Advance in Security Proofs of Quantum Key Distribution and Its Challenges towards Practical Implementation

Kazutoshi Kan and Toshihiko Sasaki

This paper provides an overview of advancements in the security proof of quantum key distribution (QKD) while discussing the rationale and challenges of its practical implementation. QKD ensures information-theoretic security, meaning even eavesdroppers with unlimited computational power cannot decipher the transmitted data. As a result, it is resilient against various attacks, including eavesdropping and harvest-now-decrypt-later attacks. QKD encompasses a range of methodologies, each supported by corresponding security proofs. Since the introduction of the first QKD protocol, BB84, theoretical progress has been made to address evolving technologies and counter implementation attacks that exploit device imperfections. In 2020, the first security proof for continuous-variable QKD (CV-QKD) was established. This method offers greater compatibility with existing optical fiber networks. Despite its advantages, QKD requires specialized devices, resulting in high costs for network construction. Currently, QKD is primarily suitable for transmitting highly confidential information across multiple hubs. To encourage its adoption, several challenges must be addressed, including advancing quantum relay technologies, enhancing performance, establishing protocol standards, and creating institutional frameworks for verifying and certifying device security.

Keywords: QKD; CV-QKD; Implementation attack
JEL Classification: L86, L96, O36

Kazutoshi Kan: Director, Institute for Monetary and Economic Studies (currently, Financial System and Bank Examination Department), Bank of Japan
(E-mail: kazutoshi.kan@boj.or.jp)
Toshihiko Sasaki: Lecturer, The University of Tokyo. Currently, Quantinuum K.K.
(E-mail: toshihiko.sasaki@quantinuum.com)

The authors are grateful for the helpful comments provided by Kiyoshi Tamaki (University of Toyama), Noboru Kunihiro (University of Tsukuba), Mikio Fujiwara (The National Institute of Information and Communications Technology), and Masaru Fukushima (The National Institute of Information and Communications Technology). The views expressed are those of the authors and do not necessarily reflect the views of the Bank of Japan or the University of Tokyo. This paper was written on the basis of information available as of February 2024.

I. Introduction

Quantum key distribution (QKD) is a communication protocol that encodes cryptographic key information into quantum bits (qubits), represented by the states of photons. The quantum-mechanical properties of these qubits ensure the secure protection of this information. Currently, widely used cryptographic algorithms on the Internet, such as RSA and elliptic curve cryptography (ECC), are theoretically known to be efficiently breakable by quantum computers with sufficient computational power.[1] QKD is considered one of the cryptographic techniques secure against the threat posed by quantum computers. It stands as a potential alternative alongside **post-quantum cryptography (PQC)**, which does not rely on quantum-mechanical properties. Demonstration experiments using QKD for encrypted communication are being conducted worldwide.[2] Encrypted communication with QKD works by first performing QKD between two parties to share a random key. This shared key, in combination with classical cryptography (such as a one-time pad [OTP]), is then used to securely transmit any arbitrary message. The following discussion focuses on QKD.

A key advantage of QKD is its ability to guarantee both the absence of eavesdropping and **information-theoretic security**. Information-theoretic security is a robust property that ensures confidentiality even if an attacker possesses unlimited computational power or employs any eavesdropping techniques permitted by the laws of physics. Unlike computational security, information-theoretic security remains unaffected by future advancements in computational power, cryptanalysis algorithms, or eavesdropping techniques, thereby ensuring the confidentiality of communications indefinitely. This property makes QKD secure against the threat of cryptanalysis by ideal quantum computers. Notably, QKD is resistant to **harvest-now-decrypt-later (HNDL) attacks**, where ciphertext is stored for future decryption once computational power becomes sufficiently advanced. This is a significant advantage that PQC does not offer. Cryptosystems like PQC and RSA rely on **computational security**, meaning their security depends on the attacker's computational resources and the efficiency of cryptanalysis algorithms. Consequently, they cannot guarantee protection against unexpected future increases in computational power or breakthroughs in algorithms, making them inherently vulnerable to HNDL attacks.

However, there are variations in QKD protocols, and while each is supported by mathematical security proofs, the security of certain implementations remains uncertain. To ensure that a QKD system achieves the same level of security as its theoretical model, the following three conditions must be met.

(a) The communication protocol used must be supported by a corresponding security

1. The security of RSA and elliptic curve cryptography is based on the assumption that the integer factorization problem and the elliptic curve discrete logarithm problem, respectively, cannot be efficiently solved. Theoretically, it is known that quantum computers can solve these problems efficiently (in polynomial time) using Shor's algorithm. However, the required specifications for quantum computers capable of cryptanalysis are extremely high, and their realization remains out of reach.
2. In Japan, the Tokyo QKD Network (Fujiwara [2023]) has been demonstrated. In Europe, the SECOQC (Secure Communication based on Quantum Cryptography) network and the EuroQCI (European Quantum Communication Infrastructure) network, which involves all 27 EU member states, have been implemented. In China, a QKD network spanning 4,600 kilometers between Shanghai and Beijing has also been demonstrated.

proof.

