or even leads to a termination, but in both cases, Eve does not obtain a usable key material.

3.2.3 General Procedure

It starts with someone using a suitable device to generate random quantum information and then sending this information. This quantum information is measured at the receiver after transmission.

This applies to both prepare-and-measure methods and methods using entangled photons. In prepare-and-measure, one of the two key exchange parties generates the quantum information (usually Alice, but in exotic QKD technologies it can also be Bob). When entangled photons are used, there is a third party in addition to the two key exchange parties, namely the source, which neither Alice nor Bob need to trust. This source generates the quantum information and sends it. Both Alice and Bob are the recipients.

However, there are also QKD technologies, such as MDI-QKD (see Chap. 3.3.5), in which both Alice and Bob generate and send quantum information. In this case, the recipient is a third party that neither Alice nor Bob need to trust.

Measurement Bases (Using the BB84 Protocol as an Example)

Measurement bases play a fundamental role in the transmission and reception of quantum information, which will be explained here in brief using the example of the BB84 QKD protocol. (A detailed description of the BB84 protocol can be found together with descriptions of several other protocols on the book's website at.[12])

The BB84 protocol uses linearly polarized photons, and the quantum information is encoded as the direction of oscillation of each individual photon, as shown in Fig. 3.1.

The photon moves along the central red line. At right angles to this is the direction along which the photon oscillates. In the BB84 protocol, this oscillation direction can have the four orientations shown in Fig. 3.1. Two directions that are at right angles to each other form a measurement basis. (⤡ and ⤢ together form the basis ×; ↕

[12] https://cryptography.study/phys/protocol.

and ↔ form the basis +.) The two directions of a basis are interpreted as opposite bit values. This allows both possible bit values to be encoded in both bases.

An example: Alice wants to send Bob the bit value 0 and chooses the measurement basis × for this purpose. (The measurement basis is chosen randomly for each photon beforehand.) Alice therefore imprints the direction ↖↘ on the photon. This photon is now the carrier of a quantum bit, or "qubit" for short. The special thing about this quantum bit is that it only corresponds to the value of a classical bit in the measurement basis ×, because it only has the bit value 0 chosen by Alice in this specific measurement basis. In the other measurement basis (the measurement basis +), the bit value of the photon is a quantum physical superposition of the two bit values 0 and 1, each with a weighting of exactly 50%. In other words, the bit value of this photon is completely indeterminate in the measurement basis +.

Bob does not know the measurement basis used by Alice at the time of his measurement and therefore has to guess. (Bob only finds out which basis Alice used after he has measured the photon.) If Bob uses the correct basis × for his measurement, he will (almost) always obtain the correct direction ↖↘ and (almost) never the wrong direction as the measurement result, because in the basis × the photon has a clearly defined bit value. (Possible rare measurement errors are discussed in more detail below.) So, if Bob uses the correct measurement basis, he will most likely obtain the correct bit value (in the example: 0).

However, if Bob measures this photon in the wrong measurement basis, i.e., in the basis +, then he will obtain the result ↕ (which he interprets as 0) with a probability of 50% and the result ↔ (which he interprets as 1) with a probability of 50%. This is not because his apparatus would only output these two measurement results, but because the qubit carried by the photon is a superposition of the two possible values 0 and 1 in the wrong measurement basis.

In this case, Bob receives a completely random result. He would also measure the values 0 and 1 with a 50:50 probability if Alice had encoded the value 1 as ↗↙.

This means that a matching measurement basis means that both Alice and Bob have the same bit value. (Apart from rare measurement errors, see below.) Different measurement bases, on the other hand, mean that neither Alice nor Bob knows which bit value the other side has generated or measured.

Of course, Bob wants to know which of his measurements were correct and which were random, and Alice also wants to know which of the bits she sent were measured correctly by Bob and which were not. Therefore, Alice and Bob exchange their measurement bases via the public channel, but only after the quantum measurements have already been completed, i.e., when the photons transmitted in the process no longer exist. This curtain is called *sifting* and is described in more detail below.

The security of the protocol is based on the fact that Eve has to guess the measurement basis just as blindly as Bob. However, in order to deceive Bob (and indirectly Alice as well), Eve must send Bob a new photon instead of the measured (and thereby destroyed) one. But Eve not only does not know which basis Alice used, she also does not know which basis Bob will choose when the photon that Eve sends to Bob as a replacement for the measured one arrives. Therefore, Eve is bound to be wrong about

the measurement basis in 50% of all cases, which leads to incorrect measurement results for Bob, driving up the quantum error rate. Alice and Bob respond to this increased error rate by making the information Eve has received completely useless to her in the end. This response involves Alice and Bob first performing error correction and then a second processing step called *privacy amplification*. Both processes are described in Chap. 8.

But even if Eve did not destroy the photon during the measurement, but instead forwarded the same photon to Bob after the measurement, it would be of no use to her because the measurement changes the state of the measured photon. This is a fundamentally unavoidable consequence of the measurement disturbance principle.

Preparation, General (All Protocols)

Whether Alice, Bob, or perhaps even an unreliable or untrustworthy source generates and sends the quantum information, and who the recipient is, varies from protocol to protocol. In the BB84 protocol just presented, Alice sends the quantum information and Bob receives it. But in some protocols that work with entangled photons, even an external source that does not have to be trusted is allowed to send the quantum information, and there are even protocols in which unreliable relays measure the quantum information.

In any case, randomness plays an important role in both the creation and measurement of these transmitted states, because ultimately it is precisely this randomness that determines the bit sequence that represents the finished shared key. Therefore, the source of randomness plays a very decisive role in the security of the respective QKD protocol (see https://cryptography.study/phys/TRNG).

In each protocol, Alice and Bob generate bit sequences that they keep secret. However, other bit sequences are also generated, which are sent to the partner via the classical channel from Alice and Bob (sometimes even from an unreliable third party). These public bit sequences are used to decide what to do with the secret bit sequences.

Sifting

This comparison of the secret bit sequence with the help of public bit sequences is called “sifting”. In the first step of the sifting process, Bob sends Alice a list of timestamps or time indices. In all processes, short time slots are defined in advance, which, depending on the process, have a length of a few micro- or nanoseconds. Each second is thus divided into several million time slots. For this reason, it is also important that Alice and Bob synchronize their clocks very precisely with each other. Bob tells Alice in which of these time slots he has measured anything at all. In procedures where Alice is also the recipient, Alice also sends such a list to Bob. Once this has been done, Alice and Bob know which bits from their own secret bit sequence they must discard because there is no matching bit on the other side.

In the second step of sifting, Bob sends the list of the measurement bases he has randomly selected to Alice, and Alice also sends her corresponding list to Bob. In doing so, the two only transmit the data from those time slots that remain after the first step. By comparing the measurement bases, Alice and Bob determine in which

time slots they happened to use measurement bases that match each other. They then discard all bits that belong to incompatible measurement bases and retain only those bits from the original sequence of measurements that belong to time slots with compatible measurement bases.

Eve can follow all of this. Eve learns in which time slots there were simultaneous measurements, and she learns in which time slots Alice and Bob are highly likely to have obtained identical measurement results. But after sifting, Eve has no information about the measurement results themselves, because Alice and Bob have not yet revealed anything about the measurement results at this point. Eve only knows how many raw bits Alice and Bob have accumulated.

Error Correction

Quantum states are very fragile and can be easily disturbed, which leads to transmission errors even without the activities of an eavesdropping attacker. Calibrating the devices used before the actual key exchange, which is usually done automatically by the devices, helps against some sources of error, but the effects of some other sources of error cannot be mitigated so easily.

The list of possible sources of error is long, and a complete enumeration would defeat the purpose of this book. Nevertheless, the most important sources of error should be briefly mentioned:

- Normal bending of fiber optics causes polarization and/or phase drift along the fiber. In extreme cases, fiber optics hanging from masts and exposed to wind movement can cause such a high calibration effort due to these drift errors that there is no free time available for the actual key exchange. However, temperature fluctuations, vibrations, and many other influences also cause errors of this type.
- Another common source of error is a time offset in the delimitation of time slots (clock offset and jitter).
- During transmission through the air (direct line of sight, but also connection to a satellite), scattered light (e.g., sunlight) causes errors. In addition, atmospheric influences (rain, fog, dust) can significantly increase signal attenuation in these transmission paths, which is not an error in the true sense, but greatly reduces the key rate because it leads to many non-measurements.
- The measuring devices themselves are also a significant source of errors. Depending on the method/technology, they must be capable of measuring individual photons, or at least very weak light pulses. This can sometimes lead to dark counts (a measurement result is triggered even though no photon has reached the detector) and the overlooking of existing photons.

Because of these and other errors, even without anyone eavesdropping on the quantum channel, after sifting, Alice and Bob usually end up with two bit sequences that match in most places, but not in all. To correct these errors, it is necessary for the two communication partners to perform error correction. The details of this procedure are described in Sect. 8.2

After error correction has been performed, Alice and Bob have identical bit sequences that they could actually already use as keys for symmetric cryptographic procedures.

Privacy Amplification

Due to the data traffic between Alice and Bob required for error correction, which takes place via the public channel, the eavesdropper Eve gains access to information that she could, at least theoretically, use to her advantage. Although Eve cannot reconstruct individual bits of the exchanged key using the intercepted data, she can at least rule out some possible bit sequences as key candidates. To deprive her of this advantage, privacy amplification is performed. This involves mixing and shortening the bit sequences that were created after error correction. The exact procedures are described in Sect. 8.3.

Result (Key Rate)

The more quantum bits Eve intercepts, the more errors she causes in the raw keys. Each error (whether caused by Eve or due to other unavoidable causes) shortens the length of the resulting key in privacy amplification, which is reflected in a reduced secure key rate. This is the number of bits that are generated within a specified period of time (e.g., within one second) and that can actually be used in a symmetric key. It should also be noted that communication via the public channel consumes an approximately constant portion of the generated key material due to the necessary MAC authentication of all data packets.

Even if an attacker intercepts only a sufficiently large fraction of the quantum bits, this can ultimately lead to a situation where, after privacy amplification and after some bits have been reserved for MAC authentication, there are no bits left for a shared key. In practice, however, most protocols terminate earlier, namely when the quantum error rate exceeds a certain threshold or when the key rate falls below a certain lower limit. If this is the case, the attacker has successfully carried out a denial-of-service (DOS) attack, but they could have achieved the same result more cost-effectively by cutting the fiber optic cable, blocking the light beam, turning off the power, or using other simpler methods.

Furthermore, legitimate communication partners do not suffer any major damage as a result of a DOS attack. They can try again at a later point in time to perform a physical key exchange.

3.3 Technology Classes

As already mentioned, there are a variety of different QKD procedures that can be grouped into technology classes based on certain characteristics. The most important of these are briefly presented here.

3.3.1 Prepare & Measure (P&M)

Prepare-and-Measure methods [WP–P&M][13] are the classic basic form of quantum key distribution. Alice generates individual quantum states, typically photons with specific polarizations, intensities, or quadratures, and sends them to the receiver (Bob). Bob measures each of the states immediately upon arrival. Security arises from the fact that each measurement irreversibly changes the quantum state: any attempt at eavesdropping leads to measurable errors. P&M methods also include a classical channel through which Alice and Bob exchange their measurement bases, error rates, and other parameters.

Within P&M, a further distinction is made between DV (Discrete Variable) and CV (Continuous Variable) (see below: Sects. 3.3.2 and 3.3.3). The best-known DV P&M protocol is BB84, and the best-known CV P&M protocol is GG02. P&M is suitable for systems with low complexity, is technologically easy to master, and forms the basis of many commercial QKD products.

3.3.2 DV-QKD

DV stands for "Discrete Variable" [QSNP–DV].[14] Discrete variables refer to physical quantities that can be counted on the basis of specific and indivisible observations, in contrast to the continuous variables (CV) discussed below, which can take any value within a certain range. DV-QKD uses discrete properties of individual photons, such as polarization, time slot, or phase. The receiver measures each photon in a specific basis and obtains discrete values ("0" or "1"). The most commonly used DV-QKD protocol is BB84. Security is based on the impossibility of copying unknown quantum states and on high error rates during eavesdropping. DV-QKD requires single-photon detectors[15] with high sensitivity, low dark rate, and often cryogenic cooling. DV-QKD is well researched, widely used worldwide, and suitable for longer distances (e.g., over longer fiber optic links or satellite). However, it is more cost-intensive and complex than CV-QKD, especially in the detection area. On the other hand, DV is currently the most standardized QKD technology.

Maturity

The technology readiness level (TRL [WP–TRL][16]) of P&M + Discrete Variable can be rated at the highest level, 9. There are several commercial providers of this technology (e.g., IDQ, Toshiba, and others), and this technology is running in projects with metro networks in continuous operation.

---

[13] https://en.wikipedia.org/wiki/Quantum_key_distribution#Quantum_key_exchange.

[14] https://qsnp.eu/glossary/dv-qkd/.

[15] See https://cryptography.study/phys/QKD-HW.

[16] https://en.wikipedia.org/wiki/Technology_readiness_level.

Key Rates Fiber Optics

In laboratory operations under optimal conditions, key rates of around 10 Mbit/s have already been achieved, but such rates cannot be reproduced in field tests. These values are more realistic [Sas11][17]:

up to approx. 50 km: 1–10 kbit/s

up to approx. 200 km: 50 bit/s and below

Key rates for satellite (Micius) [Liao17a][18]

approx. 12 kbit/s at a distance of approx. 645 km

approx. 1 kbit/s at a distance of approx. 1200 km

3.3.3 CV-QKD

CV stands for "continuous variable" [QSNP–CV],[19] [Zha24].[20] CV-QKD uses continuous properties of light, such as the amplitude and phase (quadratures) of an optical carrier. Instead of single-photon detectors, "standard" telecommunications components are used: lasers, modulators, and fast homodyne or heterodyne detectors. The measured values are continuous numbers that are later digitized. CV-QKD is more cost-effective and easier to integrate into existing telecom DWDM networks. The methods are based on Gaussian states (e.g., GG02). The additional challenge lies in the more complex information processing, the higher sensitivity to optical noise, and the more demanding modeling of security proofs. CV-QKD is particularly suitable for urban networks, short to medium distances, and multi-channel coexistence with data traffic.

3.3.4 Entanglement-Based QKD

Entanglement [QSNP–Ent],[21] [WP–QEnt][22] refers to a non-classical correlation phenomenon in which two or more quantum systems are connected in such a way that their properties cannot be described independently of each other. The state of an entangled pair of particles is completely defined, while the values of the individual particles in the pair remain indeterminate until a measurement is made. In

[17] https://doi.org/10.1364/OE.19.010387.

[18] https://doi.org/10.1038/nature23655.

[19] https://qsnp.eu/glossary/cv-qkd/.

[20] https://doi.org/10.1063/5.0179566.

[21] https://qsnp.eu/glossary/entanglement/.

[22] https://en.wikipedia.org/wiki/Quantum_entanglement.

QKD, entangled photons are used to create strong, eavesdropping-proof correlations between the parties. An eavesdropping attacker cannot copy or disrupt entangled states without being noticed. Systems based on entanglement offer particularly high security guarantees. Entanglement is more technically demanding, but offers the most robust theoretical security basis of all QKD approaches.

Entanglement-based QKD methods/technologies use entangled photon pairs instead of prepared states. A central source generates photon pairs that are distributed to Alice and Bob. Both measure their photons independently of each other. The correlations arise solely from quantum entanglement and not from classical preparation. Security is verified using so-called Bell tests [QSNP–Bell],[23] [WP–Bell][24]: Only if the measured non-locality violations are high enough can no eavesdropper possess consistent information. Entanglement-based QKD requires precise sources, extremely stable channels, and highly efficient detectors, but offers a particularly strong theoretical security basis in return. It is also the basis for device-independent QKD and future quantum repeater networks.

