WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Quantum-Secure Data Transmission Protocols

***Vaghani Divyeshkumar*** [a]

[a] *Gannon University, 109 University Square, Erie, PA 16541, USA*
*divyeshvaghani96@gmail.com*
DOI: https://doi.org/10.55248/gengpi.5.0624.1524

**ABSTRACT**

This paper x-rays quantum-secure data transmission protocols. Quantum cryptography relies on two fundamental principles of quantum theory; measuring a quantum state disturbs it unless it is an eigenstate of the measurement operator; and it is impossible to create an exact copy of an unknown quantum state. These principles enable secure communication by encoding information using quantum states. The BB84 protocol, the first quantum key distribution (QKD) protocol, was introduced in 1984 by Bennett and Brassard, with Wiesner presenting related ideas about a decade earlier. Another historical protocol is the Einstein-Podolsky-Rosen protocol proposed by Artur Erkert in 1991, which is thought of as an independent invention of Quantum Cryptography using a different route. Over the last two decades, there has been active research in QKD technology, resulting in significant enhancements in performance metrics like transmission distance and key rate for fiber-based QKD systems, alongside successful feasibility verification for satellite-based QKD. There remain several obstacles and challenges hindering the widespread adoption and commercialization of QKD-based QSC, which include; technology, application, standards and certification. Additionally, while experimental demonstrations of quantum key exchange have been successful over short distances, the limited range and low bit rates still pose challenges. Despite these hurdles, QC is progressively transitioning from laboratory settings to the telecommunications mainstream, offering commercialized quantum cryptography and key distribution systems.

Keywords: BB84 protocol, cryptography, Einstein-Podolsky-Rosen protocol, principles, protocol, quantum communication, quantum-key distribution (QKD), quantum theory.

## 1. Introduction

Quantum Cryptography (QC) introduces cryptographic protocols with proven unconditional security, unaffected by future technological advancements. This is a significant contrast to nearly all classical cryptography protocols (except the one-time pad), which offer only computational security based on the assumed difficulty of solving certain complex problems, for which no polynomial-time solutions are known (though not definitively proven). Although QC methods theoretically ensure security under ideal conditions, practical implementation faces security compromises due to inevitable technological limitations of the devices used (such as noisy communication channels, imperfect detectors, and elementary particle sources). Recent efforts have focused on enhancing the security bounds of QC protocols under non-ideal conditions. Encouragingly, despite not guaranteeing perfect security in an imperfect world, QC protocols can still achieve a higher level of security than classical ones. Furthermore, QC is transitioning from laboratory research to mainstream telecommunications, providing commercial quantum cryptography and key distribution systems grounded in fundamental quantum principles.

Two companies, the Swiss firm id Quantique and the American company MagiQ, were pioneers in bringing this technology to the market (id Quantique, 2024; MagiQ, 2024). Recently, Austrian scientists executed the world's first bank transfer encoded via quantum cryptography (FibreSystems, 2004). The intrinsic security benefits of QC attract customers seeking enhanced security beyond their current solutions, found in quantum key distribution.

The advancements in producing, manipulating, and measuring quantum states at the sub-atomic level have accelerated the development of innovative applications for acquiring, processing, and transmitting information (Martin et al., 2021). Quantum information technology surpasses the limitations of classical information technology, offering significant improvements in computational power, network security, and measurement accuracy (Deutsch, 2020). Today, quantum information science and technology, encompassing quantum computing, quantum communication, and quantum sensing, is a global focal point in the high-tech industry (NSTC, 2018; European Quantum Flagship, 2022).

Quantum communication, which utilizes quantum superposition or entanglement effects for state transmission or key distribution, ensures information-theoretic security (ITS) at the protocol level, with the aid of classical communication (Gisin, 2007). This field includes diverse protocols and applications such as quantum teleportation (Bouwmeester et al., 1997), quantum key distribution (QKD) (Bennett & Brassard, 2014), quantum secret sharing (Hillery & Buzek, 1999), quantum dense coding (Mattle et al., 1996), and quantum secure direct communication (Long et al., 2007). The development of the quantum information network, or quantum Internet (Kimble, 2008), relies on quantum teleportation, memory, and relay, representing a significant research

focus, though practical deployment remains distant. Over the past decades, quantum secure communication (QSC) using QKD for pre-shared keys in ICT systems and networks, often combined with symmetric encryption, has entered industrial practice (Martin et al., 2017).

The primary motivation for adopting QKD-based QSC in industry is to counteract potential security threats posed by quantum computing. Quantum computers capable of running Shor's algorithm, expected around 2033 (Vermeer & Peet, 2020), could break current public-key cryptography mechanisms like RSA and ECDH. Consequently, efforts to standardize and transition to post-quantum cryptography (PQC), which aims to withstand quantum computing threats, have advanced (Alagic et al., 2022). Compared to PQC, QKD protocols offer the distinct advantage of generating symmetric keys between remote locations with ITS guaranteed by quantum mechanics (Renner et al., 2005). QKD-based QSC ensures the security of symmetric key establishment, immune to degradation over time, and allows for more frequent key updates, thereby enhancing the overall security of encryption applications.

As one of the most impactful and practical quantum information technologies, QKD-based QSC has seen significant progress in scientific research, application exploration, and industrial development over the past decade. Several national quantum science and technology strategies have recognized the QKD network as the foundational step towards realizing the future quantum Internet (Wehner et al., 2018), taking advantage of its capabilities for ensuring network information security (Nicholas et al., 2020; Lewis & Travagnin, 2022). Numerous novel QKD protocols and implementations have been continuously optimized, resulting in significant advancements in system performance, such as extended maximum transmission distances and increased secure key rates (Wang et al., 2022; Yuan et al., 2018). The integration and flexible networking of QKD with ICT systems and networks have also been explored (Aguado et al., 2019). Various QKD systems and encryption solutions have been commercialized by numerous vendors and service providers (FG-QIT4N, 2021). Many countries and regions worldwide have undertaken QKD network construction and demonstration projects, primarily supported by public R&D funds (Lewis & Travagnin, 2019). The ongoing innovation, application exploration, and commercialization efforts underscore the significance of QKD-based QSC technology in the emerging quantum era, gaining widespread recognition and value from governments, academia, and industry.

### *1.1 The Need for Quantum Cryptography*

"Cryptography is about communicating in the presence of an adversary" (Goldwasser & Bellare, 1996). Modern cryptography relies on the principle that the security of a cryptographic method (algorithm) does not need to depend on keeping the method itself secret. In fact, the algorithm used for cryptographic purposes is typically required to be publicly known. What remains secret is a short message (the 'key') shared among valid users and inaccessible to an invalid one. Discrete mathematics, group theory, and function theory have enabled a wide array of cryptographic tasks such as encryption, message authentication, digital signatures, and secure electronic transactions based on this principle.

No cryptographic method is known to be provably secure against an adversary with unlimited computational resources. The sole exception is the "one-time pad" encryption method, which encrypts a binary message by XORing each bit with a random bit sequence (the key) shared by all valid users. New messages are encrypted with different random bit sequences. This method ensures that the probability of an adversary obtaining the correct message from the encrypted text (cipher-text) decreases exponentially with the message (and key) bit size. However, the "one-time pad" is impractical for most real-life applications: Firstly, the key must be as long as the total length of all messages to be exchanged. Secondly, even a slight discrepancy between the key sequences used by the sender and receiver would result in incorrectly decoded messages. Thirdly, valid users must share the exact same key, raising the challenge of securely distributing this (long) key among distant users.

This key distribution issue is a security problem inherent in all protocols based on symmetrical encryption algorithms. The "public-key" cryptographic methods, a revolutionary modern cryptography discovery, remain the most widely used classical solution to the key distribution problem. These methods also serve other applications, such as digital signatures, authentication, and bit-commitment. However, their security is only computational; it is based on the current inability to solve certain 'hard' mathematical problems, like the factorization of a very large integer, in polynomial time. Yet, it has not been proven that a classical polynomial-time algorithm for these problems does not exist. A sudden mathematical breakthrough revealing such an algorithm would cause all systems based on these methods to collapse overnight. This concern was amplified when Shor published an algorithm in 1994 that, using a quantum computer, can provably factorize large integers in polynomial time (Shor, 1994). A direct proof that there are decision problems in NP (problems whose solutions can be verified in polynomial time) that are not in P (problems whose solutions can be found and verified in polynomial time) does not exist; currently, it is known that $P \subseteq NP$. However, even if such a proof is found, the threat from the potential realization of a quantum computer will persist.

## 2. Literature Review

### *2.1 Quantum Cryptography Principles and the BB84 Protocol*

Quantum cryptography relies on two fundamental principles of quantum theory:

- Measuring a quantum state disturbs it unless it is an eigenstate of the measurement operator.
- It is impossible to create an exact copy of an unknown quantum state (Wotters & Zurek, 1982).

These principles enable secure communication by encoding information using quantum states. For instance, Alice (the sender) wants to send a message M to Bob (the recipient) while Eve (the eavesdropper) attempts to intercept it. Alice can encode the binary message as a sequence of two distinct quantum states, ψ1 and ψ2, such as two different polarization states of photons, and send them through a classical communication channel. If Eve intercepts and measures the states, she will disturb them due to principle (1), which Alice and Bob can later detect. Additionally, Eve cannot copy the states for later measurement due to principle (2). It is crucial that ψ1 and ψ2 are non-orthogonal to ensure that Eve's measurement disturbs the states.

The BB84 protocol, the first quantum key distribution (QKD) protocol, was introduced in 1984 by Bennett and Brassard, with Wiesner presenting related ideas about a decade earlier. The steps of the BB84 protocol are as follows:

Alice generates a random bit string and encodes it using two pairs of orthogonal quantum states: ψ11, ψ12 (ψ11·ψ12=0) and ψ21, ψ22 (ψ21·ψ22=0). States within each pair are orthogonal, while states from different pairs are non-orthogonal. For example, ψ11 and ψ12 could be the left-right polarization states, and ψ21 and ψ22 the +45° and -45° polarization states. Each bit is randomly encoded into one of these four states and sent to Bob.

Bob measures each state, randomly choosing between the two bases with a different random number generator. If Bob chooses the same basis as Alice for a bit, he will measure the same state Alice sent. If he chooses a different basis, he will get uncorrelated results 50% of the time, resulting in a 25% error rate in the bit string he obtains.