(b) The **device models** assumed in the security proof must be realistic.

(c) The implemented devices must operate in accordance with the device models assumed in the security proof mentioned in (a).

Condition (a) is necessary because not all proposed communication methods and protocols classified as QKD have been provided with complete security proofs. In 2021, for the first time, an information-theoretic security proof was established for a method called continuous-variable QKD (CV-QKD, see Section III.C.2. for more details), which is highly compatible with existing optical communication technologies (Matsuura *et al.* [2021]).

Condition (b) requires that security proofs be based on practical assumptions regarding communication devices. Security proven under theoretically convenient assumptions is not necessarily guaranteed in real-world communication. This is because such assumptions may be violated due to noise within the communication devices themselves, or sensitive information could be stolen through implementation attacks (see Section IV.A.3. for details), where an attacker directly exploits vulnerabilities in the devices. As a result, recent advancements in security proof theory have shifted toward accommodating realistic properties, including inherent imperfections.

Condition (c) requires that communication devices comply with security specifications. Since it is impractical for user companies to directly verify compliance with these specifications, establishing an institutional framework to evaluate and certify the performance and security of communication devices is essential for the widespread adoption of QKD.

While research and development efforts for the practical implementation of QKD are actively underway, achieving both sufficient performance and compliance with the aforementioned conditions should require more time. Additionally, implementing QKD on a large scale would involve significant network infrastructure costs. As a result, current concrete measures to counter the threat posed by quantum computers primarily focus on PQC, with increasing momentum to transition from contemporary cryptographic methods to PQC. The National Institute of Standards and Technology (NIST) is advancing the standardization of PQC, inviting public submissions for candidate encryption schemes and conducting evaluations. In its Round 3 evaluation report (NIST [2022]), NIST announced the selection of CRYSTALS-KYBER as the standard key encapsulation mechanism for key exchange, while indicating that further evaluations of other candidates would continue in Round 4. The motivation behind this cryptographic transition is to prepare for the emergence of an ideal quantum computer and to address threats posed by HNDL attacks. Moving forward, a shift to stronger cryptographic methods is anticipated, regardless of the timeline for the realization of quantum computers. Even as PQC gains traction, understanding the relative characteristics of QKD and PQC will be valuable for evaluating the potential adoption of QKD and identifying optimal use cases for each approach.

The transition to PQC may take over ten years if it requires updating hardware with integrated encryption modules. Similarly, the deployment of QKD should require an extended preparation period due to the need for building new network infrastructure.

Therefore, early planning is essential when considering the future landscape of cryptographic usage. For financial institutions, where stringent information management is critical, a comprehensive understanding of QKD's security, applicability, and the challenges associated with its practical implementation is vital for developing a long-term cryptographic strategy.

On the basis of the aforementioned information, Section II. outlines the positioning of QKD, Section III. provides an overview of the fundamentals of QKD, Section IV. reviews the security proofs associated with QKD, and Section V. examines the challenges related to the broader adoption of QKD.

II. The Positioning of Cryptographic Communication Using QKD

In Section II.A., we first explain the threat posed by quantum computers to public-key cryptography. Next, in Sections II.B. and II.C., we outline the principles of PQC and QKD, respectively. On the basis of these discussions, Section II.D. organizes the relative strengths and weaknesses of QKD.

A. Public-Key Cryptography and the Threat of Quantum Computers

In classical communication, cryptographic methods are categorized into symmetric-key encryption and public-key encryption. **Symmetric key encryption** enables fast encrypted communication, as it relies on the assumption that the sender and receiver have pre-shared a secret key. **Public-key encryption**, on the other hand, does not require a pre-shared key but generally operates more slowly. Practical communication systems leverage the strengths of both: bulk data is securely transmitted using symmetric key encryption, while the symmetric encryption key is exchanged via public-key encryption.

The predominant forms of public-key cryptography today are RSA encryption and elliptic curve cryptography. The security of these methods is based on the assumption that problems such as large integer factorization and the elliptic curve discrete logarithm problem cannot be solved within a practical timeframe. Security based on the assumed difficulty of specific computational problems is termed **computational security**. This type of security diminishes over time due to advances in computational power and algorithmic breakthroughs, rendering it time-limited. Consequently, cryptographic key lengths are progressively extended to maintain security. Cryptographic schemes relying on computational security are inherently vulnerable to HNDL attacks, posing a realistic threat to entities requiring long-term data protection. In particular, RSA and elliptic curve cryptography are theoretically vulnerable to efficient decryption by quantum computers. If such quantum computers become viable, they could decrypt accumulated ciphertexts.