3.3.5 MDI Measurement-Device-Independent

MDI-QKD [QSNP–MDI][25] eliminates the biggest point of attack in classical QKD systems: the detectors. In MDI-QKD, both parties send their quantized light signals to an untrusted relay station that only performs Bell measurements. Since detection no longer takes place at the legitimate communication partners, all detector side channels are excluded. The station can even be completely controlled by an attacker without compromising security. MDI-QKD offers very high security, but is technically more complex: it requires interfering signals from both transmitters and high stability of optical paths. MDI-QKD is considered one of the most secure architectures that can be implemented and is a step toward device-independent QKD.

3.3.6 Twin Field

Twin-Field QKD [Ars25][26] is an approach developed in 2018 that dramatically increases the range of QKD. Two remote parties send attenuated coherent light fields to an intermediate station, which causes the fields to interfere. The intermediate station does not need to be trustworthy, as no key materials are present there. The method scales with the square root of attenuation, enabling distances of over 500 km in fiber optics. This is significantly more than classic DV or CV methods/

[23] https://qsnp.eu/glossary/bell-state-measurement/.
[24] https://en.wikipedia.org/wiki/Bell_test.
[25] https://qsnp.eu/glossary/measurement-di-qkd/.
[26] https://doi.org/10.48550/arXiv.2510.26320.

technologies. Twin-Field is a type of MDI-like architecture, but combines the advantages of interference techniques with reduced detector requirements. Technically, the most difficult part is the precise synchronization of photon coherence over long distances.

Twin-Field is an experimental QKD method/technology that can significantly increase the range without trusted nodes. Two remote endpoints send coherent light pulses to a central measuring station. Security is maintained even if this station is untrusted, as the crucial information lies in the interfering fields. With TF-QKD, ranges of over 500 km in fiber optics appear quite realistic without the station in the middle having access to the key.

DI-QKD (Device-Independent QKD)

Device-Independent QKD [QSNP–DI][27] is the most stringent and theoretically secure form of quantum key distribution. Security does not depend on the correct functioning of the devices. Instead, eavesdropping security is guaranteed by the proof of quantum mechanical non-locality (Bell inequalities). As long as the measured violation is sufficiently large, the system remains secure. Even if devices are manipulated, faulty, or built entirely by the attacker. However, DI-QKD requires extremely efficient sources and detectors, low losses, and high-precision entanglement over long distances. Practical DI-QKD systems are still in the early stages of development, but are considered the ideal form of QKD to strive for.

3.4 Fiber Optic QKD

The transmission of quantum information through fiber optics is the most mature and commonly used method of operating QKD.

3.4.1 Rule of Thumb for Attenuation and Distance

In fiber optic QKD, key rates do not actually depend directly on the length of the fiber, but on the attenuation that occurs as the light travels through the fiber. However, since all common single-mode fibers are very similar in terms of attenuation, it is possible to convert between distance and attenuation using a constant factor of 0.2 dB/km or 5 km/dB, as shown in Table 1.1.

It should be noted that ultra-low-loss fibers with lower attenuation per kilometer (less than 0.16 dB/km) are available, but in most cases they are more expensive and often cannot be bent as much. In addition, glass fibers are usually supplied by the manufacturer in lengths between 2 and 4 km and must be joined together by splicing during installation, which leads to additional attenuation at these points. With optimal

[27] https://qsnp.eu/glossary/di-qkd/.

Table 1.1 Rule of thumb for attenuation and distance

Attenuation	Distance
0.2 dB	1 km
1.0 dB	5 km

execution, this amounts to 0.02–0.05 dB per splice, but with poor execution it can be considerably more. Added to this is attenuation that can occur due to minor damage to the fiber, e.g., small kinks that can happen during installation. However, this additional attenuation, which is to be expected, is already taken into account in the distance rule of thumb.

What Does "attenuation" Mean Specifically for QKD?

"Attenuation" is a term that can be easily understood intuitively if one thinks of light flux as something whose intensity can be continuously varied. Light enters a medium on one side with an initial intensity I_0 and exits on the other side with a lower final intensity I. The attenuation factor is then simply $d = \frac{I_0}{I}$.

For QKD, however, in the case of CV-QKD, extremely weak light pulses are used, which contain very few photons per pulse (typically less than 10 photons per pulse), or even only a single photon per pulse, which is the norm for DV-QKD and for methods/technologies with entangled photons.

So, what does "attenuation" mean in this context? Or rather, what is the intensity of light? It is the average number of photons per unit of time. This is because a photon has a constant energy due to its wavelength, which cannot decrease. However, a photon can disappear on its way from the beginning to the end of the fiber optic cable, e.g., through absorption or other effects. Attenuation therefore means that some photons that enter the fiber do not come out at the other end because they disappear in between.

An example: 1000 pulses, each with one photon, are fed into a glass fiber at one end, but after about 50 km, 900 of these pulses are empty and only 100 pulses still contain a photon. The attenuation factor is then $d = \frac{1000}{100} = 0.1$, or 10%, which corresponds exactly to 10 dB. (Decibel is a logarithmic measure. If 10% arrives, that is exactly 10 dB by definition. 1% corresponds to 20 dB and 0.1% is 30 dB. Halving the intensity, i.e., an attenuation factor of 50%, corresponds to approximately 3 dB.)

Security Theory Treatment of Attenuation

It should be mentioned at this point that attenuation is a completely normal and, in practice, unavoidable aspect of the movement of photons through a medium, as are small disturbances in the quantum properties of these photons (e.g., rotation of the polarization direction by a small angle). In the security theory analysis of these processes, however, it is always assumed that all transmission media have completely ideal properties. This includes the assumption that they cause no attenuation and no changes in quantum properties. Instead, the security theory analysis always assumes that an eavesdropping attacker, i.e., Eve, is the cause of all these effects. So, we act as if Eve were able to secretly replace all real components with ideal components

in order to divert and evaluate photons unnoticed. Therefore, in error correction and privacy amplification, all disruptive effects (including attenuation) are treated as if Eve were the sole cause.

3.4.2 QKD Fiber Optic Networks

When talking about quantum key distribution (QKD) in the context of fiber optics, in practice we are almost always talking about two things at once: firstly, real physical transmission links (typically telecom fibers, sometimes as dark fiber or as WDM coexistence with classic traffic), and secondly, a network and operating architecture that turns comparatively short QKD links into a widely available service that delivers the key material to applications. This second level, consisting of key management, interfaces, monitoring, operation, robustness against errors, and automatic route selection, has a greater impact on the practical value of QKD than spectacular laboratory values for individual links. This is precisely why QKD networks are particularly revealing as real infrastructure: they show where QKD crosses the threshold from a feasibility demonstration to practical operation.

In field networks, the factors that determine quality are less in pure quantum advantages and more in the classic operating metrics: stability over weeks and months, availability, average secret key rate (SKR), key transfer over multiple hops, and integration into crypto and network components via standardized interfaces (e.g., ETSI APIs).

Another key point is the assumption of trust: all fiber optic QKD networks found during research for this book are implemented as trusted node networks. This means that the key material is processed and recombined in plain text at intermediate nodes, because this is currently the only option that scales well over long distances. This circumstance raises the question of whether a network can be operated "productively" in terms of critical security requirements, and with what organizational protective measures.

Networks that do not require trusted nodes because they can teleport entangled states over long distances with the aid of quantum repeaters are already being tested, proving their basic feasibility [Luo25],[28] but they do not yet enable meaningful key exchange and are still a long way from being ready for use in real security-critical applications. (A single source reports that the system ran for 275 seconds in one day, generating approximately one bit per second as a raw key, which is very little to create a secure key from it [Koz19].[29] All other sources reporting on such experiments contain no references to key rates.)

The following is a list of the most important existing QKD networks and network infrastructures, sorted by region, with a focus on fiber-optic QKD, but also mentioning free-space and satellite links if they are integrated into the network.

---

[28] https://doi.org/10.48550/arXiv.2504.05660.

[29] https://doi.org/10.1145/3345312.3345497.

China

China appears to be the most influential region for fiber-optic-based QKD networks at present. This became apparent early on with the Beijing–Shanghai Backbone Network, whose construction began in 2013. The backbone route was completed in 2017 with around 2032 km and 32 trusted nodes [Chen25].[30] This backbone infrastructure was explicitly presented in public communications as a national demonstration and application route [CAS17].[31] The technical literature also emphasizes that the backbone and the connected metro networks were used as a platform for application testing (including in the finance and insurance sectors) [Zha18].[32]

The next step was to integrate terrestrial fiber-optic QKD with satellite and free-space QKD. A Nature publication [Chen21][33] describes an integrated network that connects a geographically extensive fiber optic QKD infrastructure with two satellite-based free-space QKD links, demonstrating QKD between more than 150 endpoints over a combined distance of 4600 km. Here, too, the architecture remains essentially trusted-node-based.

In a publication from August 2025 [Chen25],[34] the China Quantum Communication Network (CN-QCN) is described as an operational, trusted-relay-based network that spans 10,000 km, comprises 145 backbone fiber optic nodes and 20 metro networks, and covers 17 provinces and 80 cities. The article explicitly emphasizes operation and maintenance as well as hybrid networking of different QKD types as progress over pure verification networks. It is also interesting to note that, in the same context, the integration of ground stations for the Jinan-1 quantum microsatellite (see Chap. 3.5.2) is already mentioned as a supplement to the terrestrial base.

China is thus most clearly demonstrating the transition from field testing to a permanently operated infrastructure, albeit under the central prerequisite of a trusted node security model. For productive security-critical applications, this is only plausible if the nodes are understood to be highly secure operational locations. However, this architecture does not guarantee end-to-end security and requires additional trust assumptions.

EU testbeds and EuroQCI

At present, the central European goal is not a large EU-wide network, but rather many distributed testbeds with a focus on interoperability and use cases. The EU project OPENQKD (since 2019) [EC24][35] is designed precisely for this purpose: open testbeds are intended to demonstrate network functionality and use cases to stakeholders. In parallel, the EU is pursuing the establishment of a Europe-wide quantum

[30] https://doi.org/10.1038/s41534-025-01089-8.

[31] https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml.

[32] https://doi.org/10.1364/OE.26.024260.

[33] https://doi.org/10.1038/s41586-020-03093-8.

[34] https://doi.org/10.1038/s41534-025-01089-8.

[35] https://cordis.europa.eu/project/id/857156.

communication infrastructure with EuroQCI, initially with a strong terrestrial focus [EC25].[36]

Austria

Europe recognized QKD networks as a networking problem (interoperability, routing, key management, multi-vendor integration) at a very early stage. The most visible early example is the SECOQC network in Vienna (2004–2008). This was an EU project with a trusted node-based prototype network that was operational in Vienna in 2008 and was publicly demonstrated, including one-time pad telephony and a video conference secured by QKD keys across multiple nodes [Peev09].[37] This network was a technology and architecture demonstrator: it showed how heterogeneous QKD devices can be orchestrated in a network.

More recently, Austria has been visible primarily in the EuroQCI context through the national deployment project QCI-CAT, which, as Austria's contribution to the European EuroQCI infrastructure, aims to establish a QKD demonstration and testing environment for highly secure communication (especially for public authorities) [AIT26].[38] The project ran from January 2023 to June 2025. In terms of content, the project aimed to set up and test an Austria-wide quantum communication network infrastructure and to evaluate specific security applications such as secret sharing and message authentication. At the same time, QCI-CAT was integrated into the European network (including via PETRUS cross-domain demonstrations).

Switzerland

SwissQuantum was a classic reference network for long-term field operation in Switzerland: it was installed in the Geneva area and ran from the end of March 2009 to the beginning of January 2011 with a key management layer and real-world use via an application layer. The focus was on long-term stability, maintainability, and integration [Stu11].[39]

A special case that is often cited in discussions as evidence of productive use is the use of QKD to protect data transmissions in the context of elections in the canton of Geneva (2007) [OPT07].[40] The manufacturers of the QKD devices used present their use as recurring (in particular as protection for the transmission of election/counting data between locations) [IDQ17].[41]

---

[36] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

[37] https://doi.org/10.1088/1367-2630/11/7/075001.

[38] https://www.ait.ac.at/themen/cyber-security/projects/qci-cat.

[39] https://doi.org/10.1088/1367-2630/13/12/123001.

[40] https://optics.org/article/31646.

[41] https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/.

Spain

One of the most important European case studies for "real-world integration" is the MadQCI project (Madrid Quantum Communications Infrastructure; from 2021 to 2024). The central added value here was not primarily in record key rates, but in the embedding in a real, multi-tenant telecom environment: the network was built with disaggregated components, SDN paradigms, and multi-vendor QKD systems in a real telecom infrastructure, shares infrastructure with commercial traffic, and was tested over a period of approximately three years, with most nodes continuously active [Mar24].[42]

Benelux

A recent European highlight is the cross-border QKD connection between Belgium and Luxembourg as part of BeQCI/LUQCIA, which was communicated as a 132 km link and the first cross-border MDI QKD connection in the region [BEL25].[43] In this project, many weaknesses of real-world QKD implementations were tested by selecting and comparing different methods/technology architectures. This is an important step toward more robust security assumptions, even though overall operation still requires network and site-side trust models.

Germany

Germany is currently positioning QKD networks strongly as a research and testing infrastructure for government agencies and KRITIS scenarios. The QuNET initiative, for example, describes a field experiment that aims to connect multiple users in the Berlin area over 125 km of fiber plus supplementary free-space connections in a quantum-secure manner, with participating locations including Fraunhofer HHI, Deutsche Telekom, and the Bundesdruckerei [QUN24].[44] This project is one of many examples that show that in Europe, QKD networks are increasingly being conceived as hybrid systems in which fiber optic connections dominate but are supplemented by free-space links and satellite links.

Japan

Japan has built one of the best-known metro networks with the Tokyo QKD Network. It was launched in October 2010 and demonstrated as an operational network in the Greater Tokyo Area [NICT11].[45] A publication on the field test describes a mesh network with various QKD systems and cites as a prominent demonstration the world's first secure TV conference over a distance of 45 km [Sas11].[46] Later

[42] https://doi.org/10.1038/s41534-024-00873-2.

[43] https://www.belnet.be/en/news-events/news/new-milestone-quantum-communication-project-beqci-first-cross-border-qkd-network.

[44] https://qunet-initiative.de/en/news-2024/#:~:text=Start%20of%20the%20second%20key.

[45] https://www.nict.go.jp/en/pdf/copy_of_NICT_NEWS_1102_E.pdf.

[46] https://doi.org/10.1364/OE.19.010387.

reviews also highlight that the network was used as a platform for sectoral verifications, including in collaboration with players from the financial sector to assess its practicability [Stan22].[47]

South Korea

South Korea is often cited as the country that, after China, has made the most progress toward a national QKD infrastructure. In 2022, an 800-km QKD infrastructure was reported to connect 48 government organizations via a converged network [KED22].[48] The fact that this infrastructure is explicitly classified as the largest outside China is also found in independent strategy reports [SWNX23].[49]

But here, too, national coverage requires trust in trusted nodes. The fact that this network can be classified as productive is mainly due to the fact that the node locations are part of a government/authority security architecture.

USA

In North America, the best-known real-world QKD network is the DARPA Quantum Network (Boston/Cambridge). The network began operating in 2003 as a laboratory experiment and was shortly thereafter expanded via fiber optics under the streets of Cambridge, Massachusetts, including a multi-node network [Ell18].[50]

Russia

Russia strongly promotes QKD networks as a critical infrastructure application. A concrete, dated milestone is a quantum-encrypted video conference call via a QKD-secured line between Moscow and St. Petersburg on June 8, 2021, in which government officials also participated [ITMO21].[51] In addition, there are official roadmap communications (e.g., expansion targets over several thousand kilometers) [ICT21].[52] Overall, however, the information from Russia is not very transparent.

Overall Impression

The majority of existing QKD networks must currently still be classified as trial, pilot, or demonstration projects, which often follow real operating processes but do not claim to permanently supply the key material for genuine security-critical applications. At the same time, there is some reliable evidence to show that QKD is already being used productively or close to production in niche areas. This is particularly the case where (a) the costs/complexity are justified by high protection requirements and (b) the organizational trust assumptions (trusted nodes, secure locations) are acceptable.