To correct this error rate, Alice and Bob publicly announce the bases they used for each bit without revealing the measurement results. They discard bits where different bases were used, keeping only those where the bases matched, resulting in a final bit sequence that is 50% of the original size and agreed upon by both. This sequence can be used as a secret key in symmetric encryption schemes like DES or for "one-time pad" communications.

Eve cannot copy the sequence, and upon interception, she must resend something to Bob. The best she can do is measure each bit and send a photon prepared in the state she measured. Eve has a 50% chance of sending the correct state, which means in 50% of the cases, Bob and Alice won't detect her. However, in the remaining 50%, Eve will choose a different basis, introducing an extra error of 25% in Bob's sequence after Alice and Bob compare bases. This additional error will reveal Eve's intervention, prompting Alice and Bob to abort communication.

#### *2.1.1 Quantum Secure Communications under Non-Ideal Conditions: Privacy Amplification and Error Correction*

It should be noted that the BB84 protocol, and indeed all of quantum cryptography (QC) until 2003, focused exclusively on secure key distribution. At the conclusion of the protocol, the sender and receiver share a random secret key. This means no predetermined messages can be communicated this way. Therefore, QC might more accurately be called QKD (Quantum Key Distribution). However, after 2003, new protocols emerged that also address secure message encryption and bit commitment. The BB84 protocol can be proven to be unconditionally secure under ideal conditions, as any intervention by an eavesdropper (Eve) is detectable over sufficiently long bit sequences, albeit possibly reducing the secret key size. Ideal conditions entail:

**Perfect Single Photon Sources**: The sender (Alice) needs to generate and transmit single photons in a specific quantum state. In reality, multiple photons might be produced in the same state, allowing Eve to retain one copy for herself.

**Perfect Communications Channel**: The channel must be (i) lossless, meaning all photons sent by Alice should be received by Bob, and (ii) decoherence-free, meaning the quantum states of individual photons should remain unaltered during transmission. In practice, noisy channels may cause photon loss (leading to errors Bob must correct) or state changes due to interaction with the transmission medium, increasing the final key error rate. While photon state changes are minimal in air (as polarization remains stable), they pose a significant problem in optical fibers, which are dispersive, especially over long distances.

**Perfect Photon Detectors**: On Bob's side, photon detectors should fire only upon receiving a photon. However, semiconductor-based detectors may sometimes fire without an actual incoming photon, resulting in dark counts. These can be security threats because, when combined with genuine photon losses, they can be mistaken for intercepted photons by Eve.

These issues can greatly compromise the protocol's security and fidelity. However, it is crucial to recognize that these are technological problems rather than inherent flaws in the quantum protocol itself. A significant part of QC research focuses on developing methods to ensure security even under non-ideal conditions.

In this section, we examine the security challenges posed by noisy communication channels and how the BB84 protocol addresses them. A noisy channel increases the error rate in the bit string Bob receives after step 2. If the additional error rate is ε%, and assuming Eve intercepts and measures only 4ε% of the signal Alice sends, Eve could ultimately acquire 2ε% of the information from the signal, resulting in an additional ε% error after Alice and Bob complete step 3. However, Bob cannot distinguish whether this error is due to eavesdropping or channel noise. To resolve this, Alice and Bob must measure the channel's error rate to detect any statistical deviations.

Alice and Bob can then perform additional steps to reduce Eve's information about the key to zero, at the cost of shortening the key. This process, known as privacy amplification (Bennett, Brassard & Robert, 1988; Bennett, Brassard, Crepeau & Maurer, 1995), is effective only if Eve initially has less information about the key than Bob (Gisin, Ribordy, Tittel & Zbinden, 2002). To determine if this condition holds, Alice and Bob publicly announce a random subset of their bits after step 3 and compare the results to estimate the error rate. They estimate the joint probability distribution P(a,b) of the random variables a and b, representing the bits of the keys Alice and Bob hold, respectively. They then calculate the mutual information I(a,b) shared by Alice and Bob and I(a,ε) between Bob and Eve. They discard the bits they publicly announced.

If the condition I(a,ε)<I(a,b)I(a,ε) < I(a,b)I(a,ε)<I(a,b) is not satisfied, they abort the protocol. Otherwise, they proceed with classical error correction techniques to correct all errors and reduce Eve's information to zero (privacy amplification). This condition ensures that Eve has less information about the sifted key than Bob, making privacy amplification effective.

One such technique involves the following steps:

a) **Error correction**: Alice selects pairs of bits and announces their XOR value (sum modulo 2). If Bob gets the same XOR, he replies 'accept'; otherwise, he says 'reject'. In the 'accept' case, they both keep the first bit and discard the second; in the 'reject' case, they discard both bits. After this step, Alice and Bob have identical but shorter keys.

b) **Privacy amplification**: To further reduce Eve's potential information, Alice randomly chooses pairs of bits and computes their XOR value, announcing only which pairs she chose. Both Alice and Bob then replace the two bits with their XOR value. This results in an even shorter but error-free key, while significantly reducing Eve's information to an arbitrarily small value. For example, if Eve knows the first bit but nothing about the second, she has no information about their XOR. If she knows both bits with 60% probability, she knows their XOR with only $(60\%)^2 + (40\%)^2 = 52\%$ probability. More efficient algorithms than this basic example are typically used in practice (e.g., Brassard & Salvail, 1994).

### *2.1.2 Einstein-Podolsky-Rosen protocol*

Another historical protocol is the Einstein-Podolsky-Rosen protocol proposed by Artur Erkert in 1991 (Ekert, 1991), which is thought of as an independent invention of Quantum Cryptography using a different route. According to this protocol, the random bit sequence is generated by a common trusted source. Each bit is encoded by a pair of maximally *entangled* photons, one sent to Alice and the other to Bob. The security of this protocol is based on the violation of Bell's inequalities, i.e. of the inability to reproduce measurement results on entangled quantum states by any classical local theory. More specifically, in the original Ekert protocol two photons are prepared by the common source in a maximally entangled state like

$$\varphi = \frac{1}{\sqrt{2}}\left(\left|\uparrow\uparrow\right\rangle - \left|\downarrow\downarrow\right\rangle\right) \quad (1)$$

(singlet state) one photon is sent to Alice and one to Bob. Then, Alice and Bob each choose (randomly) among three different bases to measure the polarization of their respective photon. Two of these bases have common orientations between Alice and Bob and the third base is oriented differently. After all measurements are finished, Alice and Bob publicly reveal the bases on which they measured each photon. Thus, they can group all measurements into two groups: a) pairs of entangled photons measured by the *same* basis and b) pairs of entangled photons measured on a different base. Subsequently, Alice and Bob publicly announce the particular results of their measurements that belong to group (b) only. From these results they can calculate a quantity that depends on the correlations between results of measurements on different bases (for details see (Ekert, 1991)), for which quantum mechanics predicts a specific value, provided that the initial state of each pair of photons is entangled. If this value comes up, then Alice and Bob safely conclude that their initial pairs are undisturbed (eg. by an Eavesdropper), and then keep the results of the measurements of photons belonging to group (a). These measurements will certainly be perfectly *anti*correlated, thus Alice and Bob are sure to share the same random bit sequence. Now, if Eve tries to tamper the protocol, she can only intercept one photon in each pair, measure it and then resend to the other party (Alice or Bob) a photon prepared in the same state. However, by this strategy Eve destroys the entanglement in the original pair, a fact that will be detected later when Alice and Bob compute the correlations of measurements on group (b).

### *2.1.3 Other Implementations of Quantum Secure Communications*

Privacy amplification can still be achieved even if condition (1) is not met, assuming the protocol involves two-way communication between Alice and Bob (where Bob also sends signals back to Alice) (Maurer, 1993; Maurer & Wolf, 1999).

While the BB84 protocol uses a four-state quantum system, QKD can also be implemented with a two-state system (Bennett, 1992). There is also a six-state protocol that offers better accuracy and security than the two- and four-state protocols (Bruss, 1998; Bechmann-Pasquinnucci & Gisin, 1999).

Furthermore, there are different methods of encoding information in quantum systems. Instead of using photon polarization, bits can be encoded using the phase difference between photons (Bennett, 1992; Gisin, et al., 2002), which can be accurately measured with an interferometer. Variations of phase coding methods have also been proposed (e.g., Sun, et al., 1995; Mazurenko, et al., 1997; Merolla, et al., 1999).

### *2.2 Methods of Attack and Ultimate Security Proofs in Quantum Secure Communications*

Additional security compromises in practical QKD implementations include multiple photon sources and faulty detectors. The security proof for QKD with perfect apparatus and noise-free channels is straightforward. Even with perfect apparatus, conditional security can be proven in the case of noisy channels, with the only limitation being the error rate of the channel. Theoretical upper bounds to the error rate due to noisy channels, consistent with condition (1) for one-way communication, can be obtained. With two-way communication, these bounds are relaxed. It has been demonstrated (e.g., in Gisin, et al., 2002) that the privacy amplification technique reduces Eve's information to zero if the Quantum Bit Error Rate (QBER) is less than QBER%. QBER is the ratio of remaining wrong bits to the total number of bits received by Bob in the sifted key. In the case of two-way communication, this bound may increase to 30% (Gisin & Wolf, 2000; Gisin & Wolf, 1999). Equation (3) applies only when Eve performs single-qubit attacks. However, the

possibility exists for collective attacks on more than one qubit, known as coherent or joint attacks. The extent of the advantage Eve gains under these attacks is still uncertain, but an upper bound for security can be calculated, assuming perfect apparatus, yielding a maximum QBER of about 11%.

However, sources of error besides the communication channel provide Eve with advantages. For instance, if Alice's photon source produces multiple photon pulses encoding the same qubit in the same quantum state, Eve may keep one photon and send the others to Bob. In single photon pulses, Eve keeps the copy and sends nothing to Bob. If Eve uses a more efficient communication channel than Alice, Bob may not detect the reduction in incoming qubit rate, attributing it to channel loss instead. Additionally, if the 'dark count' rate of Bob's faulty detectors equals channel losses, Eve may obtain full information without detection. Eve must measure the number of photons in a multiple photon pulse without disturbing the qubits, which is theoretically possible through quantum nondemolition measurements. Present technology does not allow for such measurements, but they are foreseeable in the future. This possibility has garnered attention in recent literature as it presents realistic eavesdropping scenarios. The debate remains unsettled. Gisin argues that the assumption of Eve possessing unlimited technological power is unrealistic. For instance, to carry out a quantum non-demolition attack, Eve would need nearly perfect non-demolition experiments, maintain the quantum state of intercepted qubits until Alice and Bob reveal their bases, and use a more efficient communication channel than Alice and Bob. This last requirement is optimistic for Eve, as the efficiency of communication channels is limited by physical rather than technological reasons, according to Gisin. Therefore, Eve cannot be expected to outperform Alice and Bob in practice.