B. Comparison with PQC

In this section, we provide an overview of PQC, which is often compared with QKD. One approach to addressing the threat of quantum computers is to replace current cryptographic schemes with stronger ones. Schemes that maintain security against quantum

computers are referred to as PQC.

The security of PQC relies on the difficulty of certain computational problems considered intractable even for quantum and classical computers. These problems are closely related to the class of computational problems known as NP-hard[3] in computational complexity theory.[4] However, this theoretical assurance is based on analyzing the asymptotic behavior of computational complexity as the input size grows indefinitely. Crucially, PQC does not guarantee that finite-sized problems with practical key lengths and security parameters are unsolvable within realistic time frames.

The assessment that encryption cannot be broken within practical time frames is based on projections of future advancements in decryption algorithms and computational power. Consequently, it is anticipated that PQC, like RSA encryption, will require operational measures such as increasing key lengths over time. However, significant uncertainty remains in these projections. Notably, many experts emphasize that while the probability of realizing a quantum computer capable of efficient cryptanalysis is extremely low, its impact would be catastrophic, classifying it as a difficult-to-predict tail risk. Computational security cannot fully eliminate such risks.

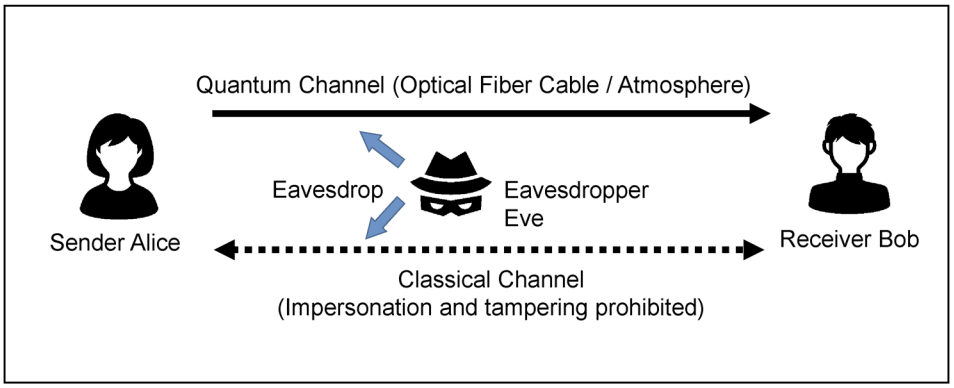
While experimental demonstrations of PQC are progressing, establishing trust in its resistance to implementation attacks and algorithmic security will take time. In contrast, RSA encryption benefits from over two decades of deployment and accumulated implementation expertise. For this reason, a **hybrid mode** combining elliptic curve cryptography and PQC for dual encryption is being standardized by the Internet Engineering Task Force (IETF). Additionally, since PQC encompasses diverse cryptographic algorithms, achieving **crypto-agility**—the ability to flexibly select appropriate algorithms—remains a key challenge. For recent discussions on hybrid modes and crypto-agility, see Une (2023a, b) and Kanno (2023).

Unlike QKD, PQC cannot inherently detect eavesdropping because classical bits[5] can be duplicated without altering the original information. Attackers can thus replicate classical bits transmitted over communication channels without leaving traces, rendering PQC vulnerable to HNDL attacks. In contrast, QKD enables post-transmission eavesdropping detection by statistically estimating its presence, as detailed in Section II.C., enabling compromised information to be discarded and secure key sharing without eavesdropping risks. This advantage, rooted in quantum-mechanical properties, is unattainable in classical cryptography, including PQC.

.....

3. Intuitively, NP-hard refers to a class of computational problems that are difficult to solve efficiently but for which a candidate solution, if provided, can be efficiently verified. More precisely, NP-hard denotes a class of problems that are at least as difficult as the hardest problems in NP (nondeterministic polynomial time). NP is the class of computational problems that can be solved by a nondeterministic polynomial-time algorithm.
4. The computational difficulty of these problems depends on the distribution of their parameters. Furthermore, the interpretation of cryptographic security assessments varies depending on whether they are based on the average computational cost across various parameter settings or the worst-case computational cost. In cryptographic security evaluations, the average computational cost is generally preferred. The lattice-based PQC scheme CRYSTALS-KYBER, selected by NIST as a standard for public-key cryptography, provides a security proof based on the average computational cost under random parameter settings.
5. A classical bit represents a state of either “0” or “1.” A device that performs computations using only classical bits is called a “classical computer.” Cryptography in which plaintext and ciphertext are represented as sequences of classical bits is known as “classical cryptography.”