---

[47] https://doi.org/10.1088/1742-6596/2416/1/012001.

[48] https://www.kedglobal.com/tech%2C-media-telecom/newsView/ked202206080023.

[49] https://swissnex.org/app/uploads/2023/05/Report_Epdf_290323_Final-Publish.pdf.

[50] https://doi.org/10.48550/arXiv.quant-ph/0412029.

[51] https://news.itmo.ru/en/science/cyberphysics/news/10393.

[52] https://ict.moscow/en/news/7000-km-of-quantum-networks-to-be-stretched-in-russia-by-the-end-of-2024.

3.4.3 Performance Data from Publicly Available Sources

During the research for this book, several specific QKD devices were also examined using publicly available sources. The detailed results of this research, together with all source references, are available on the book's website at.[53] In this book, these results are summarized and grouped according to technology classes.

It should be noted in advance that all manufacturers offer devices of varying quality. Standard configurations and premium variants are often offered, whereby the latter not only have a better success rate in detecting photons due to more sophisticated detector designs, but also have shorter dead times between detection events. Both effects mean that device variants from the same manufacturer can differ by a factor of 10 or more in terms of key rates under otherwise identical conditions. No information on device prices could be found in any of the publicly available sources. Non-binding price information for seven different products was obtained in an interview with a very experienced user with extensive knowledge. This interview is summarized in Chap. 3.4.4.

It should also be mentioned that the key rates specified by the manufacturers themselves often differ significantly from the values published in scientific papers, although some of these publications should be interpreted with caution because the authors are keen to justify the use of funding with good results. This does not mean that incorrect values have been published! However, it can be assumed that particularly low key rates are less likely to be published, while particularly good results are very likely to be published. As a result, there are indeed many publications that demonstrate the general functioning of laboratory and field trials, but when it comes to specifying concrete key rates, many publications provide no information at all, and in many others, the wording is so vague that it often remains unclear whether the raw key rates after sifting but before error correction and privacy amplification, or whether the entire post-processing has been taken into account. This is understandable and comprehensible because many research projects are primarily concerned with demonstrating the feasibility of certain procedures, whereby proof of stable continuous operation over several months can also be considered proof of feasibility.

DV-QKD

By evaluating publicly available manufacturer information, these approximate values were obtained for several different DV-QKD devices:

Distance	Key rate
50 km	Up to 300 kbit/s
60 km	2 kbit/s
65 km	2.2 to 18 kbit/s
90 km	1 kbit/s

(continued)

[53] https://cryptography.study/phys/QKD.

(continued)

Distance	Key rate
120 km	1 kbit/s

These figures illustrate two patterns typical for DV-QKD in fiber optics: First, the systems deliver several kbit/s at average attenuations of 10–15 dB, which corresponds to typical distances of 50–75 km. Second, optimized implementations (process/technology efficiency, clocking, detector technology) can be up to ten times higher at comparable attenuation, and thus in the double-digit to triple-digit kbit/s range. In particular, short distances in special configurations can even reach the Mbit/s range, but it can be assumed that these extremely high rates quoted by manufacturers can only be achieved under particularly controlled conditions that can hardly be expected in productive environments.

However, if we look at the values cited in independent scientific publications, the picture is as follows:

Distance	Key rate	Note
4 to 17 km	0.9 to 2.4 kbit/s	Average value from long-term operation
Approx. 13 km	0.48 to 1.7 kbit/s	24-h average
Just under 50 km	5.4 to 7.4 kbit/s	Stable over several weeks
50 km	36.5 to 63 kbit/s	Optimized device, 24 h
67 km	Approx. 270 kbit/s	Optimized device, 24 h

It is noticeable that the values fluctuate greatly, which is due to the fact that devices from different manufacturers with very different qualities were used for different distances. In some cases, key rates significantly higher than the manufacturer's specifications were even achieved in such test configurations. Unfortunately, it is not always clear whether the specified key rates are raw key rates or secure key rates. Especially at greater distances, a higher quantum error rate is to be expected even without eavesdropping, so that the length of the secure key after privacy amplification may only be a few percent of the raw key length, which means that a raw key rate in the three-digit kbit/s range can quickly become a single-digit secure key rate.

CV-QKD

The manufacturers surveyed who offer devices in this technology class are very reluctant to provide specific information on key rates or the maximum achievable distance.

One manufacturer claims that its current devices can bridge distances of up to 100 km, but without specifying concrete key rates.

Another manufacturer states that its devices can be used for up to 80 km (in fact, an attenuation of 16 dB is specified, which can be converted to 80 km according to the rule of thumb; see Sect. 3.4.1), and it states that speeds of up to 10 kbit/s can be

achieved with its devices. However, it is highly likely that the 10 kbit/s applies to very short distances, not to the maximum distance stated.

Unfortunately, independent sources are also not very informative. They only report that CV-QKD devices have been operated successfully over a longer period of time and that the key material generated in the process was distributed to endpoints in larger QKD networks together with the key material from other QKD systems.

QKD with Entangled Photon Pairs

One manufacturer offers a device that is suitable for fiber optic, free-space, and satellite operation, and another that is optimized for medium to long fiber optics. Both devices are specified to achieve 1.5 kbit/s at a distance of 50 km (actually: at an attenuation of 10 dB).

An independent source reported that a key rate of 0.09 kbit/s (i.e., 90 bit/s) was achieved in 10 days of operation at a distance of 70 km, while the manufacturer itself stated that 0.3 kbit/s (i.e., 300 bit/s) could be achieved in the laboratory at an equivalent attenuation. Another source stated that 70 km was the maximum distance that could be bridged.

Another manufacturer offers a device for up to 350 km of fiber optic cable, whereby, according to the manufacturer, approximately 0.007 kbit/s (7 bit/s) can be achieved. The transmitter is located in the middle of the distance, and the two receivers (Alice and Bob) are 350 km apart.

Another device from the same manufacturer is optimized for 10 to 20 km and can achieve up to 120 kbit/s at 10 km (2 dB) and 20 kbit/s at 50 km (10 dB).

It is striking that all public sources found focus heavily on the architecture of QKD networks (star topology, low trusted node density), while concrete secret key rates in kbit/s as a function of attenuation or distance are hardly to be found.

(More detailed reports with references can be found on the book's website at.[54])

MDI-QKD (Measurement Device Independent QKD)

Topologically, MDI systems are structured in exactly the opposite way to entanglement-based systems: there is a receiver in the middle that does not need to be trusted, and Alice and Bob send photons to it.

According to the manufacturer, devices in this category can bridge distances of up to 200 km. At 125 km (25 dB), a key rate of 0.5 kbit/s should be achievable. There are simulations of setups with 16 transmitters and one central receiver, in which each transmitter achieves a key rate of 1.5 kbit/s, but these figures are not based on real-world experiments.

[54] https://cryptography.study/phys/QKD.

3.4.4 User Survey

The Austrian Institute of Technology (AIT)[55] is an internationally established non-university research and technology organization and a key technical and scientific implementation partner of the EU-wide QKD initiative EuroQCI.[56] At the European level, the company is driving forward the integration of fiber optic, free-space, and satellite QKD and is actively involved in the evaluation of trusted node architectures and KMS connections. In Austria, AIT is playing a leading role in the development of national QKD test networks. AIT has been and continues to be significantly involved in many QKD projects, including OPENQKD,[57] eCausis,[58] QCI-CAT,[59] and several others. The company has extensive practical experience with QKD components. It was therefore a great pleasure and very important for the authors of this book to interview Mr. Florian Kutschera, one of the company's QKD network specialists, for this book, for which we are very grateful. In the process, we obtained the following valuable information.

DV-QKD

AIT used devices from three manufacturers that employ methods/technologies from the DV-QKD family. For devices from two of these manufacturers, the following secure key rates were specified depending on distance:

Distance	Key rate
15 km	7 kbit/s
50 km	5.4 kbit/s
65–80 km	2.2 kbit/s

In fact, no distances were mentioned in the interview, only attenuations. They were converted into distances for the book using the formula shown in Chap. 3.4.1. "Secure key rate" refers to the number of bits that are actually provided per second for symmetric encryption after post-processing (i.e., after sifting, error correction, and privacy amplification).

The above table does not include values for a device from a third manufacturer, for which only preliminary values were available at the time of the interview. This device could potentially bridge a distance of up to 150 km (attenuation: 30 dB), but this has not been officially confirmed. This particular device temporarily experienced a problem whereby the keys generated in the device could not be exported.

Approximate prices for the devices used were also quoted. AIT is paid between $140,000 and $220,000 per link for DV-QKD devices, i.e., for all devices at both

[55] https://www.ait.ac.at.

[56] https://petrus-euroqci.eu.

[57] https://www.ait.ac.at/en/research-topics/cyber-security/projects/open-qkd.

[58] http://ecausis.com.

[59] https://qci-cat.at.

ends of a fiber optic cable. According to AIT, equipment from a fourth manufacturer, for which no self-measured key rates were given, is available for around $330,000. Added to this are the costs for maintenance and operation of the equipment and the rental of the fiber optic cable.

It should be noted that these are past costs incurred by a customer with very specific requirements. It is not advisable to base a procurement decision on these individual figures. The costs mentioned here are only given to provide a very rough estimate of the approximate scale of a possible investment. Specific equipment prices must always be requested directly from the manufacturers.

Depending on the manufacturer, the devices are designed for distances of up to 80–150 km, with significantly lower key rates to be expected at greater distances.

For most manufacturers, the bridgeable distance can be increased on the receiver side by using device variants with higher-quality single-photon detectors.[60] However, higher-quality detectors are more expensive and, in most cases, require additional cryogenic cooling, which takes up extra space and consumes a lot of power.

In addition, one device was reported to have software problems and issues with remote maintenance, while another was notable for its highly fluctuating key rates. In one case, the key rates at particularly short distances also fell significantly short of expectations. However, it must be said that these are isolated cases that do not allow conclusions to be drawn about such devices in general. Nevertheless, they show that these are devices with very complex components that can cause problems in real-world operation and also require maintenance, which is a major challenge, especially for trusted nodes.

CV-QKD

In the case of CV-QKD, the AIT provided information on devices from two different manufacturers, with the following key rates being quoted for one device:

Distance	Key rate
15 km	10 kbit/s
25 km	1.4 kbit/s

Technical problems were reported with the other device, the cause of which was not suspected to be the devices themselves, but rather the fiber optic cable, which is why the device delivered only a few bits per second even over very short distances at the time of the interview. However, the same device had previously been able to deliver up to 4 kbit/s of secure key material over an unspecified distance.

In the interview, it was stated that the CV-QKD devices used are suitable for distances of up to 50–80 km, but that key rates in the single-digit bit/s range (i.e., between 0.001 and 0.01 kbit/s) are to be expected.

One of the two CV-QKD devices was described as the most pleasant and stable of the entire device fleet. The other device (the one that produced very low key

[60] See https://cryptography.study/phys/QKD-HW.

rates, presumably due to a faulty fiber optic cable) stood out due to its immature software and the fact that no certificates for the ETSI-014 protocol [ETSI19–14][61] were provided. These certificates are an important basis for the transfer of the key material to an HSM.

A major advantage of CV-QKD is that the quantum channel and the classical communication channel can be routed through the same fiber optic cable, thanks to a multiplexing process.

The acquisition costs were estimated at $180,000 to $200,000, although it should be noted that these are values from a past individual case and do not constitute a reliable basis for any calculations. In addition, several sources have assured us that there will be a significant drop in prices in the future, particularly for CV-QKD devices.

QKD with Entangled Photon Pairs

At AIT, only one device was in use that operated with entangled photons.

Distance	Key rate
A few meters	1 kbit/s
50 km	0.4 kbit/s

The operation of the device was described as very stable, but there were minor problems with the software of a receiver module. The user interface of the software was described as very clear and exemplary. The maximum usable distance mentioned in the interview was 50 km.

The equipment consists of a photon source in the middle of the route (between Alice and Bob) and two receiving stations where the photons are detected. The AIT stated that the cost for this was approximately $275,000. *(Caution: This is a single value from the past as a price range.)*

MDI-QKD (Measurement-Device-Independent QKD)

The AIT also used a device that belongs to the MDI-QKD technology class. Alice and Bob send photons to a central receiving station, which performs Bell measurements and announces the measurement results. Alice and Bob can use this information and the secret parameters they themselves contributed to generate a shared key. However, the publicly announced measurement results alone are worthless, which is why the measuring station does not have to be trusted.

The following preliminary information was provided in the interview, for which there was no official confirmation at the time of the interview, which is why this information is not very reliable: It may be possible to operate the device at an attenuation of up to 40 dB (equivalent to 200 km), and it may be possible to achieve a key rate of 0.5 kbit/s (500 bit/s) at 25 dB (equivalent to 125 km).

It was reported in the interview that a separate 16-amp power line had to be installed for the cryogenic cooling compressor in this device.

[61] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf.

The interview mentioned a price of approximately $410,000 for this. *(Caution: This is a single value from the past as a price range.)*

General Statements from the Interview

There is currently no standardization of QKD methods/technologies. This means that for each link, the devices at both ends of the link must be from the same manufacturer. However, since trusted nodes themselves are not quantum devices, but only connect individual quantum links at a higher level of abstraction, it is still possible to easily implement longer connections with individual links from different manufacturers with the help of trusted nodes. Only the devices at the ends of each individual quantum link must always be from the same manufacturer.

It was also announced that a total of approximately $165,000 had to be paid for the fiber optics for an 18-month trial setup along a 200 km route, which was divided into several links. *But here, too, the costs are from the past and are for a single customer with individual needs.*

3.4.5 Comparison of Specific Devices

This book is based on a study that included detailed descriptions of individual QKD devices. Most of the devices examined were used for fiber-optic QKD, but some devices suitable for free-space QKD or satellite QKD were also described. However, this detailed device comparison would exceed the scope of this book, so the authors decided to move it to the book's website at.[62]

3.5 Satellite QKD

In addition to the transmission of photons through fiber optics, the connection between two ground stations and a satellite also plays an important role. Because the light travels a significant portion of its distance through the Earth's atmosphere, satellite QKD suffers from the same disadvantages as free-space QKD. Since these limitations are more pronounced in free-space QKD than in satellite QKD, this topic is discussed in more detail in Chap. 3.6.

According to publicly available sources, a total of nine QKD-capable satellites have been sent into space to date, two of which have already exceeded their service

[62] https://cryptography.study/phys/QKD.

life and have probably already burned up in the atmosphere, namely SpooQy-1 [EOP19],[63] [NanSp][64] (Singapore) and Tiangong-2 [WP–Tia],[65] [N2TG][66] (China).

In December 2025, these seven QKD-capable satellites were in space:

Name	Country	Prepare and measure	Entanglement	Launch	Note
Micius [Lu22],[67] [Liao17b],[68] [Cast17][69]	China	Yes	Yes	2016	Main mission already completed in 2022. Micius is considered as an international QKD reference.
Jinan 1 [Chen21],[70] [Li25][71]	China	Yes	No	2022	"Flying" trusted node
Socrates [WP–Soc],[72] [EOPSoc],[73] [Tak17][74]	Japan	Yes	No	2017	Proof of concept, no operational key exchange, mission completed
QUBE [DLRQub],[75] [FAU25][76]	Germany	Yes	No	Aug. 2024	Technology demonstrator, focus on miniaturization and cost reduction. No results for QKD services

(continued)

[63] https://www.eoportal.org/satellite-missions/spooqy-1.

[64] https://www.nanosats.eu/sat/spooqy-1.

[65] https://en.wikipedia.org/wiki/Tiangong-2.

[66] https://www.n2yo.com/satellite/?s=41765.

[67] https://doi.org/10.1103/RevModPhys.94.035001.

[68] https://doi.org/10.1038/nature23655.

[69] https://doi.org/10.1038/nature.2017.22142.