The discussion in this section highlights that ultimate proofs of QC security demand ideal technological conditions for Eve, an unrealistic assumption given non-ideal conditions for Alice and Bob. Ultimate proofs must be differentiated from practical ones, where technological limitations on Eve are also considered.

Recently, a more 'realistic' class of attacks on QC protocols, such as the beam-splitter attack, has been proposed (Dusek, et al., 2000; Lutkenhaus, 2000; Feliz, et al., 2001). In this attack, Eve splits all pulses in two, analyzing each half in one of the two bases with photon-counting devices that can distinguish between pulses with 0, 1, and 2 photons. This requires nearly perfect detectors but does not assume completely out-of-reach technology. When Eve detects two photons in the same output, she sends a photon in the corresponding state to Bob; otherwise, she sends nothing. An analysis of Eve's information gain shows that she can undetectably obtain twice as much information on the signal compared to a simple intercept-resend strategy (Gisin, et al., 2002). Practical solutions to limit Eve's information exist, albeit at the cost of reducing the transmitted bit rate, forcing Eve to attack smaller portions of the signal to remain undetected.

Ultimately, multi-photon pulses do not threaten security as countermeasures can limit Eve's advantage to arbitrarily small amounts, though at the cost of lowering the achieved secret bit rate. Despite QC's theoretical security based on quantum principles, technological implementation remains questionable. Thus, the relationship presented by Gisin et al., 2002:

Infinite security ⇒ infinite cost ⇒ zero practical interest

is highly relevant for QC systems. So, why prefer QC over classical methods? There are compelling reasons: (i) "It is much easier to forecast progress in technology than mathematics" (Gisin, et al., 2002). The likelihood of a mathematical breakthrough rendering all classical public-key cryptography obsolete overnight is negligible for QC, as its security depends only on technological limitations. (ii) QC security depends on the adversary's technology at the protocol's realization. In classical cryptography, an enemy can 'store' a secret until future technological advances break the encoding, which is impossible with quantum-encoded information. This point is particularly relevant for secrets whose value endures over long periods.

### *2.3 QKD Technology Research Advances*

Quantum Key Distribution (QKD) is crucial in Quantum Secure Communication (QSC) systems, enabling symmetric key sharing. The performance, reliability, and practical security of QKD systems are key factors determining the feasibility of large-scale deployment and application of QSC (Xu et al., 2020). Continuous advancements in QKD technology are essential for the commercial application and industrial development of QSC.

#### *2.3.1 System Performance Enhancement*

QKD systems can be based on various protocols, each with unique strengths and limitations. Entanglement protocol-based QKD (Ekert, 1991), which relies on generating and transmitting entangled photon pairs, has limited system performance due to current technological constraints on entanglement yield and fidelity. However, it is highly compatible with future quantum Internet architecture.

Research and application efforts are more focused on preparation-measurement protocol-based QKD, which can be implemented using discrete variables (DV) or continuous variables (CV). Quantum state encoding in these systems can utilize different degrees of freedom of optical signals, such as polarization (Peng et al., 2007), phase (Hiroki et al., 2008), position, and phase difference between adjacent pulses (Bacco et al., 2016). The key rate of a typical point-to-point preparation-measurement QKD system depends on transmission efficiency. Due to the inherent loss limitations of optical fiber channels, it is challenging to exceed a single-span 500 km fiber transmission limit (Boaron et al., 2018). Additionally, imperfections in receiver-side detectors can introduce side-channel security vulnerabilities, posing risks to the practical security of preparation-measurement QKD systems.

Since 2018, the twin-field (TF) QKD protocol has gained significant attention (Lucamarini et al., 2018). This protocol uses a dual-end preparation and center measurement architecture, eliminating all detector side-channel vulnerabilities and increasing the theoretical secure key rate related to the square root of transmission efficiency, thus breaking the PLOB boundary of quantum channel capacity (Minder et al., 2019). With improvements in theories and protocols like the sending-or-not-sending (SNS) protocol (Wang et al., 2018), the two-way classical communication (TWCC) method (Xu et al., 2020),

and the active odd-parity pairing method (Jiang et al., 2019), TF-QKD has become a widely recognized next-generation solution for long-range, high-security QKD. A non-exhaustive list of recent significant QKD experiments is shown in Table 1.

**Table 1.** Typical QKD experiments and their performance.

| Protocol | Channel | Distance or Loss | Key Rate (bps) | Year | Reference |
|---|---|---|---|---|---|
| Modified BB84 | Lab fiber | 421 km | 6.5 | 2018 | (Boaron, et al., 2018) |
| Twin-field | Lab fiber | 90.8 dB | 0.045 | 2019 | (Minder, et al., 2019) |
| Twin-field | Lab fiber | 502 km | 0.118 | 2020 | (Fang, et al., 2020) |
| Twin-field | Lab fiber | 509 km | 0.269 | 2020 | (Chen, et al., 2020) |
| Twin-field | Lab fiber | 605 km | 0.97 | 2021 | (Pittaluga, et al., 2021) |
| Twin-field | Field Trial | 511 km | 3.45 | 2021 | (Chen, et al., 2021) |
| Twin-field | Lab fiber | 658 km | 0.092 | 2022 | (Chen, et al., 2022 |
| Twin-field | Lab fiber | 830 km | 0.014 | 2022 | (Wang, et al., 2022) |

In a recent breakthrough experiment, a team from USTC employed an enhanced four-phase twin-field protocol, incorporating independent source phase-locking, channel phase compensation, and high SNR single-photon detection and screening, to push the transmission distance limit of a repeater-less QKD system to 830 km (Wang et al., 2022). However, it is important to note that typical TF-QKD systems necessitate photon-level interference control between long-distance independent lasers, which demands stringent light source frequency locking and channel fluctuation compensation. The TF-QKD system remains under development in the laboratory, with no commercial products or implementation solutions yet available.

To further boost the key rate and performance of QKD systems, various multiplexing techniques such as time division multiplexing (TDM), wavelength division multiplexing (WDM), and space division multiplexing (SDM) could be used to enable parallel transmission of multiple QKD channels. Although time multiplexing based on optical path switching introduces minimal channel loss, the redundancy of the QKD system can ensure the point-to-point key rate (Aguado et al., 2017). Multi-wavelength WDM (Eriksson et al., 2020) or SDM using multi-core or few-mode fibers (Xavier et al., 2020) could allow QKD systems to transmit in parallel within the same fiber, thus improving the final key rate.

Unlike DV-QKD protocols that employ weakly coherent pulsed quasi-single photons for quantum state encoding, CV-QKD protocols generally use two-dimensional Gaussian modulation (GM) of quantum coherent states (Laudenback et al., 2018). CV-QKD systems can leverage conventional optical communication components like IQ modulators and coherent detectors, which are more advantageous for miniaturization and cost reduction. Additionally, CV-QKD can achieve a high security key rate of Mbps over transmission distances of tens of kilometers, making it a promising technology for metro-area QKD solutions.

After two decades of advancements, CV-QKD protocols have primarily concentrated on GG02 (Grosshan & Grangier, 2002), NoSwitching (Weedbrook et al., 2004), and discrete modulation (Leverrier & Grangier, 2009), with the security of these protocols now established (Jain et al., 2022). The system architecture has progressed from transmitting local-oscillation to local local-oscillation and discrete digital modulation systems. In 2022, the ISC team achieved a 21.53 Mbps secure key rate over 25 km using a single-carrier four-state discrete digital modulation CVQKD system (Wang et al., 2022), and a probabilistic shaping 256 QAM discrete modulation and digital coherent demodulation CV-QKD system achieved a 9.193 Mbps secure key rate over 50 km (Pan et al., 2022). Although the hardware for discrete digital modulation CV-QKD systems is relatively simple, they depend on high-performance DSP for coherent demodulation, signal compensation, and high-throughput post-processing. Currently, these systems remain in the laboratory development stage, with no widespread commercial products available.

High-dimensional QKD, leveraging the benefits of high-dimensional quantum states (qudits) such as increased information capacity and noise resilience, has emerged as a significant research focus (Cozzolino et al., 2019). Qudit state preparation and QKD using various degrees of freedom like OAM, time, frequency, and time-bin have been demonstrated in various scenarios (Erhard et al., 2020), including fiber optic channels (Vagniluca et al., 2020), multimode and multicore fibers, free-space channels (Steinlechner et al., 2017), and underwater channels (Bouchard et al., 2018). Experiments on high-dimensional encoding within the MDI-QKD protocol have also been validated (Sekga et al., 2023). Nonetheless, the generation and control of qudits still face theoretical and experimental challenges, and the reliance on devices and channels such as integrated photonics and multicore/multimode fibers presents practical application challenges for high-dimensional QKD.

### *2.3.2 Satellite-Based QKD Experiments*

Satellite platforms for satellite-ground quantum communication and QKD offer distinct advantages for both scientific research and practical applications (Lu et al., 2022). As QKD terminals, satellites can greatly extend transmission distances. The loss for a low earth orbit (LEO) satellite to ground downlink channel is about 40-50 dB, significantly lower—by more than 10 orders of magnitude—than that of fiber channel loss over the same distance (Wang et

al., 2013). Before quantum storage and quantum relays become practical, satellite platforms remain the only method to achieve quantum communication over thousands of kilometers. Additionally, satellites can serve as QKD relay nodes, enabling on-demand networking with ground stations worldwide. This capability offers benefits in mobility, coverage, and survivability, thereby enhancing the security of the QKD relay function.

Recently, various countries and regions have initiated and funded projects for satellite quantum communication and QKD research and applications. Canada's QEYSSat project, which received significant investment, partnered with Honeywell to develop an earth-to-satellite quantum communication uplink, featuring a ground-based quantum source and miniaturized satellite receivers (Pugh et al., 2017). The CubeSat-based Quantum Communication Mission (CQuCoM), a collaboration between the National University of Singapore and several other institutions, utilized the CubeSat platform deployed from the International Space Station for entangled photon transmission and QKD experiments. This project demonstrated a high-performance light source and pointing mechanism to establish satellite-to-ground entangled distribution, aiming to lay the groundwork for a quantum constellation of LEO trusted relays (Oi et al., 2017). The University of Grenoble in France proposed the Nanobob nano-satellite program to realize an uplink configuration for ground-to-satellite quantum communication, conducting research on precise clock synchronization among other aspects (Kerstel et al., 2018).