Figure 1 Overview of QKD Communication



C. Principles of QKD

Another countermeasure against the threat of cryptographic decryption by quantum computers is QKD. QKD leverages quantum-mechanical properties and carefully designed protocols to achieve information-theoretic security. In this section, we explain the principles of QKD.

In QKD, two channels are utilized: a quantum channel for transmitting quantum bits and a classical channel for transmitting classical bits (see Figure 1). The quantum channel provides a low-noise environment essential for the delicate transmission of quantum bits, but it is costly, making it inefficient for sending classical bits. Thus, to efficiently share deterministic information (i.e., keys), the classical channel is typically used in conjunction with the quantum channel. For the classical channel, it is assumed that an attacker can eavesdrop on the communication but cannot impersonate the participants or alter the transmitted content. To satisfy this assumption, the ability to authenticate both participants and messages is necessary. These authentication mechanisms are crucial in evaluating the overall security of QKD protocols. However, for simplicity, we assume that secure authentication is possible here. Issues related to authentication are discussed in detail in Section V.B.

A quantum bit, or qubit, can take a state that is a combination of both "0" and "1," known as a **superposition**. Furthermore, the state of any unknown qubit cannot be copied—a property derived from quantum mechanics called the **no-cloning theorem**. This is a characteristic unique to qubits. In other words, the information contained in a qubit cannot be read without affecting its state.

When extracting information from a qubit, an operation called **measurement** is performed. Generally, an observer cannot fully extract the information of an unknown qubit; instead, the observer can probabilistically obtain partial information through measurement. However, if a qubit is known to be in one of several specific states (though which one is unknown), specific measurement methods can definitively de-

termine the state.[6,7]

For example, consider a situation where an observer performs a measurement on a qubit to distinguish between the "0" and "1" states. If the qubit is in the state "0" or "1," the observer can deterministically identify it. However, if the qubit is in a superposition of these states, the measurement outcome will yield "0" or "1" probabilistically, on the basis of the degree of superposition.

QKD leverages the inherent properties of qubits in a protocol to *retrospectively* estimate the presence or absence of eavesdropping and discard information from suspected qubits, thereby enabling the secure sharing of a random number sequence. Since it is unknown in advance which qubits might be intercepted, QKD cannot be used to directly send an encrypted message. This limitation confines QKD to sharing only random number sequences. Additionally, QKD cannot distinguish between the effects of eavesdropping and environmental noise, making it impossible to definitively confirm eavesdropping. Eavesdropping involves extracting information from a qubit, which alters its state. By following a well-designed QKD protocol, the sender and receiver can detect changes in the quantum state caused by noise or potential eavesdropping, though they cannot determine the exact cause. Thus, in the security analysis of QKD, any change in quantum state is conservatively attributed to eavesdropping, providing a security framework that ensures safety regardless of the cause of state alteration.

Once a random number sequence has been securely shared, any message can be sent securely by the OTP, a classical encryption method that is information-theoretically secure. If the length of the message matches the length of the shared sequence, the message retains information-theoretic security.[8]

D. Positioning of QKD

QKD is frequently compared with PQC as a countermeasure against the threat of quantum computers. As introduced in Section V.A., numerous national white papers and position papers offer negative assessments of QKD from this perspective. However, note that these assessments primarily focus on QKD within the context of broadly applicable Internet encryption schemes. In the following section, we compare QKD with other key-sharing methods, including modern cryptography (RSA encryption and elliptic curve cryptography), PQC, and human-based random number transportation.

As shown in the Table 1, at the current technological level, the most comparable method to QKD in terms of application scenarios is human-based transportation, or the **Trusted Courier** approach, which is primarily suited for one-to-one communication. While it can be used for one-to-many communication if random numbers are transported to multiple locations, it remains poorly suited for many-to-many communica-

6. When known states are mutually orthogonal, they can be determined with certainty. In quantum state measurement, the observer must select an appropriate measurement method (measurement basis) depending on the quantum states they wish to distinguish. The details of quantum state orthogonality and basis selection are beyond the scope of this paper. For more information, refer to foundational texts on quantum computing, such as Nielsen and Chuang (2010).
7. QKD does not utilize orthogonal states to prevent eavesdropping.
8. For example, let the securely shared random number sequence be $x = 010111$ and the message be $y = 111000$. The ciphertext using the OTP is defined as the bitwise exclusive OR $z = x \oplus y = 101111$. In this case, if the random number sequence x is entirely unknown to the attacker, no information about the message y can be inferred from the ciphertext z, ensuring information-theoretic security.