[70] https://doi.org/10.1038/s41586-020-03093-8.

[71] https://doi.org/10.1038/s41586-025-08739-z.

[72] https://en.wikipedia.org/wiki/SOCRATES_(satellite).

[73] https://www.eoportal.org/satellite-missions/socrates.

[74] https://doi.org/10.1038/nphoton.2017.107.

[75] https://www.dlr.de/en/kn/research-transfer/projects/qkd-quantum-technology-for-secure-communication/qube-satellite-based-quantum-key-distribution.

[76] https://www.fau.eu/2025/08/news/research/global-quantum-encryption-small-satellites-as-quantum-key-generators/.

(continued)

Name	Country	Prepare and measure	Entanglement	Launch	Note
[QUICK3] [Ahn24],[77] [UniJ25][78]	Germany	Yes	No	June 2025	Technology and physics mission, no complete QKD service
SpeQtre [NanSpe],[79] [ISISpe][80]	Singapore + UK	No information	Yes	Nov. 2025	Already in space, but still in the commissioning phase at the time of writing. Operational launch announced for 2026.
Impulse-1 [NanImp][81]	Russia	Yes?	No	2023	Presumably QKD test

3.5.1 Micius

This satellite orbits the Earth in a sun-synchronous orbit at an average altitude of 478 km (perigee: 471 km, apogee: 485 km). It takes 94 min to orbit the planet. Figure 3.2 shows the orbit of Micius within one day (24 h).

The yellow spot above Europe in Fig. 3.2 marks the region above which Micius must be located in order to be seen from a ground station in Vienna (Austria). From Vienna, Micius can therefore only be seen in those sections of the orbit that are shown here in thicker and darker lines than the rest of the orbit. A simple geometric estimate shows that, under ideal conditions, Micius is visible from Vienna for a maximum of approximately 50 min within 24 h, divided into typically 6 overflights per day with a visibility duration per overflight of between 0 s and a maximum of 11 minutes and 16 s. Similar figures also apply to other regions of the world, with the total visibility time per day being shortest at the equator and longest at the poles.

Figure 3.3 shows the orbit of Micius in a true-to-scale comparison with the size of the Earth. It also shows how large a portion of the Earth's surface Micius sees at any given time. (Note: Micius' orbit does not pass exactly over the Earth's poles,

[77] https://doi.org/10.48550/arXiv.2301.11177.

[78] https://www.physik.uni-jena.de/en/iap/26345/quick3-mission-quantensatellit-mit-jenaer-know-how-startet-ins-all.

[79] https://www.nanosats.eu/sat/speqtre.

[80] https://www.isispace.nl/project/speqtre/.

[81] https://www.nanosats.eu/sat/impuls-1.

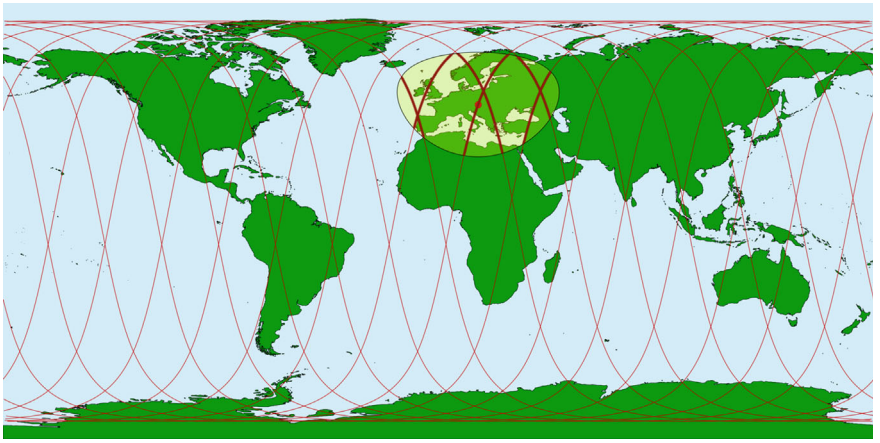

Fig. 3.2 Trace of the Micius satellite above the ground within one day

as Fig. 3.3 might suggest. The figure is only intended to show the relative sizes correctly. The exact course of the satellite's orbit above the Earth's surface is shown in Fig. 3.2.)

A total of six ground stations participated in the experiments with Micius. Four of them were in China (Xinglong, Lijiang, Nanshan, and Delhi), and the other two

Fig. 3.3 True-to-scale representation of the orbit (red circle) compared to the size of the Earth

were in Austria (in Graz and Vienna). There was also a smaller observation station in Ngari, Tibet [Liao18].[82]

Micius masters prepare-and-measure, but can also send entangled photons to two different ground stations.

Prepare and Measure

In Prepare-and-Measure, the satellite takes on the role of Alice in relation to both ground stations. Both ground stations then take on the role of Bob. However, this also means that the two ground stations do not exchange keys directly with each other; instead, each ground station exchanges keys separately with the satellite. The key material is therefore generated in the satellite, which thus also assumes the role of a trusted node. This creates a QKD network between the ground stations and the satellite, and the participants in this network obtain a negotiated key via the protocols of this network. This approach also means that it is not necessary for the two ground stations to exchange keys at the same time. For example, a ground station in China first performs a key exchange, and hours later, when the satellite becomes visible over Europe, a station in Austria performs a key exchange and then obtains the key that China received from the satellite, and a few hours later, a ground station in China obtains the key that was generated between Austria and the satellite.

The first publication on experiments with Micius from 2017 [Liao17a, Liao17b][83] reported that a total of 300,939 usable key bits were generated during a 273-second time slot (4 min, 33 s). This corresponds to 1.1 kbit/s during this time slot. Considering that the satellite typically flies over a ground station 6 times per day, this would result in a maximum of approximately 1.8 Mbit per day. From this, a long-term average of 21 bits/s can be calculated. However, only 4 flyovers within 23 days could actually be used in this experiment, which can be extrapolated to 1.2 Mbit in 23 days or 0.6 bits/s.

Four years later, in 2021, 47.8 kbit/s were published during a "typical" flyover, but these were raw key bits, before error correction and privacy amplification [Chen21].[84] However, in 2024, it was reported that during a 220-second flyover, a secure key material with a length of 310,400 bits was obtained, which corresponds to 1.4 kbit/s and is more in line with the 2017 value [Khm24].[85] But even the peak raw key value from 2021, when extrapolated to a full day under ideal conditions, averages only about 900 bits/s over the entire day.

QKD with Entanglement

In this variant, the satellite generates entangled photon pairs, which it sends to two ground stations. (One photon from each pair to Alice, the other to Bob.) For this to work, the satellite must be visible above the horizon from Alice's point of view and at the same time from Bob's point of view. The two ground stations must therefore

[82] https://doi.org/10.1103/PhysRevLett.120.030501.

[83] https://doi.org/10.1038/nature23655.

[84] https://doi.org/10.1038/s41586-020-03093-8.

[85] https://doi.org/10.1364/OE.511772.

not be too far apart. Two stations that are more than approximately 4800 km apart never see the satellite at the same time and therefore cannot exchange keys via the satellite using entanglement. (Compare this with Fig. 3.2.)

In an experiment conducted with Micius, both ground stations were in China, one in Lijiang and the other in Delhi. For key exchange to be possible, the satellite must have both ground stations in its field of view at the same time. Since these two locations are 1203 km apart, according to the publication [Yin17],[86] this was only possible once a day (at approximately 1:30 a.m. local time, i.e., at night) for a duration of 275 seconds (approx. 4½ minutes) each time. (It can be assumed that there were also flyovers during daylight hours when the satellite had both ground stations in its field of view at the same time, but this was not reported. Presumably, the scattered light from the sun was so strong during the day that key exchange was only possible at night, but again, nothing was reported about this.) In fact, in one case, measurements were taken for approximately 250 seconds, and 134 photon pairs were found to have matching polarization. Thus, after sifting, a raw key length of 134 bits was achieved. Unfortunately, despite intensive research, nothing could be found about how many bits remained after error correction and privacy amplification, or whether these steps were even performed. The sources found suggest that three such experiments were conducted on three different nights, but exact figures could only be found for one experiment [Lu22].[87]

This means that the raw key rate (before error correction and privacy amplification) for satellite-based entanglement QKD is 134 bits per day, which corresponds to approximately 0.0015 bits per second.

Criticism of Micius

In the entangled photon mode, Micius does not achieve a usable key rate and can only be considered a feasibility study.

When implemented in prepare-and-measure mode, analyses by research teams revealed a clearly measurable design flaw that is relevant to security: Micius uses the BB84 protocol with decoy states. The purpose of the decoy states is to detect an eavesdropper performing a photon number splitting (PNS) attack. However, this only works if the eavesdropper cannot distinguish signal pulses from decoy pulses. Micius uses different laser diodes for the two types of pulses, for which a clearly different timing behavior could be demonstrated. This enables the attacker to distinguish signal pulses from decoy pulses, to which they could then react. However, this means that an attacker remains undetected when carrying out a PNS attack, despite the decoy pulses. Under the usual security models, the implementation used can therefore no longer be considered information-theoretically secure [Mil25].[88]

[86] https://doi.org/10.1126/science.aan3211.

[87] https://doi.org/10.1103/RevModPhys.94.035001.

[88] https://doi.org/10.48550/arXiv.2505.06532.

3.5.2 Jinan-1

Jinan-1 is newer than Micius, but does not have a source of entangled photons on board. Jinan-1 can only be operated in prepare-and-measure mode. Its trajectory data is very similar to that of Micius. This satellite weighs only about 4% of Micius (Micius: 640 kg, Jinan-1: 23 kg) and costs only about 2.2% of the price of Micius. Unlike the Micius research satellite, Jinan-1 was developed with a greater focus on practical application. This satellite is also supposed to be able to work with portable ground stations. Such portable stations weigh around 100 kg.

The design of Jinan-1 avoids the flaw made with Micus, as Jinan-1 only has one photon source that is used for both types of pulses. This means that signal and decoy pulses cannot be distinguished by an attacker.

With Jinan-1, a peak value of up to 1.07 Mbit of secure key material was generated per flyover of a ground station. This results in up to approximately 5 Mbit per day, which averages out to just under 60 bits/s over an entire day. Other studies mention approximately 400,000 bits per flyover, which amounts to 2 Mbit per day and a daily average of 23 bits/s [Li25].[89]

3.5.3 Other Current QKD Satellites

The three satellites Socrates, QUBE, and [QUICK3] are (or were) primarily technology and feasibility demonstrators, i.e., not "productive" QKD satellites like Micius or Jinan-1, which deliver measurably large amounts of keys for real-world applications.

Socrates did not implement error correction or privacy amplification and, as a pure technology demonstrator, was only intended to show that certain QKD variants can be implemented in satellites [Car18].[90]

QUBE was also intended solely to demonstrate a specific technology, namely miniaturization. Although full-fledged key exchange is possible in principle with QUBE, this is not one of the objectives of the research project, and no publications on this topic could be found [LMU24].[91]

[QUICK3] is used for basic physics research, as this satellite is testing how a novel photon source (a dye center in a boron nitride crystal) functions in zero gravity. In principle, the satellite could be used for key exchange, but this is not mentioned as a mission objective in publicly available sources [QUICK3].[92]

SpeQtre is only the second satellite after Micius that will be able to emit entangled photon pairs. (The SpooQy-1 satellite, which has since burned up, also had an

[89] https://doi.org/10.1038/s41586-025-08739-z.

[90] https://doi.org/10.1117/12.2309624.

[91] https://www.lmu.de/en/newsroom/news-overview/news/global-quantum-key-encryption-nano-satellite-qube-launches-into-space-66e31186.html.

[92] https://www.quick3.de.

entangled source on board, but only used it to perform on-board measurements.) It was launched into space shortly before this book was completed, on November 28, 2025, and is undergoing a test phase during the completion of the book to test the functionality of all subsystems. Initial QKD experiments with ground stations in Singapore and the United Kingdom have been announced for spring 2026. All available sources refer to entangled photons. There is no information on whether SpeQtre can also be operated in prepare-and-measure mode [QZ25].[93]

However, SpeQtre is also designed as a demonstrator, not as a satellite for permanent production operation.

Impuls-1 is not actually a QKD satellite, as the main task of this Russian satellite is to observe the sun in the soft X-ray range. However, it also carries the "Vektor" laser communication payload, whose exact purpose is unclear. In any case, the Nanosats database tags Impuls-1 with "QKD – Quantum Key Distribution" and the mission text in this database reads: "solar activity monitoring in soft X-ray range, laser and quantum communications development." Unfortunately, no further information about Impuls-1 could be found [NanImp].[94]

All of the satellites mentioned are in a similar orbit to Micius (LEO = Low-Earth Orbit, between 450 and 600 km above the ground).

3.5.4 Planned QKD Satellite Missions

EAGLE-1 is a planned QKD demonstrator from the ESA (European Space Agency) and is to be used for EuroQCI. The aim of this pilot project is to offer genuine end-to-end QKD services for users in the EU. The launch of this mission was originally scheduled for fall 2024, but has already been postponed several times. Currently (January 2026), all that is known is that the launch is scheduled for "late 2025 or early 2026." Like all previous QKD satellites, EAGLE-1 will also have a low orbit (LEO) [ESA1].[95]

Eagle neXt is a planned follow-up mission to EAGLE-1. There are still no clear statements as to whether Eagle neXt will launch a single QKD satellite into space or several. However, ESA has stated its goal of having several QKD satellites orbiting the Earth at the same time in order to establish a QKD network in space, specifically mentioning the Eagle-1, Eagle neXt, SAGA, and QKDSat missions in this context [SES24].[96]

SAGA is another project by ESA and EuroQCI that is explicitly aimed at European government users. The system design is currently being developed, so there is only a

[93] https://quantumzeitgeist.com/speqtre-quantum-quantum-comms/.

[94] https://www.nanosats.eu/sat/impuls-1.

[95] https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1.

[96] https://www.ses.com/newsroom/eagle-1-advancing-europes-leadership-quantum-communications#tab-eagle-next.

preliminary draft at this stage. According to publicly available sources, nothing has been built yet, and a launch date has not yet been announced [ESA19].[97]

QKDSat is another QKD project by ESA that aims to launch an operational trusted node into space to provide governments and commercial users with secure keys. The satellite is scheduled to launch in 2027. ("QKDSat" is also the name of an older QKD project on which ESA and the British company ArQit worked. It ran from 2017 to 2021 but did not result in a satellite.) [ESA2].[98]

QKD-GEO/Caramuel will be a Spanish-led QKD satellite in geostationary orbit, with Thales Alenia Space and Hispasat as the two main players. "Geostationary" means that it will orbit the Earth directly above the equator at an altitude of 35,786 km and that it will take exactly 24 h to complete one orbit around the Earth. It will therefore be permanently visible from Europe. This means that QKD-GEO will not be subject to any restrictions due to short overflight times. However, the satellite is about 75 times farther from Earth than Micius or any other LEO satellite, which is likely to cause new problems. This is because the solid angle at which a satellite dish with a diameter of 1 m, for example, appears from the position of QKD-GEO is 5625 times smaller than the solid angle from the position of a LEO satellite. The loss of photons flying just past the receiver dish will be correspondingly higher. QKD-GEO will be the first geostationary QKD satellite and is to be integrated into the EuroQCI architecture. There is no official date for the launch into space yet, but the project was started in 2025 and the development time was predicted to be 2 years [Alv22].[99]

QEYSSat is a Canadian QKD project that aims to provide a fully developed key exchange, including with entangled photons. The launch is announced for the end of 2026 [Jen24].[100]

SpeQtral-1 is a planned QKD project from Singapore that aims to offer QKD services to commercial partners in the form of a pilot project. SpeQtral-1 will operate without entangled photons, but a follow-up project that will also use entangled photons is already planned [SPEQ].[101]

NICT–JAXA is a Japanese QKD project that began in 2025. Information about it is still sparse, in particular there is no launch date yet [VIA25].[102]

SAQTI is a possible name for an Indian QKD project, about which all that is known so far is that the program is scheduled to run until around 2030 or 2031 [Redd].[103]

---

[97] https://www.esa.int/ESA_Multimedia/Images/2019/04/SAGA_for_quantum_key_distribution.