In 2016, a collaboration between various research institutions launched the first quantum science experiment satellite, Micius, conducting several pioneering space quantum communication experiments over the next six years. The main technical achievements of Micius are detailed in Table 2.

**Table 2.** Micius quantum science satellite experiments.

| Experiment | Achievement | Year | Reference |
|---|---|---|---|
| Quantum Key Distribution | 1200 km satellite-to-ground QKD (1.1 kbps key rate) | 2017 | (Liao, et al., 2017) |
| | 1000 km satellite-to-ground entanglement-based QKD (3.5 bps key rate) | 2017 | (Yin, et al., 2017) |
| | 7600 km apart ground stations satellite relay QKD and encryption demonstration (key volume 100 KB) | 2018 | (Liao, et al., 2018) |
| | 1120 km apart ground stations entanglement-based QKD (0.12 kbps key rate) | 2020 | (Yin, et al., 2020) |
| | Increasing key rate 40 times in satellite-ground QKD (47.8 kbps key rate) | 2021 | (Chen, et al., 2021) |
| Quantum Teleportation | 1200 km apart ground stations entanglement distribution (0.869 fidelity) | 2017 | (Yin, et al., 2017) |
| | 1400 km ground-to-satellite quantum teleportation (0.80 fidelity) | 2017 | (Ren, et al., 2017) |
| | 1200 km apart ground stations quantum state transfer (0.82 fidelity) | 2022 | (Li, et al., 2022) |
| Quantum Physics | Experimental of gravitationally induced quantum decoherence model | 2019 | (Xu, et al., 2019) |
| | Satellite-to-ground quantum-secure time transfer (9 kHz time data rate, and 30 ps transfer precision) | 2020 | (Dai, et al., 2020) |

It is important to recognize that satellite-based quantum communications and QKD involve addressing numerous engineering challenges such as satellite acquisition, tracking and pointing (ATP), real-time channel compensation, and satellite-ground synchronization. Additionally, these systems must meet requirements for weather conditions, around-the-clock operation, and reliable maintenance. For instance, due to limitations from daylight background noise and its orbital altitude, the Micius satellite could only transmit quantum state signals to ground stations within a brief window (a few minutes each day) on clear nights. Future improvements might include using a 1550 nm wavelength source combined with up-conversion detectors, which could enhance detection efficiency and enable daytime operation.

## 3. Exploration of QSC Applications

In the past ten years, the maturation of QKD technology has led to widespread construction of QKD trial networks and exploration of QKD-based QSC applications in various countries and regions worldwide (Aguado et al., 2019; Sasaki et al., 2011; Peters et al., 2022). The US has made significant strides in QKD-based QSC application development, including the integration of quantum encryption with various ICT protocols and systems, building QKD networks, and demonstrating QSC applications using QKD satellites.

### *3.1. Integration of Quantum Encryption and ICT Systems*

Key exchange mechanisms (KEM), digital signatures (DS), and authentication mechanisms in public key cryptography—such as RSA and ECC—and symmetric encryption algorithms like AES, ensure the integrity, non-repudiation, and confidentiality of information (Joshi & Singh, 2017). To counter the security threats posed by quantum computing to current public-key cryptography, quantum encryption utilizing QKD and/or quantum random number generators (QRNG), along with new key exchange mechanisms and digital signature algorithms in post-quantum cryptography (PQC), can be incorporated into ICT systems and networks in various ways, as illustrated in Table 3.

**Table 3:** Quantum encryption and ICT systems integration

| **Solution** | **Entropy Source** | **Key Establishment** | **Digital Signature** | **Encryption** |
|---|---|---|---|---|
| Current | CSPRNG * | ECDH (SM2 **) | RSA (SM2) | AES (SM4 **) |
| PQC | CSPRNG | PQC KEM *** | PQC DS **** | AES (SM4) |
| QRNG + PQC | QRNG | PQC KEM | PQC DS | AES (SM4) |
| QKD-based QSC | CSPRNG or QRNG | QKD | RSA (SM2) or Pre-shared Key | AES (SM4) |
| QRNG + QKD + PQC | QRNG | QKD | PQC DS | AES (SM4) |
| ITS Encryption | QRNG | QKD | Pre-shared Key | OTP |

* CSPRNG: Cryptographically secure pseudo-random number generator. ** SM2/SM4: Commercial cryptographic algorithms standard in the market. *** PQC KEM: CRYSTALS-KYBER, BIKE, Classic McEliece, HQC, SIKE (Alagic, et al., 2022). **** PQC DS: CRYSTALS-Dilithium, FALCON, SPHINCS+ (Alagic, et al., 2022).

Cryptographically secure pseudo-random number generators (CSPRNGs) are widely used as entropy sources for various algorithms. Enhancing randomness and performance can be achieved by integrating a quantum random number generator (QRNG) as an entropy source or combining its output with a PRNG (Jacak et al., 2021).

With the advent of large-scale quantum computers, current KEM and DS methods based on factoring, discrete logarithms, and elliptic curve cryptography will be vulnerable. However, symmetric cryptographic methods like AES and hash functions will be less affected (Yunakovsky et al., 2021). ISO and industry are actively working on upgrading KEM and DS to post-quantum cryptography (PQC) to mitigate this risk. It's important to note that transitioning to PQC requires secure algorithm standards, reliable commercial products, and considerations of algorithm performance, implementation ease, and compliance. Updating numerous ICT system devices to PQC will be a lengthy process (Joseph et al., 2022).

In high-security scenarios with available fiber resources, QKD offers a new ITS solution for KEM. A typical QSC use case involves using QKD systems or networks to provide symmetric keys for encryption. Here, the QKD-generated quantum key or relay key from the QKD network is used by the encryptor as real-time updatable key primitives in symmetric encryption, enhancing overall security. However, QKD only addresses KEM; DS and authentication still rely on current encryption algorithms or PQC. Given the limited secure key rate, QKD keys are often used as primitives in symmetric encryption algorithms like AES and are involved in session key generation (Mohammed et al., 2014).

Challenges in commercializing and promoting QKD include the need for fiber resources, deployment, calibration, hardware maintenance, and system sensitivity to environmental factors like fiber and equipment vibrations and temperature fluctuations.

To achieve ITS encryption, stringent requirements must be met: QRNG-based random entropy sources, practical security-verified QKD systems or networks for KEM, and the avoidance of trusted nodes for key storage and forwarding. Instead, pre-shared keys and universal hash checks for DS and authentication, and one-time-pad (OTP) for encryption should be used. Such use cases are rare and hold more theoretical significance than practical value.

### *3.2. Application Schemes of Quantum Keys*

In QKD-based QSC, delivering an end-to-end quantum key or relayed key for various encryption methods is essential for expanding use cases and commercial opportunities. A typical QSC setup between virtual private network (VPN) gateways, as illustrated in Figure 1a, can directly request keys from the QKD system or network and receive quantum keys or relay keys online. The security of these symmetrical keys depends on the practical security of the QKD system and QKD network (QKDN), which necessitates standardization and verification. These use cases represent the mainstream applications of QSC. Different types of quantum encryption VPNs, and routers have been developed and deployed in several experimental and demonstration networks (Xin et al., 2021).

For application scenarios where direct quantum key access from QKD systems and QKDN is not feasible, key charging and storage schemes can enable offline quantum key services, as depicted in Figure 1b. The terminal key service (TKS) manages quantum key charging and storage functions, as well as synchronization and certification between encryption equipment and terminals (Feng, 2021). Based on this offline QKD key service, quantum-encrypted mobile phones and customer premise equipment (CPE) have begun tentative commercialization with several network operators and infrastructure

providers (Xinhua, 2022). It is important to note that the security of the final symmetrical keys may be compromised and not meet ITS requirements due to the additional key storage and interaction functions of TKS.

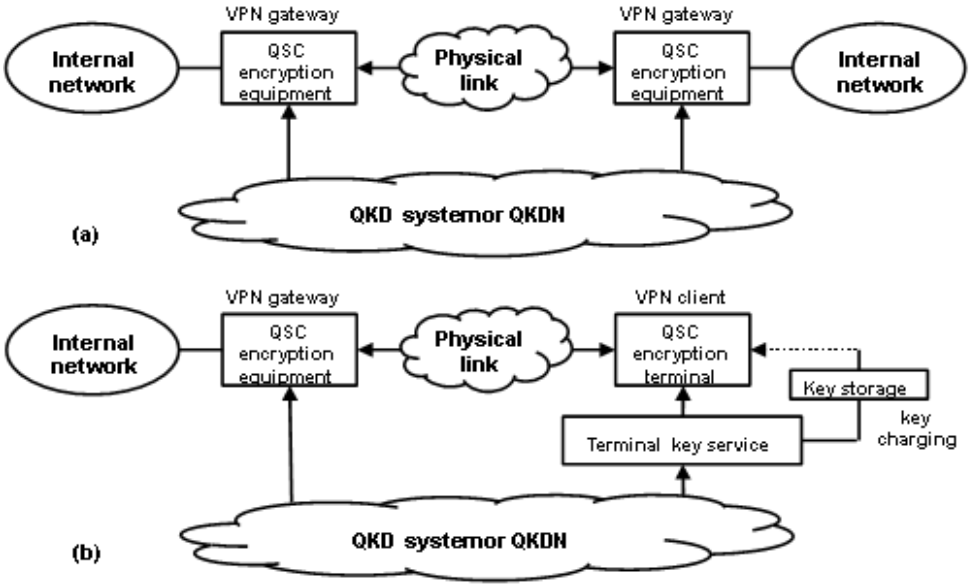


**Figure 1.** QKD key service schemes in QSC encryption. (**a**) Typical QSC between virtual private network gateways. (**b**) The offline quantum key services.

After acquiring quantum keys, effectively incorporating them into encryption algorithms is crucial for supporting QSC applications. Encryption protocols like IPSec, MacSec, TLS, OTNSec, among others, typically utilize self-negotiated key mechanisms rooted in public-key cryptography. These mechanisms ensure the establishment of security alliances and identity authentication to maintain the integrity and non-repudiation of information. Therefore, directly substituting the self-negotiated key with quantum keys in the mentioned protocols is impractical.