Table 1 Comparison among Encrypted Communication Schemes

	RSA, ECC	PQC	QKD	Trusted Courier
Methodology	Public Key Encryption	Public Key Encryption	Quantum Cryptography	Delivered by Human
Security	Computational Security	Computational Security	Information Theoretic Security	—
Principle of Security	Computational Difficulty of Prime Factorization	Computational Difficulty of NP-Hard Problems[1]	Quantum Mechanics (Laws of Nature)	Closed Channel, Trustworthiness of Courier
Quantum Safe	×	△	○	○
Eavesdropping detection	×	×	○	× (difficult for eavesdropping)
Resistance against Implementation Attacks	Reliable	Not Sufficiently Reliable. Used in Hybrid Mode Recommended	Seems to Sufficiently Consider the Risks. Need to Develop Verification and Certification Frameworks	Reliable
Specialized Devices	Not Required	Not Required for Internet (Implemented as Software) Some Cases Require Replacement of Cryptographic Modules	DV-QKD Requires Dedicated Networks CV-QKD Can Coexist with Existing Optical Networks	Not Required
Network Topology	from N to N	from N to N	from N to N	1 to N
Secured Area	End-to-End	End-to-End	Between Specialized Devices Need to Trust Relay Nodes[2]	End-to-End
Authentication	○	○	PQC Signature Offers Computational Security Wegman-Carter Authentication Requires Small Pre-Shared Key	Certification of the Courier

Notes: 1. There are several PQC encryption schemes with corresponding computational problems of which difficulties guarantee their security.
2. The trust to relay nodes will be less required if quantum relay will be realized.

tion. This limitation stems from the significant time required for key (random number sequence) transportation and the burden of securely managing keys equal in length to the total message volume communicated over a period. In contrast, QKD, as long as a communication path is available, is better suited for many-to-many communication between nodes and enables rapid key sharing per communication instance.

As noted earlier, QKD's primary advantage is its information-theoretic security. It is well-suited for communications involving a limited number of nodes, even in many-to-many configurations, where long-term confidentiality or highly sensitive information is critical. Examples include genetic information managed by life insurance companies and certain financial institutions' credit information. However, if only the main communication line between sender and receiver buildings is protected by QKD, securing the "last mile" of communication, from the QKD receiver device to individual user terminals on the receiver's side, may still require alternative methods. Additionally, since **quantum relay**[9] technology remains underdeveloped, implementations must rely on trusted conventional relay devices.

Conversely, for information requiring confidentiality for approximately 10 years, PQC is likely more cost-effective. Similarly, if the security of the shared random number sequence can be ensured through other means—such as a one-time password generator used by financial institutions—QKD's advantage diminishes. Furthermore, QKD does not authenticate participant identities, necessitating supplementary authentication methods as discussed in Section V.B. Given these significant differences in security guarantees, applications, and assumptions between QKD and PQC, careful selection and complementary deployment of these technologies are essential.

III. Fundamentals of QKD

A. Embedding Quantum Bits in Light

In QKD, light serves as the medium for carrying qubits due to its stability at room temperature and its ability to propagate at the fastest possible speed. One example of a qubit utilizes a property of light called **polarization**. As an electromagnetic wave, light naturally oscillates in various directions of electric and magnetic fields. When passed through a polarizing filter, light with oscillations restricted to a specific angle is extracted, a state referred to as polarization. Digital information can be encoded in these oscillation angles.[10] Polarization may take the form of **linear polarization**, where the oscillation angle remains constant (typically represented by four states: 0°, 45°, 90°, and 135°) or **circular polarization**, where the oscillation angle rotates (either clockwise or counterclockwise) as light propagates. In addition to polarization, qubits can also be encoded using two phase-controlled light pulses with defined **phase differences**. All these encoding methods—linear polarization, circular polarization, and phase-controlled pulses—are theoretically equivalent for realizing qubits.

QKD protocols that treat single photons as qubits benefit from theoretically straightforward security proofs. However, practical implementations face challenges in achieving precise control over single-photon generation. For this reason, weak light pulses—short laser bursts attenuated to approximately the single-photon level—are commonly used in practice.

9. Quantum relay refers to a relay method in which the relay device receives quantum bits and forwards them to the next relay device without converting them into classical bits.
10. In classical communication, information is transmitted by associating the on-off states of light with the bits "0" and "1."

B. Communication Channels and Relays in QKD

Quantum channels consist of optical fiber cables for terrestrial communication or the atmosphere for satellite-to-ground communication, resembling conventional optical or satellite communication systems. However, in quantum channels, the optical signal's intensity is extremely weak, necessitating exceptionally low-noise tolerance. In several QKD implementations, signals are handled at the single-photon level, making long-distance communication challenging due to increased noise. Thus, establishing reliable relay points is crucial, often referred to as **trusted nodes** or **trusted points**, at regular intervals along the communication route.