[98] https://www.esa.int/Applications/Connectivity_and_Secure_Communications/QKDSat_Secure_communication_via_quantum_cryptography.

[99] https://doi.org/10.1109/ICSOS53063.2022.9749720.

[100] https://doi.org/10.48550/arXiv.2306.02481.

[101] https://speqtralquantum.com.

[102] https://www.satellitetoday.com/technology/2025/08/28/sky-perfect-jsat-joins-quantum-cryptography-satellite-rd-project.

[103] https://www.reddit.com/r/ISRO/comments/1gczzq5/planned_satellite_for_quantum_key_distribution_is/

China is currently working on several QKD satellite projects. Among other things, a quantum communication mega-constellation is planned, which will consist of several QKD satellites in low orbit and will be operated in cooperation with the BRICS countries. Two to three satellites are to be launched as early as 2026. China also plans to launch a geostationary QKD satellite into space in 2027 or 2028 [[CAS25],[104] [CRF25],[105] [TQI25],[106] [YIC24],[107] [SCM25][108]].

Russia tends to focus on terrestrial projects in the field of QKD, but is collaborating with other BRICS countries on Chinese projects. There are also plans to test QKD services from the ISS space station. Russia has had its own satellite (Impuls-1, see above) in space since 2023 with the potentially QKD-capable payload Vektor, which also points to its own initiatives in this area, but little information about this is publicly available. [[MER24],[109] [JRC19],[110] [TAS18][111]].

USA: In an official paper [NSA],[112] the [NSA] warns of practical limitations of QKD and recommends that US national security systems focus on post-quantum cryptography until the known QKD problems (scaling, infrastructure, trust assumptions) are solved. Therefore, at least from the government's perspective, QKD is not a central pillar of a crypto strategy in the US. Nevertheless, DARPA has developed a roadmap for quantum communication between ground stations and LEO and MEO satellites (MEO = Medium Earth Orbit, i.e., orbits at altitudes between 2000 and 36,000 km; often with a period of 12 h and a highly elliptical orbit), but has not yet named any specific QKD missions [[NAS24],[113] [NSc05].[114]

However, there are commercial companies in the US that see satellite QKD as a lucrative market and are therefore investing in such projects. For example, following its acquisition of Capella Space, IonQ plans to build a "global space-to-space and space-to-ground satellite QKD network," and Boeing is distributing PR material about the Q4S satellite, which is scheduled to launch in 2026 to demonstrate

---

104 https://english.casad.cas.cn/newsroom/ma/202503/t20250325_908666.html.

105 https://www.crfindia.org/-/media/Project/ChintanResearchFoundation/Publications-PDF/19-Sep/Chinas-Ascent-as-a-Quantum-Space-Power.ashx.

106 https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa.

107 https://www.yicaiglobal.com/news/china-is-likely-to-build-global-quantum-communication-network-in-near-future-scholar-says.

108 https://www.scmp.com/news/china/science/article/3315963/new-dawn-pan-jianwei-reveals-high-orbit-quantum-satellite-global-network.

109 https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf.

110 https://doi.org/10.2760/38407.

111 https://tass.com/science/1008731.

112 https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

113 https://ntrs.nasa.gov/api/citations/20240003113/downloads/AQCF_March2024_SCaNPresentation.pdf.

114 https://www.newscientist.com/article/dn7484-quantum-cryptography-network-gets-wireless-link/.

"quantum networking in space." However, apart from such marketing statements, no concrete information has yet been forthcoming. [Ion25],[115] [Boe].[116]

Brazil: The situation here is very similar to that in all other BRICS countries: the focus is on terrestrial QKD projects (e.g., "Rio Quântica" [Fon24][117]), and satellite QKD projects are being left to China. Apart from concept studies, no concrete evidence of Brazil's own efforts in this direction could be found. Instead, the intention is to communicate with Chinese QKD satellites from Brazilian ground stations [MER24].[118]

3.6 Free-Space QKD (Line-of-Sight Connection through the Air)

In addition to fiber optics and satellite connections, this is the third way to transport photons from a transmitter to a receiver. It should be noted that in satellite QKD, the photons also travel part of their distance through layers of air, so all the problems mentioned here for free-space QKD also apply to satellite QKD.

The following rule of thumb applies: The entire column of air above a point on the ground (up to outer space) contains approximately the same amount of air as between two points on the ground that are 10 km apart. Since satellites are only in exceptional cases located exactly vertically above a ground station, the photons in satellite QKD usually move diagonally upward through the air, so that the path between the ground station and the satellite can be roughly estimated at an air distance of approximately 15 km [OU23].[119]

Almost all known QKD applications use wavelengths in the near-infrared range. Although this light is not visible to the human eye, it shares many properties with visible light. Some research groups even use wavelengths in the visible range. In the case of free-space QKD in particular, the situation is roughly comparable to someone trying to observe the glow of a very faint candle at a great distance with binoculars. This does not work in fog, rain, or snowfall. Smog can also impair visibility, especially in cities. When looking up (at a satellite), clouds block the view, and during the day, the air between the candle and the binoculars deflects so much sunlight into the binoculars as scattered light that the light from the candle is lost in this scattered

[115] https://www.ionq.com/news/ionq-completes-acquisition-of-capella-space-advancing-vision-for-space-based.

[116] https://www.boeing.com/space/quantum.

[117] https://revistapesquisa.fapesp.br/en/brazils-first-quantum-cryptography-network-is-expected-to-connect-five-research-institutions/.

[118] https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf.

[119] https://www.open.edu/openlearn/science-maths-technology/engineering-environmental-fluids/content-section-3.1.

light. And on hot days, heated air causes turbulence that also makes it impossible to observe the candle [Vas17].[120]

Therefore, both free-space and satellite QKD work best on starry, cold nights.

3.6.1 Current and Completed Free-Space Projects

- A paper published in 2023 entitled "Towards metropolitan free-space quantum networks" [Krz23][121] by authors from the German Fraunhofer Institute and the Austrian AIT reports on a free-space project in **Jena** (Germany). The research group bridged a distance of 1.7 km with mobile QKD devices using entangled photons. A key rate of "up to 5.7 kbit/s" was achieved at night. During daylight hours, 2.5 kbit/s was measured. The same group had already demonstrated the feasibility of entangled free-space QKD on a 300-meter distance in Bonn (Germany) in 2021. The project is clearly designed as a network testbed. The keys generated are processed using a simple KMS with a network stack. As far as can be seen, however, no permanently productive critical application is planned. The project is a demonstrator for future EuroQCI-type infrastructures.
- Back in 2007, Austrian researchers (University of Vienna; IQOQI) demonstrated that a distance of 144 km between the two Canary Islands **of La Palma and Tenerife** could be bridged using free-space QKD. A key rate of 12.8 bits/s was achieved. This unique experiment was a historically important milestone in QKD research [Schm07].[122]
- Since 2023, a research group led by Nobel Prize winner Anton Zeilinger (Austria) has been operating a 10.4 km free-space link between a transmitter on Bisamberg (a hill north of Vienna) and a receiver on the roof of the University **of Vienna**. The research group is using this to test new entanglement-based methods/technologies and has also demonstrated the fundamental feasibility of QKD over 10.4 km of free space. The publications focus on the entanglement quality and stability of the connection. Explicit long-term key rates are not highlighted [Bul23].[123]
- **AirQKD** is an open-air QKD project that has been running in the United Kingdom since 2020 over a 135-meter open-air distance in Suffolk. Key rates of "up to" 84.3 kbit/s have already been achieved. The goal of the project is to secure the last mile in 5G networks. Unfortunately, long-term averages could not be found. The project can be seen as a pilot or field trial in which very specific 5G use cases are to be demonstrated [Zha25].[124]
- In Italy, at the University of Padua, the "**Full daylight QKD at 1550 nm**" project has been running since 2021. The test track runs between two roofs in Padua

[120] https://doi.org/10.1103/PhysRevA.96.043856.
[121] https://doi.org/10.1038/s41534-023-00754-0.
[122] https://doi.org/10.1103/PhysRevLett.98.010504.
[123] https://doi.org/10.1103/PhysRevX.13.021001.
[124] https://doi.org/10.1364/JOCN.553171.

and is 145 meters long. Key rates of 30 kbit/s on average are achieved in bright daylight. In principle, the keys generated could be fed directly into an HSM, but the project is not about practical usability, but rather about demonstrating daylight robustness [Ave21].[125]

- An Italian-Austrian research group also attempted to demonstrate **daylight robustness** in 2021 (publication in 2022/23), but with entangled photons. The group conducted several experiments at different distances (mostly between 300 and 500 meters) and obtained raw key rates of around 100 bit/s and a secure key rate of 12 bit/s after sifting [Bas23].[126]
- Several European research groups have collaborated with partners in **China** and achieved key rates between 100 and 400 bits/s over distances between 500 meters and approximately 1 km [Gon18],[127] [Shen18].[128]
- Also in **China**, a 53 km free-space link was operated as a technology demonstrator in 2017 with the aim of simulating QKD connections between satellites. In 1756 seconds (approximately half an hour), 157,179 bits were generated, from which a key rate of 90 bits/s can be calculated [Liao17a, Liao17b].[129] This was followed in 2024 by a follow-up project that achieved a key rate of 495 bits/s over a distance of 20 km on a daily average (day and night operation) [Cai24].[130]
- As early as 2002, a 10 km long free-space link was tested in **Los Alamos (USA)**. Key rates in the single-digit kbit/s range were achieved, and a strong dependence of the key rate on the weather and the time of day was reported. The keys generated in this test were actually used to initialize real crypto devices, but this project was also designed as a test only [Hug02].[131]

There are a number **of other free-space projects worldwide** that have published similar results to the examples cited here. All of these projects are research projects focused on feasibility and on operating such applications in daylight conditions. The distances bridged are usually in the range of 1 km or even significantly less, and the key rates rarely exceed the 1 kbit/s limit. As far as could be ascertained, at the time of completion of this book, there are no free-space QKD applications in productive continuous operation for security-related applications.

[125] https://doi.org/10.1038/s41534-021-00421-2.
[126] https://doi.org/10.1088/2058-9565/acae3d.
[127] https://doi.org/10.1364/OE.26.018897.
[128] https://doi.org/10.1103/PhysRevA.100.012325.
[129] https://doi.org/10.1038/nphoton.2017.116.
[130] https://doi.org/10.1364/OPTICA.511000.
[131] https://doi.org/10.1088/1367-2630/4/1/343.

3.6.2 QKD Projects with Planned Free-Space Components

- **MOZART** (a K-PASS project of the FFG) is an AIT project whose project description was published in October 2025 and which is just getting underway at the time of this book's completion. The aim of the project is to develop requirements and feasibility for future QKD-based connections between the Vienna government network and the federal fallback system in St. Johann (Austria). A large part of the project will be implemented using fiber optics, but the project description also explicitly mentions the use of free-space QKD. Whether this will be done on a section between Vienna and St. Johann or whether it will be used to connect buildings within Vienna could not be determined from publicly available sources. MOZART is the only publicly known QKD project in Austria that refers to free-space QKD [KPa25].[132]
- **LAiQa** is a Horizon Europe project led by Greece with the participation of the Austrian company QTLabs. The project has been running since January 2024 and has, among other things, a 2.5 km free-space link and a ground-to-satellite connection on its to-do list, but no results have been published yet [COR25].[133]
- **QuFree** is a QKD project launched in 2023 in northern Italy, which also plans to test free-space QKD connections. Many fiber optic connections have already been put into operation, and in February 2025 it was reported that work on the free-space connection would begin soon, including the installation of receivers on ships. More recent information could not be found [Uni25].[134]
- There are **many other ongoing QKD projects** in which free-space links are also being tested "on the side," but the associated publications usually only mention the results on fiber optic links, so it is unclear for many ongoing projects whether testing on free-space links has even begun. Pure, permanently operated free-space QKD infrastructures without integration into other technologies are currently hard to find; they are usually test beds or field trials. It should also be mentioned that all projects mentioned so far use DV-QKD, i.e., QKD with single photons. However, there are also free-space research projects that work with CD-QKD.

3.6.3 Free-Space QKD with Mobile Devices

For some time now, attempts have been made to carry out quantum key distribution using balloons, drones, aircraft, and ships. However, it must be strongly emphasized that all experiments in this direction are still purely research-based and that, as far

[132] https://www.k-pass.at/en/financed-proposals/detail/mozart-requirements-for-quantum-communication-solutions-for-connecting-the-vienna-public-authority-network-and-the-zas-st-johann/.

[133] https://cordis.europa.eu/project/id/101135245.

[134] https://portale.units.it/en/news/quantum-link-over-fibre-optics-inaugurated-between-units-and-uniud.

as can be gleaned from the researched material, no devices for continuous use can be purchased now or in the coming years.

In 2021, a Chinese research group published a survey paper on this topic [Xue21].[135]

In it, they define "airborne QKD" on the one hand as an intermediate stage between satellite QKD and terrestrial QKD variants (fiber optics, free beam), but on the other hand also as a variant of free beam QKD with mobile transmitters or receivers, some of which have relatively high relative speeds. A distinction is made between:

- **UAVs/drones**: "last mile" relays, temporary nodes in inner-city or field networks.
- **Slow-flying aircraft**: greater ranges, longer visibility windows, tactical applications.
- **HAPs/stratospheric platforms**: relays between satellite and ground, large-area coverage.

The survey paper describes several experiments conducted between 2013 and 2021 using drones and balloons. In an experiment conducted in 2015, a key exchange was even carried out using a moving pickup truck. (The car on which Bob was mounted drove past Alice at a speed of 33 km/h at a distance of 650 m, during which a 4-second key exchange session was successful, yielding 160 bits [Bou15].[136])

The authors report that distances of 200 m to 20 km were covered in such experiments and that key rates in the order of up to approx. 300 bit/s were achieved, in some cases at relative speeds of up to approx. 260 km/h. In addition to the physical characteristics of such approaches, the authors also briefly touch on the security aspect of such mobile QKD applications and mention device imperfections in particular as a possible source of side-channel attacks, but security is only a marginal topic in this paper.

In 2024, another research group published a similar paper [Dub24].[137] It addresses many technical and physical challenges, such as atmospheric effects (turbulence, humidity) and weather dependence, coupling problems, target tracking, stabilization, synchronization, and timing. The authors also outline visions for the future, such as QKD networks implemented with drone swarms.

In their conclusion, the authors emphasize that they see great potential for military applications, but also for other field operations (e.g., natural disasters), but that there is still a long way to go before such systems reach a level of maturity that allows them to be used in real-world scenarios. The specific key rates and distances cited by the authors in this comprehensive survey paper are similar to those described in the paper mentioned above for moving transmitters and receivers. In an experiment, the authors of the survey paper claimed that a key rate of 868 kbit/s was achieved with an aircraft, which would be a very high value even for a fiber optic connection. However, the abstract of the original paper [Pug17][138] correctly states that the key

[135] https://doi.org/10.3788/COL202119.122702.

[136] https://doi.org/10.1364/OE.23.033437.

[137] https://doi.org/10.1016/j.physo.2024.100210.

[138] https://doi.org/10.1088/2058-9565/aa701f.

material with a total length of 868 kbit was collected "in a few minutes." There appear to be several such errors in the survey paper, but it nevertheless provides a good overview of current efforts in this field of research.