Instead, the QKD key can serve as a specialized pre-shared symmetric key, integrated with a self-negotiated key across various encryption protocols to form quantum-enhanced hybrid session keys. By combining different keys using XOR or abstract operation-based stirring functions, better compatibility and reliability can be achieved, especially in scenarios where the QKD key is unavailable due to system or fiber channel issues. Implementing key hybrid protocols in software is relatively straightforward, but acquiring quantum keys from QKD systems or QKDNs requires standardized application interfaces and protocol support to ensure interoperability.

### *3.3. Building QKD Networks and Their Applications*

By integrating the quantum key generation function of point-to-point QKD systems, the key storage and relay function of trusted nodes, and the key routing and networking function of the network controller, the QKDN can achieve end-to-end quantum key services. Establishing large-scale "quantum key infrastructure" stands as the most ambitious goal of the QKD industry.

Since the inception of the first 125 km commercial fiber QKD system in 2004, teams from academic and industrial sectors have completed numerous QKD network constructions and demonstration applications. Notably, the Beijing–Shanghai Backbone project in 2016 established a quantum secure communication backbone spanning over 2000 km, linking metro-area networks across various cities and serving as a vast platform for quantum communication technology verification and application demonstrations.

Building upon the success of the Beijing–Shanghai Backbone, efforts are underway to construct an even larger-scale wide area QKD network. This national project, spanning over 10,000 km, aims to connect major metropolitans like Harbin, Wuhan, Chengdu, and Guangzhou, forming a ring network in eastern China. This expansion is poised to enhance the accessibility, service capability, and reliability of the entire QKD network.

In QKD metro-networks such as Hefei and Jinan, dozens of user nodes including government departments, financial agencies, and research institutes are interconnected with trusted nodes through star-type or ring-type networking configurations, facilitating QKD services and enabling quantum-encrypted real-time voice communication, file transfer, and more.

Beyond China, several QKD network construction projects and demonstration applications have been conducted in Europe, a key region for QKD-based quantum secure communication exploration. Since 2008, multiple QKD networks have been experimentally validated in Austria, Switzerland, Spain, and France. The Open European Quantum Key Distribution Testbed project, initiated in 2019, supported over twenty EU projects and teams in conducting experiments on QKD networks and cryptographic applications, marking the initial steps toward constructing inter-European quantum networks for deployment and applications.

During the construction and deployment of QKD networks, leveraging existing fiber communication network infrastructure is crucial, achieved through wavelength division multiplexing between QKD and optical communication systems like OTN. Given the vulnerability of quantum signals to classical

signal impairments like spontaneous Raman scattering, careful wavelength selection, reduction of classical optical signal launch power, and specialized time and frequency domain filters are essential to enable co-propagation between QKD and classical optical signals across tens of square kilometers. However, the co-propagation of QKD and OTN systems is limited to point-to-point links due to the inability of quantum signals to pass through optical amplifiers like EDFA, posing significant challenges for long-distance and multi-span integration.

### *3.4. Quantum Secure Communication (QSC) Applications Using QKD Satellites*

Apart from the scientific experiments mentioned earlier, the Micius satellite in conjunction with a ground fiber QKD network has validated the feasibility of a combined space and ground quantum communication network. Through enhancements in the operating frequency, telescope size, and coupling efficiency of ground stations, along with the optimized unbalanced basis selection protocol, the QKD key rate reached up to 47.8 kbps for a single orbit (approximately 6 minutes) under ideal weather conditions, with a maximum satellite-relayed QKD key of about 36 Mbit per week.

To capitalize on the mobility and adaptability of satellite-based QKD, a portable ground station is indispensable supporting equipment. Successfully developed portable ground stations, weighing less than 100 kg and requiring less than 1 m3 of space, can be swiftly installed within 12 hours and deployed on urban building rooftops to conduct space-to-ground QKD experiments with Micius. Satellite-based QKD stands as one of the most significant applications to leverage QKD advantages, offering quantum key services to remote locations or mobile objects lacking fiber accessibility.

However, satellite-based QKD applications encounter numerous technical and engineering hurdles. Micius, being a Low Earth Orbit (LEO) satellite, has limited transmission time windows and ground coverage in a single orbit, functioning primarily at night due to constraints on light source working wavelengths and solar background noise. Consequently, Micius primarily serves to verify space-to-ground QKD feasibility rather than practical capability.

Efforts have been made in recent years to enhance satellite-based quantum communication capacities, including achieving daytime free-space QKD to counter sunlight scattering background noise. By employing a 1550 nm wavelength light source and detector, daylight intensity and scattering effects can be mitigated. Additionally, combining a narrow bandwidth grating filter with an ultra-low noise up-conversion single photon detector further reduces background noise, enabling a 20 bps key rate in QKD.

To establish a global space-to-ground quantum communication and QKD network, increasing the number of satellites and elevating orbit altitudes to create a quantum constellation merging Low Earth Orbit (LEO) and geosynchronous orbit (GEO) satellites is necessary. In 2022, the successful launch of the new QKD nano-satellite "Jinan-1", weighing only 1/6 of Micius, boasting approximately six times higher light source frequency, and equipped to handle real-time post-processing and key generation, marks a significant advancement. Expectations are high for nano-satellites and portable ground stations to conduct more intriguing QKD experiments and demonstrate QSC applications in the future.

QSC Testing and Verification Practices In the QSC sector, testing and verification stand as crucial components driving the deployment and application of QKD-based QSC networks. By adhering to technical specifications and employing corresponding testing and verification methods, QKD-based QSC systems and networks can undergo thorough evaluation to assure users of their performance, quality, and reliability, thus facilitating their procurement and deployment as commercial products and application solutions.

It's important to highlight that testing and evaluating the practical security of QKD systems and networks is equally critical. However, the development of QKD security-related standards is ongoing, and the reference frameworks for standardized verification remain incomplete, necessitating greater collaboration within the industry. Currently, market-oriented testing and verification efforts primarily concentrate on the functionality, performance, and reliability of QKD-based QSC systems and networks.

## 4. Evaluation of QKD System Tests

In the market, testing and evaluating QKD systems are conducted based on the technical requirements and test methods outlined for the decoy state BB84 protocol DV-QKD system. Table 4 illustrates the test items undertaken. Recently, mainstream system vendors' typical commercialized products in the market have undergone testing and certification.

In QKD system testing, the security key rate holds paramount importance. Since the key rate is contingent upon transmission distance and channel loss, specifying application codes in terms of typical channel loss, like 10 dB and 20 dB, offers an effective means to gauge QKD system performance. By standardizing the methods and formulas utilized in post-processing, including basis comparison, QBER calculation, error correction, and privacy amplification, key rate comparisons for QKD systems can be conducted across different implementations. Additionally, the randomness testing of quantum key outputs from QKD systems, in accordance with standards, ensures the security of symmetric keys.

Optical characteristics of quantum channel, synchronization channel, and distillation channel for QKD transmitters and receivers are pivotal for the deployment and implementation of QKD networks. Testing these characteristics at the system level provides accurate reference points for applications. Moreover, verifying the accuracy of decoy state and quantum state modulation, such as intensity fluctuations of signal and decoy states, quadrature and conjugate error of quantum state modulation, and differences in pulse time and frequency domain characteristics, offer partial evidence supporting practical system security. Furthermore, single-photon detectors (SPDs) serve as the primary limiting factors in QKD system performance and are crucial parameters in secure key rate calculations. Thus, testing and verifying SPD performance parameters, including detection efficiency, post-pulse probability, and dark count rate, among others, are imperative.

**Table 4.** QKD system testing and evaluation according to YDT 3834.1/3835.1.

| QKD Test Objects | QKD Test Items |
|---|---|
| System performance | Average secure key rate of QKD |
| | System channel-loss margin |
| | QKD output key consistency |
| | QKD output key randomness |
| QKD transmitter | Optical source time-domain characteristics |
| | Optical source frequency-domain characteristics |
| | Random number generator characteristics |
| | Decoy state modulation time-domain characteristics |
| | Decoy state modulation probability distribution |
| | Quantum state modulation time-domain characteristics |
| | Quantum state modulation frequency-domain characteristics |
| | Quantum state modulation demodulation accuracy |
| | Average photon number of quantum state signal Injection optical isolation |
| QKD receiver | Injected light leakage threshold |
| | SPD time-domain response characteristics |
| | SPD dark count probability |
| | SPD dead time |
| | SPD detection efficiency |
| | SPD post-pulse probability |
| Synchronization channel | Optical signal time-domain characteristics |
| | Optical signal frequency-domain characteristics Optical signal receipt sensitivity |
| Distillation channel | Optical signal time-domain characteristics Optical signal frequency-domain characteristics |
| Other system features | System long-term stability |
| | System redundancy protection |
| | System start-up time |
| | System recovery time |
| | System environmental reliability Power supply tolerance |
| Network management | System management features Network management features |

The optical signals in QKD systems are extremely faint, typically below −70 dBm. When deploying commercial QKD systems alongside other optical communication systems, there are heightened requirements for reliability and adaptability to varying environments. These demands are often overlooked in laboratory experiments or field trials. Ensuring the continuity of service involves verifying the reliability of commercial QKD systems, including their long-term stability, system redundancy protection, fault recovery capability, and resilience to different temperature and humidity conditions.

The development of standards and testing verification provides valuable guidance and facilitates the transition of QKD systems from research-focused prototypes to commercially mature products. With ongoing advancements in standardization and testing verification, it is reasonable to anticipate further improvements in the engineering and practical capabilities of QKD systems.

### *4.1 Evaluation of QKD System Testing*

Establishing QKD networks by interconnecting multiple QKD systems is crucial for expanding and enhancing key services. Quantum keys produced by point-to-point QKD links undergo synchronization, authentication, and storage by key managers (KMs) at trusted nodes. Subsequently, these quantum keys are relayed hop-by-hop through classical communication channels between KMs to furnish end-to-end symmetric keys, typically utilizing OTP encryption during relay to maintain key integrity and trustworthiness. The networking functions across different layers of the QKDN are facilitated by network management and controllers, with the QKD network framework and functional architecture aligning with ITU-T Y.3800 series Recommendations (ITU-T, 2019).

The relay key provisioning capability of an end-to-end link hinges on the minimum key rate among all point-to-point QKD links within it; thus, it's imperative to test and verify the actual key rate of all QKD links in the network. The channel loss in legacy fiber networks may deviate from the nominal value due to factors like station distance and fiber cable conditions, which could impact the QKD key rate. Deploying multiple pairs of QKD systems simultaneously in high channel loss fiber links is a common approach to ensure the key rate meets design specifications. It's noteworthy that this stacked QKD system deployment differs from typical redundant protection used in optical communication networks, like 1 + 1 or 1:1 protection, as all systems operate concurrently to ensure the key rate of point-to-point links.