In general, increasing the distance between relay points reduces the cost of building a network. However, this comes at the expense of slower key generation rates due to the attenuation of light in the communication channel. As of February 2024, in the most commonly implemented QKD protocol—the decoy-state BB84 protocol[11] (Hwang [2003]; Lo, Ma, and Chen [2005]; Wang [2005])—the key generation rate decreases tenfold for every additional 50 kilometers of optical fiber distance. At a distance of 50 kilometers, the transmission speed is at most approximately 1 megabit per second. Consequently, the distance between relay points is constrained by the required speed of key generation.

Relay methods in QKD can be categorized into classical relays and quantum relays. In **classical relays**, qubits are read at each relay device, converted into classical bits, and then re-encoded into qubits for transmission to the next relay device. To prevent information leakage from stored data within each relay device, safeguarding the devices is essential.

Quantum relays eliminate the effects of light attenuation in the channel. Since the relays avoid conversion into classical bits, stringent protection of the relay devices is not required. However, as of now, quantum relays have yet to be established.

C. Classification of QKD Protocols

While the decoy-state BB84 protocol is the most commonly employed in demonstrations and commercialization, many other protocols have also been proposed. These protocols are classified on the basis of communication schemes, the type of optical detectors, and device reliability.

1. Classification by communication schemes

QKD protocols can be categorized into the following three types on the basis of the communication schemes between the two parties:

- **Prepare-and-Measure QKD (PM-QKD)**: One party transmits light while the other measures it. Examples include the BB84 protocol and the decoy-state BB84 protocol.
- **Measurement-Device-Independent QKD** (**MDI-QKD**; Lo, Curty, and Qi [2012]): Both parties send light to a device at an intermediate point. At the

11. For details on the BB84 protocol, refer to Section III.D. The decoy-state BB84 protocol is a variant of the BB84 protocol that uses weak laser pulses (light pulses), which are cost-effective and easier to handle, instead of single photons. The sender randomly selects the intensity of the laser pulses from a predefined set of values and transmits them. This approach ensures performance equivalent to that of the single-photon-based protocol.

device, the incoming lights are interfered with and measured. The outcomes are then disclosed. A notable example is the Twin-Field protocol (Lucamarini *et al.* [2018]).

- ➢ **Entanglement-Based QKD (EB-QKD)**: The device at an intermediate point generates pairs of correlated photons (quantum entangled[12] photon pairs). One photon from the pair is sent to the sender and the other to the receiver. Each then independently measures the photons they receive. Examples include the BBM92 protocol (Bennett, Brassard, and Mermin [1992]) and the E91 protocol (Ekert [1991]).

The characteristics of the protocols are as follows: **PM-QKD** is the simplest type and has already been widely commercialized. **MDI-QKD** requires a measurement device placed at an intermediate point in the channel. This method offers an advantage: even if the measurement device is entirely under the control of an eavesdropper, any eavesdropping attempts can still be detected as errors. Moreover, the protocol's security is guaranteed regardless of whether the outcomes at the measurement device can be trusted. Additionally, depending on the specific protocol, MDI-QKD can significantly reduce the impact of performance degradation caused by distance. Compared with PM-QKD, MDI-QKD can effectively double the communication distance before encountering similar levels of performance degradation. Furthermore, MDI-QKD is considered robust against **implementation attacks**, which often target receiver devices. This robustness stems from the fact that both parties use transmitter devices in MDI-QKD. In contrast, receiver devices are generally more vulnerable to such attacks, as they must accept signals from the communication channel, which is exposed to potential manipulation by eavesdroppers. For a detailed discussion on implementation attacks, refer to Section IV.

In **EB-QKD**, the use of specialized light sources capable of generating entangled photon pairs typically results in higher costs and complexity, making it less common in practice. However, EB-QKD offers certain advantages, such as reducing the need for random number generators. Additionally, it is considered useful for **frequency-division multiplexed communication** (Wengerowsky *et al.* [2018]), though it requires specific optical fibers for optimal performance.

2. Classification by optical detectors and the advantages of CV-QKD

QKD protocols can be categorized into two types on the basis of the optical detectors: **Discrete-Variable QKD (DV-QKD)** and **Continuous-Variable QKD (CV-QKD)**. The terms "DV" and "CV" originally referred to whether the transmitted information was discrete or continuous. However, in modern implementations, even CV-QKD can transmit discrete information. Thus, the prefixes "DV" and "CV" are now used primarily to distinguish the types of detectors employed in the protocols.

- ➢ **DV-QKD**: This approach employs **photon detectors** to identify the presence or absence of individual photons. For example, by placing a photon detector behind a polarization filter (or a polarization beam splitter), the polarization angle of

12. The measurement outcomes of particles in quantum entangled states are correlated regardless of the distance between them. Quantum entanglement is a fundamental quantum mechanical property in quantum computing but is not essential for QKD.

the photon can be determined. All QKD protocols discussed so far fall into this category.