3.7 Trusted Nodes and KMS Networks

Trusted nodes [QNu][139] play a central role in today's large-scale QKD infrastructures. In China in particular, there are networks with more than 40 nodes, some of which bridge distances of several thousand kilometers [Che21],[140] [CAS17],[141] and almost every country in Europe also operates such a network. Initial plans are already in place to connect these national networks into a large pan-European QKD network, which will then consist of hundreds of such trusted nodes [EC25].[142]

Trusted nodes serve as intermediate stations where the key material is received, temporarily decrypted, re-encrypted, and forwarded to the next station. Their existence is due to the physical limitations of today's QKD systems: the losses of optical fibers increase exponentially with distance, and the range of pure end-to-end QKD is therefore typically limited to a few hundred kilometers. Free-space and satellite QKD can also only enable point-to-point key exchange. To bridge very large distances, such as continental or national backbone routes, chains of QKD links are therefore established, which are connected to each other via trusted nodes.

The key advantage of this architecture lies in its technical feasibility and scalability: trusted node networks can already be set up today using commercially available QKD systems and enable the cascading of the key material over hundreds or even thousands of kilometers. They form the backbone of many current demonstrators and pilot networks, including European, Asian, and North American QKD initiatives. At the same time, a new type of critical infrastructure is emerging: since trusted nodes have access to plaintext key material, they must be operated under strict security conditions. Physical security, access control, protection against manipulation, trusted modules for key processing, and organizational measures are essential, because even a single compromised trusted node can jeopardize the entire network path.

Trusted nodes are therefore both a technical necessity and a security vulnerability in current QKD networks. In the long term, they should be replaced or at least relieved by new concepts, such as interferometric methods like twin-field QKD, or by real quantum repeaters, which would enable entanglement-based quantum networking without trust assumptions. Since such technologies are being researched

---

[139] https://www.qnulabs.com/glossary/trusted-nodes-quantum-network-architecture.

[140] https://doi.org/10.1038/s41534-021-00474-3.

[141] https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml.

[142] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

in experiments but are still far from being commercially viable, trusted nodes will continue to be the dominant architectural principle of large QKD networks in the coming years.

3.7.1 Important Terms and Definitions

Trusted Node

A trusted node is an intermediate station in a QKD network that processes key material in plain text. The node receives the key generated by QKD from a quantum link, stores it, combines it with other keys, and forwards the combined keys to other trusted nodes or end nodes via a classical channel. The security of the entire path depends on each individual node being completely trustworthy and physically and organizationally protected. An attacker who compromises a trusted node can access the key material of all passing connections [ETSI19–14].[143]

Quantum Repeaters [QSNP–QR].[144]

A quantum repeater is a device that enables entangled quantum states to be distributed over very long distances without intermediate stations gaining access to Technically, a quantum repeater does the following:

- It generates entanglements,
- it distributes the entanglements across multiple segments,
- it connects segments using entanglement swapping,
- it uses quantum memories to temporarily store quantum states without measuring them.

A functioning quantum repeater would make trusted nodes superfluous, as no intermediate station would need to know the keys. However, only laboratory prototypes exist so far. Intensive work is being done on quantum repeaters worldwide, including in China, Europe, the US, and South Korea. However, no fully practical implementation is available yet.

KMS

This is the abbreviation for *Key Management System.* This refers to the way in which multiple trusted nodes, connected to each other via quantum links, interact with each other to distribute shared key pairs to the endpoints of such a network without requiring a direct quantum link between these endpoints. In addition to distribution across multiple trusted nodes, a KMS typically also includes the secure

[143] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf.

[144] https://qsnp.eu/glossary/quantum-repeater/.

storage, management, deletion, and assignment of keys to specific applications [ETSI20–04],[145] [ETSI22–18].[146]

3.7.2 How a Trusted Node Works

A trusted node is the endpoint of two or more quantum links belonging to different terminals. For example, the trusted node named "Tom" may be connected to Alice via a fiber optic link running the BB84 protocol and to Bob via a satellite station, with the satellite emitting entangled photons and Tom and Bob using the E91 protocol to generate shared key material. (In this example, therefore, no key material is generated in the satellite.)

Over time, Alice and Tom have generated a large number of key bits, which they combine into key packets. Packets of 256 bits each are very common and can be used for AES encryption, for example. Alice and Tom have generated the key packets S_{a1}, S_{a2}, S_{a3}, etc. in this way. The keys S_{b1}, S_{b2}, S_{b3}, etc. are generated between Bob and Tom via the satellite link. This means that Tom knows all the keys mentioned and that Alice and Bob do not (yet) have a shared key.

If Alice wants to send a message to Bob, she needs a key that Bob knows. Therefore, Alice requests such a key from Tom. Tom now takes a key that Alice and Tom know (e.g., S_{a1}) and a key that Bob and Tom know (e.g., S_{b1}) and combines them with an XOR operation[147] to obtain S_{a1b1} with this formula: $S_{a1b1} = S_{a1} \oplus S_{b1}$. This is known as one-time pad encryption (OTP), and in OTP-terminology, S_{b1} is the plain text, S_{a1} is the secret key, and S_{a1b1} is the cypher text.

Tom sends the bit sequence S_{a1b1} to Alice, and Alice also performs an XOR operation with S_{a1} to obtain S_{b1} as follows: $S_{b1} = S_{a1} \oplus S_{a1b1}$. The key S_{a1} is now used up, which means that Alice and Tom delete this key from their memory. More importantly, Alice and Bob now both know the key S_{b1}, which they can use for their intended purpose. Typically, Alice and Bob do not use the key S_{b1} for one-time pad encryption, but for AES or, a comparable encryption method. Nevertheless, the key S_{b1} is removed from the KMS network because there are now two endpoints that share it.

And in the same way as in this simple example, where there was only one trusted node between Alice and Bob, there can also be a chain of several trusted nodes between Alice and Bob, for example: Alice—T_1—T_2—T_3—Bob. If Alice needs one of Bob's keys, she sends the request to T_1, which forwards the request along the chain to T_3, and from there the key is forwarded in the opposite direction to Alice,

[145] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf.

[146] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018v010101p.pdf.

[147] See Chap. 6.

with one key being used on each section of the route. In this way, extensive QKD networks can be implemented.

However, there are other methods for supplying the endpoints of a QKD network with shared keys. In this case, the keys generated by quantum physics are not used for OTP encryption (where they are consumed), but new keys are generated in the trusted nodes with the aid of random number generators, which are distributed to the end points, and the "real" quantum keys are used as AES keys to secure transport between neighboring trusted nodes. No "real" quantum keys are consumed in this process, and only keys that originate directly from the random number generators of the trusted nodes reach the end points. This prevents key scarcity in a QKD network, but it does create new attack vectors that jeopardize the security of the entire network. To mitigate this problem somewhat, the real quantum keys are also considered "used up" after a certain period of time (or after a certain number of uses) and are deleted.

3.8 Implementation and Side-Channel Attacks on QKD Systems

The basis for the description of implementation and side-channel attacks on QKD systems is a study by the German Federal Office for Information Security (*Bundesamts für Sicherheit in der Informationstechnik*—BSI) entitled "Implementation Attacks against QKD Systems," which was published in fall 2023. Details on implementation and side-channel attacks can therefore be found there [BSI23].[148]

3.8.1 Theoretical QKD Security Versus Real Systems

The implementation and side-channel attacks investigated by the BSI highlight the need to distinguish between the theoretical security of QKD methods/technologies and the security that can actually be achieved by real QKD systems. Security assurances derived from formal models and physical assumptions apply under idealized conditions. They assume that all components involved correspond exactly to the assumed security model and also operate within defined parameters.

Real QKD systems inevitably deviate from this. Hardware components have imperfections, additional functions are required to ensure stability and availability, and ongoing operation requires calibration, monitoring, and control mechanisms. The security that can actually be achieved therefore does not result solely from the method/technology used, but from the specific design of the overall system, including hardware, software, control logic, and operating processes.

[148] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.pdf.

Side-channel attacks exploit precisely this difference between model and implementation. They do not attack the QKD method/technology itself, but exploit deviations, side effects, or additional functions of real implementations. The BSI study shows that such attacks are not exceptional cases of individual faulty systems, but are structurally related to the complexity of modern QKD implementations. As the range of functions and automation increase, so does the potential attack surface.

A key conclusion of the analysis is that security in QKD cannot be understood as an inherent property of a process/technology. Rather, it is the result of a specific implementation and continuously monitored operation. Theoretical security guarantees remain ineffective without appropriate technical and organizational measures if real systems are operated outside of idealized assumptions.

3.8.2 Typical Points of Attack and Affected System Components

Real QKD systems consist of a variety of specialized hardware and software components whose interaction enables functioning key generation. The BSI study shows that side-channel attacks typically do not target abstract protocol steps, but rather specific system elements whose physical properties, control logic, or integration requirements deviate from the idealized assumptions of the security models. The attack surface results less from individual components than from the interaction of complex integrated components and operating mechanisms.

Interface Between the Quantum World and Classical Processing

One particularly relevant area concerns the interfaces between quantum physical signal processing and subsequent classical processing. *Time and clock synchronization, trigger and gating mechanisms, signal and power monitoring,* and *digital evaluation of measurement* results form a transition area in which measured values are interpreted, filtered, and prepared for further processing.

The BSI study shows that attacks that influence *calibration and estimation processes* in these paths can lead to noise, loss, or error parameters being systematically misjudged. Such manipulations often remain within plausible operating limits and are therefore not necessarily recognized as a malfunction.

Downstream *classic processing* also represents a relevant point of attack. Implementations of parameter estimation, error correction, key compression, and authentication can unintentionally reveal information about runtime, memory, or access patterns. (See Chap. 8 Postprocessing).

In addition, the BSI study considers scenarios with *maliciously modified hardware or software components* that can leak security-relevant information via covert communication channels. Although such attacks do not affect the quantum physical processes themselves, they can completely undermine the practical security gains.

Attack Paths Close to the Sender and Receiver

A central block of the attack paths analyzed in the BSI study concerns components of real QKD systems close to the sender and receiver. On the receiver side, detector-related attack classes such as

- targeted blinding by feeding in bright light
- efficiency mismatch attacks
- time-dependent effects
- correlations due to dead times
- after-gate pulses, and
- nonlinear detector behavior

are described.

In addition, *backflash* and *breakdown flash effects* are discussed, in which optical emissions generated during the detection process can reveal information about internal states. Characteristically, these attacks exploit permissible operating states that are not covered by the idealized security model.

At the transmitter and modulator level, the study deals with *Trojan horse attacks,* in which light is deliberately fed into optical modules and reflected signals are evaluated in order to reconstruct internal settings such as modulation states or phase positions.

Closely related to this are *laser damage attacks,* in which detectors or photodiodes are deliberately damaged, or their characteristics altered in order to facilitate subsequent attacks or circumvent monitoring mechanisms.

In addition, *transmitter- and source-proximal side channels* are analyzed, in which secondary information in frequency, phase, wavelength, temporal structure, or intensity can undermine statistical assumptions of the process/technology without directly violating it.

The majority of attack vectors documented in the BSI study relate to *discrete QKD implementations (DV-QKD),* while significantly fewer specific attacks have been described for continuously variable systems to date. Entanglement-based QKD approaches, on the other hand, are hardly addressed, as they are currently only available in a few, predominantly experimental implementations and, at least at the time of completion of the BSI study in fall 2023, there was correspondingly little reliable attack literature available.

CV-QKD-Specific Attacks

For continuously variable QKD systems, the BSI study describes its own attack paths that target *calibration and reference assumptions* in particular. These include saturation attacks and manipulations of reference signals and noise estimates, which can lead to security parameters being systematically overestimated.

Random Number Generators

Another security-relevant component is random number generators, which are used for base selection, modulation, and process/technology parameters. Even with quantum-based random sources, real implementations can be influenced by

hardware-related limitations, manufacturing influences, or targeted manipulations during integration and maintenance without producing immediately noticeable deviations. The BSI has examined random number generators in separate documents and proposed a classification of these devices [BSI24].[149] (See also https://cryptography.study/phys/TRNG.)

Trusted nodes, KMS, and Operating Environment

Trusted node architectures and higher-level key management infrastructures extend the attack surface beyond individual QKD links. In such systems, key material is temporarily stored, redistributed, or re-encrypted, creating additional security-critical components and interfaces.

Practical security here depends on the entire end-to-end chain of physical protection, access control, key handling, process/technology integration, and organizational measures. Vulnerabilities in management and orchestration layers can neutralize the security gains of the underlying QKD connections without attacking the process/technology itself.

Other Vulnerabilities

Finally, the BSI's analysis makes it clear that side channels do not only arise during operation. Attack vectors during development, manufacturing, integration, and maintenance are equally relevant. The combination of high technical complexity, specialized hardware, and limited transparency favors scenarios in which vulnerabilities remain permanent and inconspicuous (see Sect. 7.2).

3.8.3 Practical Implications and Limitations of Countermeasures

Successful side-channel attacks on QKD systems do not typically manifest themselves in practice as immediate system failure or clearly recognizable security incidents. Rather, there is a gradual loss of assumed security, in which information about the generated key can leak out unnoticed. The systems often remain within specified operating parameters and continue to generate keys. The error monitoring provided in QKD systems is designed to detect disturbances in the quantum channel and does not offer any inherent mechanism for reliably detecting side-channel attacks or subsequently identifying compromised keys.

The BSI study describes a variety of countermeasures that operate at different levels. Technical hardening measures aim to make known attack paths more difficult, for example through improved optical isolation, shielding against electromagnetic radiation, robust design of sensitive components, or limiting the external signals that can be applied. In addition, surveillance and monitoring approaches are discussed that

[149] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2024.pdf.

are designed to continuously record operating parameters such as optical power, electrical signals, or temporal characteristics in order to reveal deviations from expected behavior. Furthermore, conceptual approaches are considered in which certain attack surfaces are reduced by alternative variants or system architectures, for example, by changing the distribution of security assumptions across system components.

At the same time, the study makes it clear that these measures have narrow limits. For the majority of the documented attack paths, there are several proposed countermeasures, but their effectiveness is based on different assumptions and cannot yet be evaluated comparatively or quantitatively. The BSI study explicitly points out that attack assessments were carried out independently of implemented countermeasures, as there are no reliable statements about their effectiveness. In addition, many protection mechanisms themselves require complex additional functions that introduce new sources of error, additional attack surfaces, or increased calibration and maintenance costs.

Overall, it is clear that countermeasures do not fundamentally eliminate side-channel attacks, but rather make them more difficult to exploit or address individual known attack paths. The practical security of QKD systems therefore does not result from a closed catalog of measures, but from the ongoing interaction of system design, monitoring, updating, and the consideration of new attack findings, as documented in the BSI study.

3.8.4 Consequences for the Procurement, Evaluation, and Operation of QKD Systems

The attack vectors and countermeasures documented in the BSI study show that side channels are not a one-off problem, but rather a permanent operational risk for real QKD systems. The attack surface continues to evolve with the system configuration, operating mode, and the state of attack research. Security-relevant deviations can arise without immediately manifesting themselves in malfunctions or noticeable operating parameters.

The study by the German BSI also highlights the limitations of traditional assessment tools. Certificates, laboratory tests, and manufacturer specifications inevitably refer to a defined system state and a known set of assumptions. They can document that a system meets specified requirements under certain conditions, but they do not reflect the dynamics of operation or the full spectrum of possible implementation attacks. Such evidence provides only a snapshot, especially for side channels, the exploitation of which often lies outside the modeled threat scenarios.

Against this background, characteristics that go beyond the individual product are becoming increasingly important. These include the traceability of the system architecture, the ability to analyze security-relevant components and interfaces, and

clearly defined concepts for updating, maintenance, and responding to newly identified vulnerabilities. Equally relevant are continuous monitoring mechanisms and procedures that can be used to evaluate and address conspicuous deviations.

Overall, QKD is thus classified as a security-critical special component whose benefits can only be realized in conjunction with suitable system integration and continuous operation. The results presented in the BSI study underscore that the practical security gain does not arise from the isolated consideration of individual components, but from the ongoing control of a complex, changing system.

3.8.5 Meta-Information on the BSI Study

The BSI study comprises around 250 pages and evaluates more than 300 scientific papers. A total of 49 specific attack paths with known attack sequences are described, 35 of which are specific to the currently most widely used QKD family of discrete QKD systems (DV-QKD). In addition, 9 further vulnerabilities are listed for which no complete attack path has been documented to date. Furthermore, the study identifies 18 general countermeasures and assigns them to the various attack classes.