Protection and recovery of QKD networks are predominantly managed in the key management layer, often requiring multiple key relay paths or the creation of ring-type networks to offer backup routing support. Network protection necessitates classical communication systems like OTNs and routers to support network management and QKD distillation, with capabilities for their own protection and recovery. Moreover, it demands functionalities from network controllers and management to achieve key relaying re-routing. Since the KM features caching functionality, upper-layer key applications are typically unaffected during the protection recovery process of key-relay rerouting. For large and intricate topology QKD networks, verifying protection and recovery capabilities at both classical communication and key relaying levels is essential to ensure key provisioning Quality of Service (QoS).

Essential service support systems and networks within QKD networks, such as OTNs, IP networks, time synchronization, and network management, form the foundation for overall service quality and require scrutiny in network-level test verification. Planning and configuring OTN and IP networks, multi-service support capability, and long-term service stability are key considerations. NTP-based network time synchronization offers millisecond-level timing accuracy and supports key lifecycle management, network performance, fault monitoring, service billing, and other management functions. Testing and verifying time deviation and redundancy protection for NTP time servers and clients are crucial to ensure the reliability of the overall time service capability of QKD networks. Other network-level tests encompass verifying functions like network management systems, business support, and application service platforms.

### *4.2 Discussion and Future Prospects*

Over the last two decades, there has been active research in QKD technology, resulting in significant enhancements in performance metrics like transmission distance and key rate for fiber-based QKD systems, alongside successful feasibility verification for satellite-based QKD. Numerous vendors have embarked on commercializing QKD-based QSC systems, with network deployments occurring worldwide, particularly in sectors like government, finance, and infrastructure. Moreover, international and regional standards development organizations (SDOs) have undertaken standardization efforts for QKD and QSC devices, systems, networks, services, and security, with ongoing test verification and certification activities for QKD systems and networks based on these standards. Looking ahead, the momentum in QKD-based QSC technology development and application exploration is poised to continue. However, despite these advancements, the industry has not witnessed the anticipated "exponential growth" in the application and commercialization of QKD-based QSC over the past decade. Financial data and market performance of related companies have been relatively lackluster. There remain several obstacles and challenges hindering the widespread adoption and commercialization of QKD-based QSC, including:

**Technology:** The inherent trade-off between the security of key generation and transmission robustness in QKD systems poses a critical barrier to enhancing transmission capability and key rate, limiting their adaptability and reliability outside laboratory settings. Although newer protocols like TF and MDI have shown performance improvements, and satellite-based QKD is technically viable, widespread commercial adoption of products based on these protocols and platforms still requires significant development.

**Application:** Implementing QKD-based QSC applications necessitates dedicated fiber resources, potential network architecture changes, specialized configuration and maintenance of QKD systems, and substantial expenses due to the relatively high costs associated with QKD systems. Developing QKD technology and systems based on integrated photonics can enhance system integration and robustness while reducing costs, thereby enhancing scalability and expanding QKD applications.

**Standards and Certification:** While progress has been made in QKD-related standards, there is still much work to be done, particularly in establishing credible specifications and test verification for the practical security proof of QKD systems. This is crucial to fully realize the advantage of Information-Theoretic Security (ITS) and gain the trust of customers with high security requirements. Additionally, specifying interfaces and protocols for Key Management (KM) layers in QKD networks to facilitate cross-domain interoperability is another priority for future standardization efforts. In conclusion,

QKD offers unique advantages in securely distributing symmetric keys between remote locations, with applications spanning cryptography, encryption, authentication, and long-term security in the era of quantum computation. Supported by both academia and industry, QKD technology has made steady progress from theoretical protocols of the past to achieving thousand-kilometer transmission distances and key sharing today. With the emergence of new protocol systems, the miniaturization of Photonic Integrated Circuit (PIC)-based systems, and the maturation of commercial products, the deployment and application of QKD-based QSC are expected to become more prevalent, particularly in high-security network communication scenarios. The continued development of standardization and test verification efforts will provide valuable guidance and support for industrialization. In the quantum era, cautious optimism about the future development and application of QKD-based QSC is warranted.

## 5. Conclusion

In this paper, we provided a brief summary of the foundational aspects and significant milestones in quantum cryptography (QC). QC protocols hold certain advantages over classical ones as they are theoretically secure under ideal technological conditions. While unconditional security proofs are feasible, they may not hold under all non-ideal circumstances. Attaining ultimate security is improbable due to potential imperfections in technological implementations. Nonetheless, the QC framework remains robust as it shifts the security challenge from theory to technology, which is advantageous given the slower and more predictable pace of technological advancements. However, there remain several unresolved issues in the theoretical domain. Although formal security bounds have been calculated under specific conditions, achieving a satisfactory level of generality in these analyses remains elusive. Moreover, the comparison of different QC implementations lacks sufficient reliance on quantitative metrics. Additionally, while experimental demonstrations of quantum key exchange have been successful over short distances, the limited range and low bit rates still pose challenges. Despite these hurdles, QC is progressively transitioning from laboratory settings to the telecommunications mainstream, offering commercialized quantum cryptography and key distribution systems (FibreSystems, 2004).

**References**

«Quantum cryptography: the key to secure data transfer», *FibreSystems Europe/ Lightwave Europe, June 2004.*

Aguado, A., Hugues-Salas, E., Haigh, P. A., Marhuenda, J., Price, A. B., Sibson, P., Kennard, J. E., Erven, C., Rarity, J. G., Thompson, M. G., ... (2017). Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. *Journal of Lightwave Technology*, *35*, 1357–1362. https://doi.org/10.1109/JLT.2017.2666118

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., Folgueira, J., & Martin, V. (2019). The engineering of software-defined quantum key distribution networks. *IEEE Communications Magazine*, *57*, 20–26. https://doi.org/10.1109/MCOM.2019.1700655

Alagic, G., Cooper, D., Dang, Q., Dang, T., Kelsey, J. M., Lichtinger, J., Liu, Y. K., Miller, C. A., Moody, D., Peralta, R., ... (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process*. Gasburg, MD: U.S. National Institute of Standards and Technology.

Bacco, D., Christensen, J. B., Castaneda, M. A. U., Ding, Y., Forchhammer, S., Rottwitt, K., & Oxenløwe, L. K. (2016). Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Scientific Reports*, *6*, 36756. https://doi.org/10.1038/srep36756

Barbosa, G.A., Corndorf, E., Kumar, P. and Yuen, H. P., (2003), *Phys. Rev. Lett.* 90, 227901.

Bechmann-Pasquinucci, H., and Gisin, N., (1999), *Phys. Rev. A* 59, 4238–4248.

Bell, J. S., 1964, Rev. Mod. Phys. **38**, 447–452 [reprinted in Bell, J. S., 1987, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University, Cambridge, England)].

Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Bennett, C. H., (1992), *Phys. Rev. Lett.* 68, 3121–3124.

Bennett, C. H., and Brassard G.,(1984) In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp.175–179. IEEE, New York.

Bennett, C. H., G. Brassard, and J.-M. Robert, (1988), *SIAM J. Comput*. 17, 210– 229.

Bennett, C. H., G. Brassard, C. Crepeau, and Maurer, U. M., (1995), *IEEE Trans. Inf. Theory* 41, 1915–1923.

Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M.-J., ... (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, *121*, 190502. https://doi.org/10.1103/PhysRevLett.121.190502

Bouchard, F., Sit, A., Hufnagel, F., Abbas, A., Zhang, Y., Heshami, K., Fickler, R., Marquardt, C., Leuchs, G., Boyd, R. W., & et al. (2018). Quantum cryptography with twisted photons through an outdoor underwater channel. *Optics Express*, *26*(18), 22563–22573. https://doi.org/10.1364/OE.26.022563

Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., & Zeilinger, A. (1997). Experimental quantum teleportation. *Nature*, *390*, 575–579. https://doi.org/10.1038/37539

Brassard, G., and Salvail, L. (1994) In: *Advances in Cryptology—EUROCRYPT '93 Proceedings*, Lecture Notes in Computer Science, Vol. 765, pp. 410. T. Helleseth (Eds). Springer, New York.

Bruss, D., (1998), *Phys. Rev. Lett.* 81, 3018–3021.

Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhang, W., Hu, X.-L., Guan, J.-Y., Yu, Z.-W., Xu, H., Lin, J., ... (2020). Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Physical Review Letters, 124,* 070501. https://doi.org/10.1103/PhysRevLett.124.070501

Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhang, W.-J., Han, Z.-Y., Ma, S.-Z., Hu, X.-L., Li, Y.-H., Liu, H., ... (2021). Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nature Photonics, 15*, 570–575. https://doi.org/10.1038/s41566-021-00796-z

Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhao, D.-F., Zhang, W.-J., Chen, F.-X., Li, H., You, L.-X., Wang, Z., ... (2022). Quantum key distribution over 658 km fiber with distributed vibration sensing. *Physical Review Letters, 128*, 180502. https://doi.org/10.1103/PhysRevLett.128.180502

Chen, T.-Y., Jiang, X., Tang, S.-B., Zhou, L., Yuan, X., Zhou, H., Wang, J., Liu, Y., Chen, L.-K., Liu, W.-Y., & et al. (2021). Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information, 7*, 134. https://doi.org/10.1038/s41534-021-00450-0

Chen, W., Han, Z.-F., Zhang, T., Wen, H., Yin, Z.-Q., Xu, F.-X., Wu, Q.-L., Liu, Y., Zhang, Y., Mo, X.-F., & et al. (2009). Field experiment on a "star type" metropolitan quantum key distribution network. *IEEE Photonics Technology Letters, 21*(8), 575–577. https://doi.org/10.1109/LPT.2009.2013721

Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., & et al. (2021). An integrated space-to-ground quantum communication network over 4600 kilometres. *Nature, 589*(7841), 214–219. https://doi.org/10.1038/s41586-020-03093-8

Cozzolino, D., Da Lio, B., & Bacco, D. (2019). High-dimensional quantum communication: Benefits, progress, and future challenges. *Advanced Quantum Technologies, 2*(12), 1900038. https://doi.org/10.1002/qute.201900038

Dai, H., Shen, Q., Wang, C.-Z., Li, S.-L., Liu, W.-Y., Cai, W.-Q., Liao, S.-K., Ren, J.-G., Yin, J., Chen, Y.-A., & et al. (2020). Towards satellite-based quantum-secure time transfer. *Nature Physics, 16*(8), 848–852. https://doi.org/10.1038/s41567-020-0913-3

Deutsch, I. H. (2020). Harnessing the power of the second quantum revolution. *PRX Quantum, 1*, 020101. https://doi.org/10.1103/PRXQuantum.1.020101

Dusek, M., M. Jahma, and Lütkenhaus, N., (2000), *Phys. Rev. A* 62, 022306.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters, 67*, 661–663. https://doi.org/10.1103/PhysRevLett.67.661

Ekert, A. K., (1991), *Phys. Rev. Lett.* 67, 661–663.