- **CV-QKD**: This approach uses **optical detectors**, employing techniques like homodyne detection or heterodyne detection (dual-homodyne detection),[13] to measure the amplitude of light. In this case, the sender encodes information in the amplitude of the light. Historically, the GG02 protocol (Grosshans *et al.* [2003]) is a well-known example. However, many modern protocols do not have specific names.

Photon detectors are devices designed to detect the presence or absence of extremely weak light, such as single photons. In practice, most photon detectors distinguish between 0 photons and 1 or more photons, a process referred to as on-off photon detection. DV-QKD, which leverages the properties of single photons, enables simpler descriptions of quantum states, making security proofs more straightforward. However, it has limitations: DV-QKD is susceptible to interference from strong light signals used in classical communication operating at similar frequencies. Additionally, photon detectors are expensive, making cost-effective implementation of DV-QKD challenging.

Optical detectors measure the intensity of light but cannot detect light as weak as single photons. To overcome this limitation, homodyne and heterodyne detection amplify weak single-photon-level light by interfering it with laser light before measurement by the optical detector. CV-QKD has a cost advantage over DV-QKD, as optical detectors are inexpensive.

Another advantage of CV-QKD is its ability to share optical fiber networks with classical communication. In optical communication, signals can be multiplexed on a single optical fiber by encoding them on light pulses of different wavelengths, thereby increasing communication capacity. This technology is known as **wavelength-division multiplexing (WDM)**. CV-QKD's light measurement benefits from wavelength filters, which selectively isolate the desired wavelength of light. Thus, CV-QKD is less affected by signals at other wavelengths, making it more robust than DV-QKD. By assigning a dedicated wavelength to CV-QKD within a WDM system, it becomes possible to coexist with classical optical communication systems without requiring new optical fiber installations.

According to Pirandola *et al.* (2017), CV-QKD has the potential to surpass DV-QKD in communication speed, provided that theories and implementation technologies continue to advance. However, establishing security proofs for CV-QKD is not straightforward. The first security proof for a practically implementable discrete-modulated CV-QKD protocol was provided by Matsuura *et al.* (2021). As of February 2024, existing CV-QKD protocols with established security proofs still exhibit inferior performance compared with DV-QKD. Thus, future improvements in CV-QKD performance depend on advancements in protocols, device implementation, and theories for security

13. This is a detection technique for measuring weak optical signals, characterized by its resistance to noise from light with different frequencies. In homodyne detection, the target optical signal is combined with a reference light, amplified, and then converted into an electrical signal by a detector. In this process, the target and reference lights must have the same frequency. Heterodyne (or dual-homodyne) detection, on the other hand, splits the input light into two parts and performs homodyne detection on each, using reference lights with a phase difference of one-quarter wavelength.

proofs.

3. Classification by device reliability

QKD protocols can also be classified on the basis of assumptions regarding the reliability of the devices. These assumptions affect both the security proofs and the design of the communication protocols.

- ➢ **Device-Dependent QKD (DD-QKD)**: This approach assumes that the devices function consistently with their specified models, and security is guaranteed under this assumption. All the QKD protocols discussed earlier fall under this category.
- ➢ **Device-Independent QKD (DI-QKD)**: In this approach, security is guaranteed under minimal assumptions about the devices. Specifically, it assumes that the devices do not leak information intended for the sender or receiver to an eavesdropper, that they can generate genuine random numbers, and that they do not possess internal memory storage (Barrett, Colbeck, and Kent [2013]). An example is the E91 protocol.

DI-QKD adopts a security-proof approach that does not rely on specific device models. Due to the limited assumptions available for security proofs, developing protocols with security proofs is highly challenging. However, because DI-QKD does not assume particular device models, the number of testing criteria for verifying device properties is smaller compared with DD-QKD.