The attack options are also evaluated in terms of the effort required, including the expertise, time, and technical resources needed. These evaluations show that many attacks require considerable skills and resources on the part of the attacker, but this does not mean that the all-clear can be given. The study makes it clear that the assessment of attacks is deliberately carried out independently of implemented countermeasures and that even complex attacks remain relevant in the context of highly secure systems as soon as the necessary skills or motivation are available. The assumption of highly capable attackers follows the established security methodology of not tying threat models to current practical limitations. Especially in the context of information that needs to be protected in the long term, the multitude of documented attack paths should therefore be understood less as a theoretical limit and more as a realistic description of the existing and growing attack surface on QKD systems.

3.9 Summary QKD

3.9.1 Fiber Optics

In the following comparison, a strict distinction must be made between peak results measured and published by research groups in one-off experimental setups under optimal conditions and values that can be achieved with commercially available equipment. In addition, information was obtained exclusively for this study from users, which paints a different picture.

Comparison of Peak Values from Research Groups

- Prepare-and-measure with continuous variables (**CV-QKD**)

  In 2022, a research group published 190.5 Mbit/s for 5 km, 137.8 Mbit/s for 10 km, and 52.5 Mbit/s for 25 km [Wang22].[150] In 2024, another group increased this record to 0.7 Gbit/s at 5 km and 0.3 Gbit/s at 10 km [Haj24].[151] However, research groups consistently report that although CV-QKD achieves significantly higher secure key rates than DV-QKD over short distances, this rate also drops much faster than with DV-QKD as the distance increases because CV-QKD is much more sensitive to a deteriorating signal-to-noise ratio. There are statements that CV-QKD can hardly be used effectively at distances of more than 30 km. Nevertheless, there are also attempts to use CV-QKD over long distances. In 2020, a research group succeeded in doing so over a distance of 202.81 km. They achieved a key rate of 6.2 bit/s [Zha20].[152]
- Prepare-and-measure with single photons (**DV-QKD**)

  In 2023, a research team reported a secure key rate of 115.8 Mbit/s at a distance of 10 km, 22.2 Mbit at 50 km, and 2.6 Mbit/s at 101 km [LiW23].[153] Another group reported 233 bit/s at 328 km, and a third group even succeeded in exchanging keys over a distance of 405 km at 6.5 bit/s.
- **With Entangled Photons**:

  Raw key rates of 151 kbit/s have already been achieved over distances of 20 km, and even at a distance of 40 km, a raw key rate of 40 kbit/s has already been achieved. In a more practical application, these raw keys would then have to be post-processed with error correction and privacy amplification, which could significantly reduce the secure key length.

  For entangled photons, experiments have already been conducted in which, at great expense, a secure key rate of 440.8 bit/s was achieved at 201 km, 1.87 bit/s at 301 km, and 0.0015 bit/s at 404 km [Zhu25][154] (corresponding to 5 bits per hour).

No information could be found on the amount of money that had to be spent to achieve these peak results. It was also not possible to find out any operating costs in this regard. However, several articles report that special detectors were used that require complex cryogenic cooling.

Especially in experiments involving long distances, glass fibers that have actually been laid between two measuring stations at this distance are not usually used. Instead, glass fiber coils supplied directly by the manufacturer of the glass fibers

[150] https://10.1038/s42005-022-00941-z.

[151] https://doi.org/10.1364/OPTICA.530080.

[152] https://doi.org/10.1103/PhysRevLett.125.010502.

[153] https://doi.org/10.1038/s41566-023-01166-4.

[154] https://doi.org/10.1103/PhysRevLett.134.230801.

are used. Although it would be possible to lay such fibers, they are left wound on the drums for the experiments. This prevents the risk of kinks or other disturbances in the fiber optic cable, which can lead to additional attenuation in fibers that are actually laid.

Comparison of Manufacturer Specifications

- **Continuous Variables (CV-QKD)**

  For CV-QKD systems in fiber optic environments, manufacturers specify key rates in the range of approximately 10 to 100 kbit/s for short to medium distances (typically 10–20 km). However, the 100 kbit/s is probably a raw key rate (after sifting; before error correction and privacy amplification).

  For longer distances of up to about 50 to 80 km, key rates in the lower kbit/s range are still specified, i.e., about 1 to 10 kbit/s.

  In this borderline range of 80 to 100 km of fiber optic cable, the explicitly stated key rates are around 1 kbit/s or less.

  According to current research, there appear to be no manufacturers offering devices with CV technology for fiber optic distances of more than 100 km.
- **Discrete Variables (DV-QKD)**

  Only a few manufacturers provide explicit specifications for short distances (10 to 20 km; or attenuations corresponding to these distances). When they do, they mention a few kbit/s, but they also like to refer to products designed purely for research purposes, specifying key rates in the range of 100 to 400 kbit/s.

  For medium distances of around 50 to 80 km, most manufacturers quote typical key rates in a range of 1 to 5 kbit/s. However, there are also high-performance variants that promise key rates of 10 to 300 kbit/s for such distances (or for the corresponding attenuations).

  For distances in the range of around 100 to 150 km, the manufacturer's specifications typically range from 150 to 1700 bit/s.

  In long-range configurations for 200 km and more, key rates of several hundred bit/s are still specified. Variants with measuring device-intensive architectures (e.g., MDI-QKD) specify key rates of more than 500 bit/s at these distances.
- **Entanglement-Based QKD**

  Over short distances of around 10 km, key rates of up to 120 kbit/s are sometimes reported. For medium distances of around 50 km, manufacturers typically report rates in the range of approximately 1.5 to 20 kbit/s.

  There is one system that can also bridge distances of up to 300 km, for which the manufacturer specifies a key rate of approximately 7 bit/s.

	Manufacturer specifications key rate fiber optic		
Distance	CV-QKD	DV-QKD	Entanglement**
10–20 km	Over 10 kbit/s	Typical: 1–20 kbit/s high-end*: 300–400 kbit/s	Approx. 120 kbit/s
50–80 km	1–10 kbit/s	Typical: Approx. 1–5 kbit/s high-end*: Approx. 18–300 kbit/s	Approx. 1.5–20 kbit/s
Approx. 100 km	Maximum range Rate below 1 kbit/s	Typical: Approx. 1.7 kbit/s	No information
Approx. 150 km	No products available	Typical: Approx. 0.5 kbit/s	No information
Approx. 200 km	No products available	High-end: Approx. 0.04–0.4 kbit/s	0.007 kbit/s

*These values are manufacturer specifications for peak configurations that are otherwise very uncommon on the market

**Due to the still low level of technological maturity and the mainly experimental use under very different conditions, the values for entanglement solutions vary greatly

Detailed manufacturer-specific reports are provided together with all source references on the book's website at.[155]

References

[WP-QKD] Wikipedia contributors, Quantum key distribution. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Quantum_key_distribution

[WP-MAC] Wikipedia contributors, Message authentication code, Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Message_authentication_code

[WP-Bit] Wikipedia contributors, Bit, Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Bit

[WP-Qbit] Wikipedia contributors, Qubit, Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Qubit

[WP-MQM] Wikipedia contributors, Measurement in quantum mechanics. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Measurement_in_quantum_mechanics

[WP-NCT] Wikipedia contributors, No-cloning theorem. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/No-cloning_theorem

[WP-QEnt] Wikipedia contributors, Quantum entanglement. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Quantum_entanglement

[WP-QSup] Wikipedia contributors, Quantum superposition. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Quantum_superposition

[WP-Unc] Wikipedia contributors, Uncertainty principle. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Uncertainty_principle

[QRep] Quantum Flagship, Quantum Repeaters, Quantum Technology (Quantum Principles; Communication), no date. https://qt.eu/quantum-principles/communication/quantum-repeaters

[Weg81] M.N. Wegman, L. Carter, New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**, 265–279 (1981). https://doi.org/10.1016/0022-0000(81)90033-7

[155] https://cryptography.study/phys/QKD.

[WP-P&M] Wikipedia contributors, Quantum key distribution; Quantum key exchange; Prepare-and-measure protocols. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Quantum_key_distribution#Quantum_key_exchange

[QSNP-DV] Quantum Secure Networks Partnership (QSNP), DV QKD, QSNP Glossary, no date. https://qsnp.eu/glossary/dv-qkd/

[WP-TRL] Wikipedia contributors, Technology readiness level; Quantum key exchange; Prepare-and-measure protocols. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Technology_readiness_level

[Sas11] M. Sasaki et al., Field test of quantum key distribution in the Tokyo QKD network. Opt. Express **19**(11), 10387–10409 (2011). https://doi.org/10.1364/OE.19.010387

[Liao17a] S.-K. Liao et al., Satellite-to-ground quantum key distribution. Nature **549**(7670), 43–47 (2017). https://doi.org/10.1038/nature23655

[QSNP-CV] Quantum Secure Networks Partnership (QSNP), CV QKD, QSNP Glossary, no date. https://qsnp.eu/glossary/cv-qkd/

[Zha24] Y. Zhang et al., Continuous-variable quantum key distribution system: Past, present, and future. Appl. Phys. Rev. **11**(1) (2024). https://doi.org/10.1063/5.0179566

[QSNP-Ent] Quantum Secure Networks Partnership (QSNP), Entanglement. QSNP Glossary, no date. https://qsnp.eu/glossary/entanglement/

[QSNP-Bell] Quantum Secure Networks Partnership (QSNP), Bell state measurement, QSNP Glossary, no date. https://qsnp.eu/glossary/bell-state-measurement/

[WP-Bell] Wikipedia contributors, Bell test. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Bell_test

[QSNP-MDI] Quantum Secure Networks Partnership (QSNP), Measurement-DI QKD. QSNP Glossary, no date. https://qsnp.eu/glossary/measurement-di-qkd/

[Ars25] Arslan, Syed M., et al., Twin-Field Quantum Key Distribution: Protocols, Security, and Open Problems. arXiv preprint https://arxiv.org/abs/2510.26320 (2025). https://doi.org/10.48550/arXiv.2510.26320

[QSNP-DI] Quantum Secure Networks Partnership (QSNP), DI QKD, QSNP Glossary, no date. https://qsnp.eu/glossary/di-qkd/

[Luo25] Luo, Xi-Yu, et al., Entangling quantum memories over 420 km in fiber. arXiv preprint https://arxiv.org/abs/2504.05660 (2025). https://doi.org/10.48550/arXiv.2504.05660

[Koz19] W. Kozlowski, S. Wehner, Towards large-scale quantum networks, in *Proceedings of the sixth annual ACM international conference on nanoscale computing and communication*, (2019). https://doi.org/10.1145/3345312.3345497

[Chen25] H.-Z. Chen et al., Implementation of carrier-grade quantum communication networks over 10000 km. NPJ Quantum Inf. **11**(1), 137 (2025). https://doi.org/10.1038/s41534-025-01089-8

[CAS17] Chinese Academy of Sciences, Beijing-Shanghai Quantum Communication Network Put into Use. (News Updates). 01 Sep 2017. https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml

[Zha18] Q. Zhang et al., Large scale quantum key distribution: Challenges and solutions. Opt. Express **26**(18), 24260–24273 (2018). https://doi.org/10.1364/OE.26.024260

[Chen21] Y.-A. Chen et al., An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature **589**(7841), 214–219 (2021). https://doi.org/10.1038/s41586-020-03093-8

[EC24] European Commission (CORDIS), Open European Quantum Key Distribution Testbed (OPENQKD)—Project fact sheet (Horizon 2020), 25 Jun 2024. https://cordis.europa.eu/project/id/857156

[EC25] European Commission, European Quantum Communication Infrastructure—EuroQCI. 8 Jul 2025. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[Peev09] M. Peev et al., The SECOQC quantum key distribution network in Vienna. New J. Phys. **11**(7), 075001 (2009). https://doi.org/10.1088/1367-2630/11/7/075001

[AIT26] AIT Austrian Institute of Technology GmbH. QCI-CAT: Quantenkommunikations-Infrastruktur für hochsichere behördliche Anwendungen in Österreich (project page), no date. https://www.ait.ac.at/themen/cyber-security/projects/qci-cat

[Stu11] D. Stucki et al., Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New J. Phys. **13**(12), 123001 (2011). https://doi.org/10.1088/1367-2630/13/12/123001

[OPT07] optics.org. Cryptography secures Swiss elections. Historical Archive, 29 Oct. 2007.; https://optics.org/article/31646

[IDQ17] ID Quantique SA. IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation (news post). 23 Nov. 2017. https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/

[Mar24] V. Martin et al., MadQCI: A heterogeneous and scalable SDN-QKD network deployed in production facilities. NPJ Quantum Inf. **10**(1), 80 (2024). https://doi.org/10.1038/s41534-024-00873-2

[BEL25] Belnet. New milestone in quantum communication project BeQCI: first cross-border QKD network established (news post). 5 Jun. 2025. https://www.belnet.be/en/news-events/news/new-milestone-quantum-communication-project-beqci-first-cross-border-qkd-network

[QUN24] QuNET. Start of the Second Key Experiment of the QuNET Initiative for Secure Quantum Communication (news post). Berlin, 19 Sep. 2024. https://qunet-initiative.de/en/news-2024/#:~:text=Start%20of%20the%20second%20key

[NICT11] National Institute of Information and Communications Technology (NICT). NICT NEWS, No. 401 (Feb. 2011): Features on: Quantum cryptography. NICT, 2011. https://www.nict.go.jp/en/pdf/copy_of_NICT_NEWS_1102_E.pdf

[Stan22] Stanley, Manoj, et al. Recent progress in quantum key distribution network deployments and standards. Journal of Physics: Conference Series. Vol. 2416. No. 1. IOP Publishing, 2022. https://doi.org/10.1088/1742-6596/2416/1/012001

[KED22] KED Global (The Korea Economic Daily Global Edition). SK Broadband applies quantum cryptography to Korea network. 9 Jun. 2022. https://www.kedglobal.com/tech%2C-media-telecom/newsView/ked202206080023

[SWNX23] Swissnex Network in Asia and Australia. nexttrends Asia Regional Report 2022: The state of quantum technologies in the APAC region: Views from Asia and Australia. Swissnex Network in Asia, 2023. https://swissnex.org/app/uploads/2023/05/Report_Epdf_290323_Final-Publish.pdf

[Ell18] C. Elliott, The DARPA quantum network, in *Quantum Communications and Cryptography*, (CRC Press, 2018), pp. 91–110. https://doi.org/10.48550/arXiv.quant-ph/0412029

[ITMO21] ITMO University News. First-Ever "Quantum Call" Between Moscow and St. Petersburg Conducted. 8 Jun. 2021. https://news.itmo.ru/en/science/cyberphysics/news/10393

[ICT21] ICT.Moscow. 7 Thousand km of Quantum Networks to be Stretched in Russia by the End of 2024 (news post). 18 Oct. 2021. https://ict.moscow/en/news/7000-km-of-quantum-networks-to-be-stretched-in-russia-by-the-end-of-2024

[ETSI19-14] European Telecommunications Standards Institute (ETSI). ETSI GS QKD 014 V1.1.1 (2019-02): Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. ETSI Group Specification, Feb. 2019. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

[EOP19] eoPortal. SpooQy-1 CubeSat Mission (Satellite Missions database entry). 17 Dec. 2019. https://www.eoportal.org/satellite-missions/spooqy-1

[NanSp] nanosats.eu. SpooQy-1 (satellite page). no date. https://www.nanosats.eu/sat/spooqy-1

[WP-Tia] Wikipedia contributors, Tiangong-2, Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Tiangong-2

[N2TG] N2YO.com. Tiangong-2, Satellite details (NORAD ID 41765/2016-057A). no date. https://www.n2yo.com/satellite/?s=41765