Erhard, M., Krenn, M., & Zeilinger, A. (2020). Advances in high-dimensional quantum entanglement. *Nature Reviews Physics, 2*(7), 365–381. https://doi.org/10.1038/s42254-020-0193-5

Eriksson, T. A., Luis, R. S., Puttnam, B. J., Rademacher, G., Fujiwara, M., Awaji, Y., Furukawa, H., Wada, N., Takeoka, M., & Sasaki, M. (2020). Wavelength division multiplexing of 194 continuous variable quantum key distribution channels. *Journal of Lightwave Technology, 38*(9), 2214–2218. https://doi.org/10.1109/JLT.2020.2981418

European Quantum Flagship. (2022). *Strategic research and industry agenda*. Retrieved from https://qt.eu/about-quantumflagship/introduction-to-the-quantum-flagship/sab-strategic-advisory-board/ (accessed on February 20, 2023).

Fang, X.-T., Zeng, P., Liu, H., Zou, M., Wu, W., Tang, Y.-L., Sheng, Y.-J., Xiang, Y., Zhang, W., Li, H., ... (2020). Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nature Photonics, 14*, 422–425. https://doi.org/10.1038/s41566-019-0532-1

Felix, S., A. Stefanov, Zbinden, H. and Gisin, N., (2001), *J. Mod. Opt.* 48, 2009– 2021.

Feng, C. (2021, January 7). China Telecom launches quantum encrypted phone calls on smartphones in a new pilot programme. *The Star*. https://www.thestar.com.my/news/regional/2021/01/07/china-telecom-launches-quantum-encrypted-phone-calls-on-smartphones-in-new-pilot-programme

FG-QIT4N. (2021). *Standardization outlook and technology maturity: Quantum key distribution network*. Geneva, Switzerland: ITU-T.

Gisin, N., & Thew, R. (2007). Quantum communication. *Nature Photonics, 1*, 165–171. https://doi.org/10.1038/nphoton.2007.22

Gisin, N., and Wolf S., (2000), *Advances in Cryptology—Proceedings of Crypto 2000*, Lecture Notes in Computer Science, Vol. 1880, pp. 482–500. Bellare, M. (Ed.) Springer, New York.

Gisin, N., and Wolf, S., (1999), *Phys. Rev. Lett.* 83, 4200–4203.

Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., (2002), *Rev. Mod. Phys.*, 74(1), 145-196.

Goldwasser S., Bellare, M. (1996), Cryptography: Lecture Notes, (compiled for a summer course in cryptography taught at MIT in July 1996).

Grosshans, F., & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters, 88*(5), 057902. https://doi.org/10.1103/PhysRevLett.88.057902

Hardy. L., (2004), *Phys. Rev. Lett.* 92, 157901.

Hillery, M., Bužek, V., & Berthiaume, A. (1999). Quantum secret sharing. *Physical Review A, 59*, 1829–1834. https://doi.org/10.1103/PhysRevA.59.1829

Hiroki, T., Honjo, T., Tamaki, K., & Tokura, Y. (2008, May 12–13). Differential phase shift quantum key distribution. In *Proceedings of the 2008 First ITU-T Kaleidoscope Academic Conference—Innovations in NGN: Future Network and Services* (pp. 243–248). Geneva, Switzerland. https://doi.org/10.1109/KALEIDOSCOPE.2008.4552074

Hwang, W. Y., (2003), *Phys. Rev. Lett.* 91, 057901.

id Quantique, available online at http://www.idquantique.com.

ITU-T. (2019). Y.3800: Overview on networks supporting quantum key distribution. International Telecommunication Union. https://www.itu.int/rec/T-REC-Y.3800-201912-I

Jacak, M. M., Jóźwiak, P., Niemczuk, J., & Jacak, J. E. (2021). Quantum generators of random numbers. *Scientific Reports, 11*, 16108. https://doi.org/10.1038/s41598-021-95645-4

Jain, N., Chin, H.-M., Mani, H., Lupo, C., Nikolic, D. S., Kordts, A., Pirandola, S., Pedersen, T. B., Kolb, M., Ömer, B., & et al. (2022). Practical continuous-variable quantum key distribution with composable security. *Nature Communications, 13*(1), 4740. https://doi.org/10.1038/s41467-022-32475-8

Jiang, C., Yu, Z.-W., Hu, X.-L., & Wang, X.-B. (2019). Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Physical Review Applied, 12*, 024061. https://doi.org/10.1103/PhysRevApplied.12.024061

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7908), 237–243. https://doi.org/10.1038/s41586-022-04547-8

Joshi, C., & Singh, U. K. (2017). Information security risks management framework—A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

Kent, A., (2003), *Phys. Rev. Lett.* 90, 237901.

Kerstel, E., Gardelein, A., Barthelemy, M., The CSUG Team, Fink, M., Joshi, S. K., & Ursin, R. (2018). Nanobob: A CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technology, 5*, 6. https://doi.org/10.1140/epjqt/s40507-018-0071-7

Kimble, H. J. (2008). The quantum internet. *Nature, 453*, 1023–1030. https://doi.org/10.1038/nature07127

Lamoureux, L. P., Brainis, E., Amans, D., Barrett, J., and Massar S., (2005), *Phys. Rev. Lett.* 94, 050503.

Laudenbach, F., Pacher, C., Fung, C.-H. F., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P., & Hübel, H. (2018). Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations. *Advanced Quantum Technologies, 1*(3), 1800011. https://doi.org/10.1002/qute.201800011

Leverrier, A., & Grangier, P. (2009). Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters, 102*(18), 180504. https://doi.org/10.1103/PhysRevLett.102.180504

Lewis, A. M., & Travagnin, M. (2019). *Quantum key distribution in-field implementations*. Luxembourg: Publications Office of the European Union.

Lewis, A. M., & Travagnin, M. (2022). *A secure quantum communications infrastructure for Europe: Technical background for a policy vision*. Luxembourg: Publications Office of the European Union.

Li, B., Cao, Y., Li, Y.-H., Cai, W.-Q., Liu, W.-Y., Ren, J.-G., Liao, S.-K., Wu, H.-N., Li, S.-L., Li, L., & et al. (2022). Quantum state transfer over 1200 km assisted by prior distributed entanglement. *Physical Review Letters, 128*(17), 170501. https://doi.org/10.1103/PhysRevLett.128.170501

Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., & et al. (2018). Satellite-relayed intercontinental quantum network. *Physical Review Letters, 120*(3), 030501. https://doi.org/10.1103/PhysRevLett.120.030501

Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., & et al. (2017). Satellite-to-ground quantum key distribution. *Nature, 549*(7670), 43–47. https://doi.org/10.1038/nature23655

Liao, S.-K., Yong, H.-L., Liu, C., Shentu, G.-L., Li, D.-D., Lin, J., Dai, H., Zhao, S.-Q., Li, B., Guan, J.-Y., & et al. (2017). Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics, 11*(8), 509–513. https://doi.org/10.1038/nphoton.2017.116

Lo, H.-K., and Chau, H. F., (1999), *Science* 283, 2050–2056.

Long, G.-L., Deng, F.-G., Wang, C., Li, X.-H., Wen, K., & Wang, W.-Y. (2007). Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China, 2*, 251–272. https://doi.org/10.1007/s11467-007-0050-7

Lu, C.-Y., Cao, Y., Peng, C.-Z., & Pan, J.-W. (2022). Micius quantum experiments in space. *Reviews of Modern Physics, 94*(3), 035001. https://doi.org/10.1103/RevModPhys.94.035001

Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature, 557*, 400–403. https://doi.org/10.1038/s41586-018-0066-6

Lütkenhaus, N., (2000), *Phys. Rev. A* 61, 052304.

MagiQ- Quantum Information Solutions for the Real World, available online at http://www.magiqtech.com.

Martin, V., Brito, J. P., Escribano, C., Menchetti, M., White, C., Lord, A., Wissel, F., Gunkel, M., Gavignet, P., Genay, N., ... (2021). Quantum technologies in the telecommunications industry. *EPJ Quantum Technology*, *8*, 19. https://doi.org/10.1140/epjqt/s40507-021-00109-7

Martin, V., Martinez-Mateo, J., & Peev, M. (2017). Introduction to quantum key distribution. In *Wiley Online Library* (pp. 1–17). Hoboken, NJ: Wiley. https://doi.org/10.1002/9781119061123.ch1

Mattle, K., Weinfurter, H., Kwiat, P. G., & Zeilinger, A. (1996). Dense coding in experimental quantum communication. *Physical Review Letters, 76*, 4656–4659. https://doi.org/10.1103/PhysRevLett.76.4656

Maurer, U. M., (1993), *IEEE Trans. Inf. Theory* 39, 733–742.

Maurer, U. M., and Wolf, S., (1999), *IEEE Trans. Inf. Theory* 45, 499–514.

Mazurenko, Y., R. Giust, and J. P. Goedgebuer, 1997, Opt. Commun. **133**, 87–92.

Mérolla, J-M., Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes (1999), Phys. Rev. Lett. **82**, 1656–1659.

Minder, M., Pittaluga, M., Roberts, G. L., Lucamarini, M., Dynes, J. F., Yuan, Z. L., & Shields, A. J. (2019). Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics, 13*, 334–338. https://doi.org/10.1038/s41566-019-0377-7

Mo, X.-F., Zhu, B., Han, Z.-F., Gui, Y.-Z., & Guo, G.-C. (2005). Faraday–Michelson system for quantum cryptography. *Optics Letters, 30*(20), 2632–2634. https://doi.org/10.1364/OL.30.002632

Mohammad, O. K. J., Abbas, S., El-Horbaty, E.-S. M., & Salem, A.-B. M. (2014). Advanced encryption standard development based quantum key distribution. In *Proceedings of the 9th International Conference for Internet Technology and Secured Transactions, London, UK, 8–10 December 2014* (pp. 115-120). IEEE. https://doi.org/10.1109/ICITST.2014.7038816

National Science and Technology Council. (2018). *National strategic overview for quantum information science*. Washington, DC: Author. Retrieved from https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf (accessed on February 20, 2023).

Nicholas, P., van Dam Kleese, K., Inder, M., & Thomas, S. (2020). *From long-distance entanglement to building a nationwide quantum internet: Report of the DOE Quantum Internet Blueprint Workshop*. Oak Ridge, TN: U.S. Department of Energy Office of Scientific and Technical Information.

Oi, D. K., Ling, A., Vallone, G., Villoresi, P., Greenland, S., Kerr, E., Macdonald, M., Weinfurter, H., Kuiper, H., Charbon, E., & et al. (2017). CubeSat quantum communications mission. *EPJ Quantum Technology, 4*, 6. https://doi.org/10.1140/epjqt/s40507-017-0060-1

Pan, Y., Wang, H., Shao, Y., Pi, Y., Li, Y., Liu, B., Huang, W., & Xu, B. (2022). Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *Optics Letters, 47*(13), 3307–3310. https://doi.org/10.1364/OL.462868

Peng, C.-Z., Zhang, J., Yang, D., Gao, W.-B., Ma, H.-X., Yin, H., Zeng, H.-P., Yang, T., Wang, X.-B., & Pan, J.-W. (2007). Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical Review Letters, 98*, 010505. https://doi.org/10.1103/PhysRevLett.98.010505

Peters, N. A., Alshowkan, M., Chapman, J. C., Evans, P. G., Hooper, D. A., Grice, W. P., Lu, H.-H., Lukens, J. M., Pooser, R. C., Marvinney, C. E., & et al. (2022). Quantum networking and communications at Oak Ridge National Laboratory. In *Proceedings of the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2–5 May 2022* (pp. 1-6). IEEE. https://doi.org/10.1109/INFOCOMWKSHPS54753.2022.9798285

Pittaluga, M., Minder, M., Lucamarini, M., Sanzaro, M., Woodward, R. I., Li, M.-J., Yuan, Z., & Shields, A. J. (2021). 600-km repeater-like quantum communications with dual-band stabilization. *Nature Photonics, 15*, 530–535. https://doi.org/10.1038/s41566-021-00801-5

Pugh, C. J., Kaiser, S., Bourgoin, J.-P., Jin, J., Sultana, N., Agne, S., Anisimova, E., Makarov, V., Choi, E., Higgins, B. L., & et al. (2017). Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology, 2*(2), 024009. https://doi.org/10.1088/2058-9565/aa701f

Ren, J.-G., Abulizi, M., Yong, H.-L., & Yin, J. (2022). Portable ground stations for space-to-ground quantum key distribution. *arXiv*, arXiv:2205.13828. https://arxiv.org/abs/2205.13828

Ren, J.-G., Xu, P., Yong, H.-L., Zhang, L., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Yang, M., Li, L., & et al. (2017). Ground-to-satellite quantum teleportation. *Nature*, *549*(7670), 70–73. https://doi.org/10.1038/nature23675

Renner, R., Gisin, N., & Kraus, B. (2005). Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, *72*, 012332. https://doi.org/10.1103/PhysRevA.72.012332

Ribezzo, D., Zahidy, M., Vagniluca, I., Biagi, N., Francesconi, S., Occhipinti, T., Oxenløwe, L. K., Lončarić, M., Cvitic, I., Stipčević, M., & et al. (2023). Deploying an inter-European quantum network. *Advanced Quantum Technologies*, *6*(1), 2200061. https://doi.org/10.1002/qute.202200061

Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., & et al. (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express*, *19*(11), 10387–10409. https://doi.org/10.1364/OE.19.010387

Satnews. (2022, July 31). China launches new satellite in important step towards global quantum communications network. *Satnews*. https://www.satnews.com/story.php?number=2083146669

Sekga, C., Mafu, M., & Senekane, M. (2023). High-dimensional quantum key distribution implemented with biphotons. *Scientific Reports*, *13*(1), 1229. https://doi.org/10.1038/s41598-023-29149-4

Shor, P. W., (1994), *Proceedings of the 35th Symposium on Foundations of Computer Science*,, pp. 124–134. Goldwasser, S. (Ed). IEEE Computer Society, Los Alamitos, California.

Shor, P. W., and Preskill, J., (2000), *Phys. Rev. Lett.* 85, 441–444.

Steinlechner, F., Ecker, S., Fink, M., Liu, B., Bavaresco, J., Huber, M., Scheidl, T., & Ursin, R. (2017). Distribution of high-dimensional entanglement via an intra-city free-space link. *Nature Communications*, *8*(1), 15971. https://doi.org/10.1038/ncomms15971

Sun, P. C., Y. Mazurenko, and Y. Fainman (1995), Opt. Lett. **20**, 1062–1063.

Sun, S., & Huang, A. (2022). A review of security evaluation of practical quantum key distribution system. *Entropy*, *24*(2), 260. https://doi.org/10.3390/e24020260

Tsurumaru, T, Phys. Rev. A, 71, 012313 (2005).

Vagniluca, I., Da Lio, B., Rusca, D., Cozzolino, D., Ding, Y., Zbinden, H., Zavatta, A., Oxenløwe, L. K., & Bacco, D. (2020). Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Physical Review Applied*, *14*(1), 014051. https://doi.org/10.1103/PhysRevApplied.14.014051

Vermeer, M. J. D., & Peet, E. D. (2020). *Securing communications in the quantum computing age: Managing the risks to encryption*. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RR3140

Wang, H., Li, Y., Pi, Y., Pan, Y., Shao, Y., Ma, L., Zhang, Y., Yang, J., Zhang, T., & Huang, W. (2022). Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Communications Physics*, *5*(1), 162. https://doi.org/10.1038/s42005-022-00924-8

Wang, J.-Y., Yang, B., Liao, S.-K., Zhang, L., Shen, Q., Hu, X.-F., Wu, J.-C., Yang, S.-J., Jiang, H., Tang, Y.-L., & et al. (2013). Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photonics*, *7*(5), 387–393. https://doi.org/10.1038/nphoton.2013.89

Wang, L.-J., Zou, K.-H., Sun, W., Mao, Y., Zhu, Y.-X., Yin, H.-L., Chen, Q., Zhao, Y., Zhang, F., Chen, T.-Y., & et al. (2017). Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *Physical Review A*, *95*(1), 012301. https://doi.org/10.1103/PhysRevA.95.012301

Wang, S., Yin, Z.-Q., He, D.-Y., Chen, W., Wang, R.-Q., Ye, P., Zhou, Y., Fan-Yuan, G.-J., Wang, F.-X., Zhu, Y.-G., ... (2022). Twin-field quantum key distribution over 830-km fibre. *Nature Photonics*, *16*, 154–161. https://doi.org/10.1038/s41566-021-00847-5

Wang, X.-B., Yu, Z.-W., & Hu, X.-L. (2018). Twin-field quantum key distribution with large misalignment error. *Physical Review A*, *98*, 062323. https://doi.org/10.1103/PhysRevA.98.062323

Weedbrook, C., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C., & Lam, P. K. (2004). Quantum cryptography without switching. *Physical Review Letters*, *93*(17), 170504. https://doi.org/10.1103/PhysRevLett.93.170504

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*, eaam9288. https://doi.org/10.1126/science.aam9288

Wiesner, S., (1983), *SIGACT News* 15, 78–88.

Wootters, W. K., and Zurek, W. H., (1982), *Nature* (London) 299, 802–803.

Xavier, G. B., & Lima, G. (2020). Quantum information processing with space-division multiplexing optical fibres. *Communications Physics*, *3*, 9. https://doi.org/10.1038/s42005-020-0288-6

Xin, H. (2021). China realizes secure, stable quantum communication network spanning 4600 km. China.org.cn. http://www.china.org.cn/china/2021-01/07/content_77088150.htm

Xinhua. (2022, May 17). China launches quantum-secured, 'unhackable' smartphone. *China Daily*. http://www.chinadaily.com.cn/a/202205/17/WS62838a9fa310fd2b29e5c46c.html

Xu, F., Chen, W., Wang, S., Yin, Z., Zhang, Y., Liu, Y., Zhou, Z., Zhao, Y., Li, H., Liu, D., & et al. (2009). Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chinese Science Bulletin*, *54*(17), 2991–2997. https://doi.org/10.1007/s11434-009-0550-8

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, *92*, 025002. https://doi.org/10.1103/RevModPhys.92.025002

Xu, H., Yu, Z.-W., Jiang, C., Hu, X.-L., & Wang, X.-B. (2020). Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. *Physical Review A*, *101*, 042330. https://doi.org/10.1103/PhysRevA.101.042330

Xu, P., Ma, Y., Ren, J.-G., Yong, H.-L., Ralph, T. C., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Han, X., & et al. (2019). Satellite testing of a gravitationally induced quantum decoherence model. *Science*, *366*(6461), 132–135. https://doi.org/10.1126/science.aay5820

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., & et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, *356*(6343), 1140–1144. https://doi.org/10.1126/science.aan3211

Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., & et al. (2017). Satellite-to-ground entanglement-based quantum key distribution. *Physical Review Letters*, *119*(20), 200501. https://doi.org/10.1103/PhysRevLett.119.200501

Yin, J., Li, Y.-H., Liao, S.-K., Yang, M., Cao, Y., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, S.-L., & et al. (2020). Entanglement-based secure quantum cryptography over 1120 kilometres. *Nature*, *582*(7813), 501–505. https://doi.org/10.1038/s41586-020-2401-y

Yuan, Z., Murakami, A., Kujiraoka, M., Lucamarini, M., Tanizawa, Y., Sato, H., Shields, A. J., Plews, A., Takahashi, R., Doi, K., ... (2018). 10-Mb/s quantum key distribution. *Journal of Lightwave Technology*, *36*, 3427–3433. https://doi.org/10.1109/JLT.2018.2832766

Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., Kiktenko, E. O., Kolycheva, E., Borisov, A., & Fedorov, A. L. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology*, *8*, 14. https://doi.org/10.1140/epjqt/s40507-021-00108-2

Zhou, S., Zhai, G., & Shi, Y. (2018). What drives the rise of metro developments in China? Evidence from Nantong. *Sustainability*, *10*(8), 2931. https://doi.org/10.3390/su10082931