[Lu22] C.-Y. Lu et al., Micius quantum experiments in space. Rev. Mod. Phys. **94**(3), 035001 (2022). https://doi.org/10.1103/RevModPhys.94.035001

[Cast17] D. Castelvecchi, China's quantum satellite clears major hurdle on way to ultrasecure communications. Nature **15** (2017). https://doi.org/10.1038/nature.2017.22142

[Li25] Y. Li et al., Microsatellite-based real-time quantum key distribution. Nature, 1–8 (2025). https://doi.org/10.1038/s41586-025-08739-z

[WP-Soc] Wikipedia contributors, SOCRATES (satellite), Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/SOCRATES_(satellite)

[EOPSoc] eoPortal. SOCRATES (Space Optical Communications Research Advanced Technology Satellite) (Satellite Missions database entry). no date. https://www.eoportal.org/satellite-missions/socrates

[Tak17] H. Takenaka et al., Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. Nat. Photonics **11**(8), 502–508 (2017). https://doi.org/10.1038/nphoton.2017.107

[DLRQub] Deutsches Zentrum für Luft- und Raumfahrt (DLR), Institute of Communications and Navigation. QUBE – Satellite-based Quantum Key Distribution (project page). no date. https://www.dlr.de/en/kn/research-transfer/projects/qkd-quantum-technology-for-secure-communication/qube-satellite-based-quantum-key-distribution

[FAU25] Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). Global quantum encryption: small satellites as quantum key generators (FAU news, Research). 11 Aug. 2025. https://www.fau.eu/2025/08/news/research/global-quantum-encryption-small-satellites-as-quantum-key-generators/

[Ahn24] N. Ahmadi et al., QUICK 3 ^3-Design of a Satellite-Based Quantum Light Source for quantum communication and extended physical theory tests in space. Adv. Quantum Technol. **7**(4), 2300343 (2024). https://doi.org/10.1002/qute.202300343

[UniJ25] Friedrich-Schiller-Universität Jena; Institut für Angewandte Physik (IAP), QUICK3-Mission: Quantum Satellite with Jena Expertise Launches into Space (news post). 24 Jun. 2025. https://www.physik.uni-jena.de/en/iap/26345/quick3-mission-quantensatellit-mit-jenaer-know-how-startet-ins-all

[NanSpe] nanosats.eu. SPECTRE (QKD Cubesat) (satellite page). no date. https://www.nanosats.eu/sat/speqtre

[ISISpe] ISISPACE, SPEQTRE (project page) no date. https://www.isispace.nl/project/speqtre/

[NanImp] nanosats.eu. Impuls-1 (satellite page). no date. https://www.nanosats.eu/sat/impuls-1

[Liao18] S.-K. Liao et al., Satellite-relayed intercontinental quantum network. Phys. Rev. Lett. **120**(3), 030501 (2018). https://doi.org/10.1103/PhysRevLett.120.030501

[Khm24] A. Khmelev et al., Eurasian-scale experimental satellite-based quantum key distribution with detector efficiency mismatch analysis. Opt. Express **32**(7), 11964–11978 (2024). https://doi.org/10.1364/OE.511772

[Yin17] J. Yin et al., Satellite-based entanglement distribution over 1200 kilometers. Science **356**(6343), 1140–1144 (2017). https://doi.org/10.1126/science.aan3211

[Mil25] A. Miller, Micius, the world's first quantum communication satellite, was hackable, in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, (IEEE, 2025) https://doi.org/10.48550/arXiv.2505.06532

[Car18] A. Carrasco-Casado et al., QKD from a microsatellite: The SOTA experience, in *Quantum Information Science, Sensing, and Computation X*, vol. 10660, (SPIE, 2018) https://doi.org/10.1117/12.2309624

[LMU24] Ludwig-Maximilians-Universität München (LMU Munich), Global quantum key encryption: Nano-Satellite QUBE launches into Space (news post). 10 Jul. 2024. https://www.lmu.de/en/newsroom/news-overview/news/global-quantum-key-encryption-nano-satellite-qube-launches-into-space-66e31186.html

[QUICK3] Technische Universität München (TUM), QUICK3—QUantum phonIsChe Komponenten für sichere Kommunikation mit Kleinsatelliten (project website), no date. https://www.quick3.de/

[QZ25] Quantum Zeitgeist (Quantum News), SpeQtre Quantum Comms Satellite Launched Successfully. 1 Dec.2025. https://quantumzeitgeist.com/speqtre-quantum-quantum-comms/

[ESA1] European Space Agency (ESA). Eagle-1 (web page), no date. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1

[SES24] SES S.A. EAGLE-1: EAGLE-neXt; Advancing Europe's Leadership in Quantum Communications (newsroom page). 22 Apr. 2024. https://www.ses.com/newsroom/eagle-1-advancing-europes-leadership-quantum-communications#tab-eagle-next

[ESA19] European Space Agency (ESA), SAGA for quantum key distribution (news post), 08 Apr. 2019. https://www.esa.int/ESA_Multimedia/Images/2019/04/SAGA_for_quantum_key_distribution

[ESA2] European Space Agency (ESA), QKDSat: Secure communication via quantum cryptography (web page). no date. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/QKDSat_Secure_communication_via_quantum_cryptography

[Alv22] A. Alvaro et al., Caramuel: The future of space quantum key distribution in geo, in *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, (IEEE, 2022) https://doi.org/10.1109/ICSOS53063.2022.9749720

[Jen24] T. Jennewein et al., QEYSSat 2.0—White paper on satellite-based quantum communication missions in Canada. Can. J. Phys. **103**(4), 328–376 (2024) https://doi.org/10.48550/arXiv.2306.02481

[SPEQ] SpeQtral Pte. Ltd., Securing Global Networks in the Quantum Era. Website. no date. https://speqtralquantum.com/

[VIA25] R. Jewett, SKY Perfect JSAT Joins Quantum Cryptography Satellite R&D Project. Via Satellite (SatelliteToday.com) (2025) https://www.satellitetoday.com/technology/2025/08/28/sky-perfect-jsat-joins-quantum-cryptography-satellite-rd-project/

[Redd] Ohsin, Planned satellite for Quantum Key Distribution is called SAQTI. Reddit, r/ISRO (post). no date. https://www.reddit.com/r/ISRO/comments/1gczzq5/planned_satellite_for_quantum_key_distribution_is/

[CAS25] Chinese Academy of Sciences (CAS), Academic Divisions (CASAD). USTC Demonstrates Successful Satellite-Enabled Quantum Key Distribution (Member Activities). 24 Mar 2025. https://english.casad.cas.cn/newsroom/ma/202503/t20250325_908666.html

[CRF25] Anand, V., China's Ascent as a Quantum Space Power. Issue Brief, Chintan Research Foundation (CRF) (2025). https://www.crfindia.org/-/media/Project/ChintanResearchFoundation/Publications-PDF/19-Sep/Chinas-Ascent-as-a-Quantum-Space-Power.ashx

[TQI25] M. Swayne, China establishes quantum-secure communication links with South Africa. Quantum Insid. (2025) https://thequantuminsider.com/2025/03/14/china-established-quantum-secure-communication-links-with-south-africa/

[YIC24] Tongxin, Q., China Is Likely to Build Global Quantum Communication Network in near Future, Scholar Says. Yicai Global (Yicai). 8 Oct 2024. https://www.yicaiglobal.com/news/china-is-likely-to-build-global-quantum-communication-network-in-near-future-scholar-says

[SCM25] Xin, L, China's New Dawn: Pan Jianwei Reveals High-Orbit Quantum Satellite for Global Network. South China Morning Post (SCMP). 26 Jun 2025. https://www.scmp.com/news/china/science/article/3315963/new-dawn-pan-jianwei-reveals-high-orbit-quantum-satellite-global-network

[MER24] Jeroen Groenewegen-Lau; Antonia Hmaidi, China's long view on quantum tech has the US and EU playing catch-up. MERICS Report, Dec 2024. https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf

[JRC19] M. Travagnin, A. Lewis, Quantum key distribution in-field implementations, in *Publications Office of the European Union*, (Luxembourg, 2019). https://doi.org/10.2760/38407

[TAS18] TASS Russian News Agency. Russia to test quantum data transmission from space station in 3 years. 8 Jun. 2018. https://tass.com/science/1008731

[NSA] National Security Agency/Central Security Service (NSA/CSS), Quantum Key Distribution (QKD) and Quantum Cryptography (QC) (cybersecurity guidance web page). no date. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[NAS24] Nasser Barghouty, NASA SCaN and Space-Based Quantum Communications and Navigation: Towards A Vision (presentation). NASA Technical Reports Server (NTRS), Document ID 20240003113, acquired 13 Mar 2024. https://ntrs.nasa.gov/api/citations/20240003113/downloads/AQCF_March2024_SCaNPresentation.pdf

[NSc05] Will Knight, Quantum cryptography network gets wireless link. New Scientist (Info-Tech). 07 Jun 2005. https://www.newscientist.com/article/dn7484-quantum-cryptography-network-gets-wireless-link/

[Ion25] IonQ, Inc. IonQ Completes Acquisition of Capella Space, Advancing Vision for Space-Based Quantum Communications (press release). 15 Jul 2025. https://www.ionq.com/news/ionq-completes-acquisition-of-capella-space-advancing-vision-for-space-based

[Boe] The Boeing Company, Q4S–A quantum entanglement swapping experiment in space (web page). no date. https://www.boeing.com/space/quantum

[Fon24] Renata Fontanetto. Brazil's first quantum cryptography network is expected to connect five research institutions. Revista Pesquisa FAPESP, 342 (2024). https://revistapesquisa.fapesp.br/en/brazils-first-quantum-cryptography-network-is-expected-to-connect-five-research-institutions/

[OU23] The Open University (OpenLearn), Engineering: environmental fluids Section 1.1 The properties of the atmosphere. 12 Dec 2023. https://www.open.edu/openlearn/science-maths-technology/engineering-environmental-fluids/content-section-3.1

[Vas17] D. Vasylyev et al., Free-space quantum links under diverse weather conditions. Phys. Rev. A **96**(4), 043856 (2017). https://doi.org/10.1103/PhysRevA.96.043856

[Krz23] A. Kržič et al., Towards metropolitan free-space quantum networks. npj Quantum Inf. **9**(1), 95 (2023). https://doi.org/10.1038/s41534-023-00754-0

[Schm07] T. Schmitt-Manderbach et al., Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys. Rev. Lett. **98**(1), 010504 (2007). https://doi.org/10.1103/PhysRevLett.98.010504

[Bul23] L. Bulla et al., Nonlocal temporal interferometry for highly resilient free-space quantum communication. Phys. Rev. X **13**(2), 021001 (2023). https://doi.org/10.1103/PhysRevX.13.021001

[Zha25] P. Zhang et al., Daylight quantum key distribution over free-space optics for future security networks. J. Opt. Commun. Netw. **17**(6), B61–B70 (2025). https://doi.org/10.1364/JOCN.553171

[Ave21] M. Avesani et al., Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. **7**(1), 93 (2021). https://doi.org/10.1038/s41534-021-00421-2

[Bas23] F.B. Basset et al., Daylight entanglement-based quantum key distribution with a quantum dot source. Quantum. Sci. Technol. **8**(2), 025002 (2023). https://doi.org/10.1088/2058-9565/acae3d

[Gon18] Y.-H. Gong et al., Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror. Opt. Express **26**(15), 18897–18905 (2018). https://doi.org/10.1364/OE.26.018897

[Shen18] Shen, Shi-Yang, et al., Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent-states in urban environment. arXiv preprint https://arxiv.org/abs/1810.00408.(2018). https://doi.org/10.1103/PhysRevA.100.012325

[Liao17b] S.-K. Liao et al., Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. Nat. Photonics **11**(8), 509–513 (2017). https://doi.org/10.1038/nphoton.2017.116

[Cai24] W.-Q. Cai et al., Free-space quantum key distribution during daylight and at night. Optica **11**(5), 647–652 (2024). https://doi.org/10.1364/OPTICA.511000

[Hug02] R.J. Hughes et al., Practical free-space quantum key distribution over 10 km in daylight and at night. New J. Phys. **4**, 43 (2002). https://doi.org/10.1088/1367-2630/4/1/343

[KPa25] K-PASS, Cybersecurity research funding program, MOZART: Requirements for quantum-communication solutions for connecting the Vienna public authority network and the ZAS St. Johann. 2025. https://www.k-pass.at/en/financed-proposals/detail/mozart-requirements-for-quantum-communication-solutions-for-connecting-the-vienna-public-authority-network-and-the-zas-st-johann/

[COR25] European Commission (CORDIS), *Leap in Advancing of crItical Quantum Key Distribution-spAce Components (LaiQa). Project Fact Sheet* (Horizon Europe, 2025) https://cordis.europa.eu/project/id/101135245

[Uni25] University of Trieste, Quantum link over fibre optics inaugurated between UniTS and UniUD (news post). 14 Feb 2025. https://portale.units.it/en/news/quantum-link-over-fibre-optics-inaugurated-between-units-and-uniud

[Xue21] Y. Xue et al., Airborne quantum key distribution: A review. Chin. Opt. Lett. **19**(12), 122702 (2021). https://doi.org/10.3788/COL202119.122702

[Bou15] J.-P. Bourgoin et al., Free-space quantum key distribution to a moving receiver. Opt. Express **23**(26), 33437–33447 (2015). https://doi.org/10.1364/OE.23.033437

[Dub24] U. Dubey et al., A review on practical challenges of aerial quantum communication. Physics Open **19**, 100210 (2024). https://doi.org/10.1016/j.physo.2024.100210

[Pug17] C.J. Pugh et al., Airborne demonstration of a quantum key distribution receiver payload. Quantum Sci. Technol. **2**(2), 024009 (2017). https://doi.org/10.1088/2058-9565/aa701f

[QNu] QNu Labs., Trusted Nodes (Quantum Network Architecture) (glossary entry). no date. https://www.qnulabs.com/glossary/trusted-nodes-quantum-network-architecture

[Che21] T.-Y. Chen et al., Implementation of a 46-node quantum metropolitan area network. NPJ Quantum Inf. 7:134, 07 Sep 2021. https://doi.org/10.1038/s41534-021-00474-3

[QSNP-QR] Quantum Secure Networks Partnership (QSNP), Quantum repeater. QSNP Glossary, no date. https://qsnp.eu/glossary/quantum-repeater/

[ETSI20-04] European Telecommunications Standards Institute (ETSI), ETSI GS QKD 004 V2.1.1 (2020-08): Quantum Key Distribution (QKD); Application Interface. ETSI Group Specification (2020). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf

[ETSI22-18] European Telecommunications Standards Institute (ETSI), ETSI GS QKD 018 V1.1.1 (2022-04): Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks. ETSI Group Specification (2022). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018v010101p.pdf

[BSI23] BSI, *Implementation Attacks against QKD Systems. Study (BSI Publications—Studies)* (Bonn, Germany, 2023). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.pdf

[BSI24] BSI, A Proposal for Functionality Classes for Random Number Generators (scheme interpretation/certification guidance). 10 Sep 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2024.pdf

[Wang22] Heng Wang, et al., Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. Commun. Phys. 5, 162, 25 (2022). https://doi.org/10.1038/s42005-022-00941-z

[Haj24] A.E. Adnan, Hajomer, et al., Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver. Optica **11**(9), 1197–1204 (2024). https://doi.org/10.1364/OPTICA.530080

[Zha20] Yichen Zhang, et al., Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys. Rev. Lett., 125, 010502. 30 Jun. 2020. https://doi.org/https://doi.org/10.1103/PhysRevLett.125.010502

[LiW23] Wei Li, et al., High-rate quantum key distribution exceeding 110 Mb s−1. Nat. Photonics 17, 416–421. 13 Mar. 2023. https://doi.org/10.1038/s41566-023-01166-4

[Zhu25] Shi-Chang Zhuang, et al., Ultrabright entanglement based quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett., 134, 230801. 09 Jun. 2025. https://doi.org/10.1103/PhysRevLett.134.230801