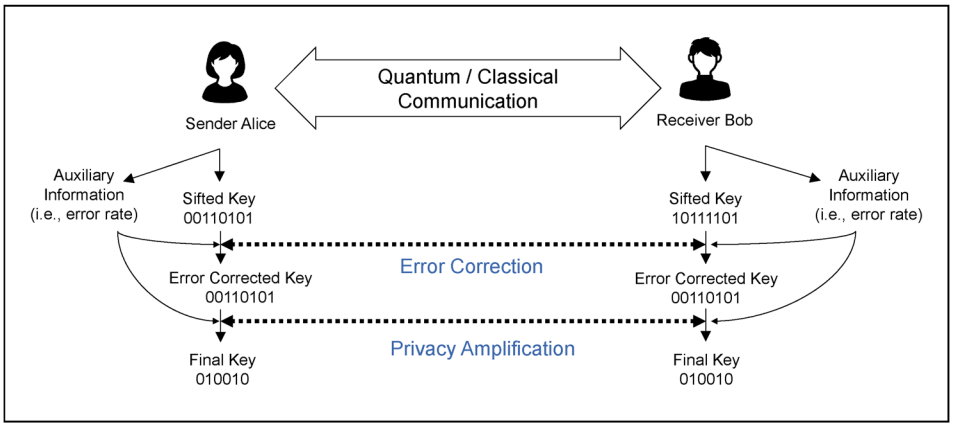
When considering the differences between DI-QKD and DD-QKD, the following two points should be noted. First, it is sometimes misunderstood that DI-QKD does not require device verification since it avoids assuming specific device models. However, it is necessary to verify that the devices satisfy fundamental theoretical assumptions. These assumptions are not about specific device models but are universal and fundamental from a quantum-mechanical perspective, as required by Bell experiments. Second, in both types of QKD, ensuring that devices do not leak information intended for the sender or receiver to an eavesdropper is essential. This requirement remains critical for addressing implementation attacks, leaving little difference between the two types of QKD. Given this point, the fundamental differences between DI-QKD and DD-QKD remain subject to debate.

From a performance standpoint, however, DI-QKD has drawbacks. Without advanced components such as **quantum memory** for preserving qubits, its performance is drastically inferior to DD-QKD. Furthermore, long-term retention of qubits poses considerable technical challenges. Several experts estimate that the practical implementation of DI-QKD may require over 20 years of further development. Thus, unless otherwise specified, the following discussion assumes DD-QKD.

D. Basic Structure of the Protocol

A representative QKD protocol is the BB84 protocol (Bennett and Brassard [1984]). BB84 was introduced by Charles Bennett and Gilles Brassard in 1984 and was named after the initials of its proposers and the year of its proposal. Experimental demonstrations of QKD conducted across various countries are mostly based on the BB84 protocol. For details of this protocol, excellent resources are already available in the

Figure 2 Three Broad Steps of the QKD Protocol



literature. Readers are encouraged to refer to Koashi and Koshiba (2008), Goto (2009), and Nielsen and Chuang (2010).

This section outlines an overview of QKD protocols (see Figure 2). Most QKD protocols, including the BB84 protocol, are executed in three broad steps. In Step 1, an incomplete random number sequence, known as the **sifted key**, is shared. In Steps 2 and 3, the secure portions of the sifted key are extracted, and the **final key** is obtained. Each step is described in the following.

Step 1 involves sharing the sifted key. A random number sequence is shared, and the states of the quantum and classical channels are monitored. Specifically, in PM-QKD, the sender transmits a sequence of qubits through the quantum channel, while the receiver measures the qubits. During this process, the sender probabilistically switches between types of quantum states, and the receiver also switches between types of measurement methods (**measurement bases**; see Footnote 6). These choices are later communicated and reconciled between the sender and receiver via the classical channel. The random number sequence shared during this step is not perfectly identical between the sender and receiver due to noise.[14] Moreover, there is a possibility that parts of this sequence have been intercepted by an eavesdropper. This imperfect sequence is referred to as the **sifted key**.

Step 2 involves **error correction**. By communicating partial information about the sifted key (e.g., **syndromes** in error-correcting codes) through the classical channel,[15] the sender and receiver identify discrepancies in their keys and correct one party's key to match the other's. This procedure is analogous to error correction in a noisy classical channel. The proportion of discrepancies is referred to as the **error rate**, and the length of the obtained key increases as the error rate decreases.

Step 3 involves **privacy amplification**. A random number sequence independent of the key is shared via the public classical channel. Using a predetermined algorithm,

14. For example, noise in the communication channel, eavesdropping by an attacker, and quantum mechanical fluctuations in measurement outcomes.
15. In some protocols, it is necessary to encrypt and transmit information using a pre-shared key. In such cases, the key generation rate of the protocol is defined as the total amount of keys generated minus that of the pre-shared keys used during this step.

the key is shortened to eliminate any partial information that may have leaked to a potential eavesdropper. The more information suspected to have leaked, the shorter the key must be adjusted. As a result of this process, the sender and receiver can share a highly secure and identical key with an extremely high level of certainty.

IV. Theory of Security Proof in QKD

A. Security Criteria and Assumptions for Security Proofs

The components of a QKD security proof include the security criteria that define the level of security to be proven, the device model that mathematically represents the properties of the communication devices, and the QKD protocol itself.

1. Security criteria

The security criteria, which serve as the goal of a security proof, are based on information-theoretic security. A protocol is considered secure if the key shared by a real-world protocol P_{real} is indistinguishable from the key shared by an ideal protocol P_{ideal}, where the ideal protocol assumes no noise or eavesdropping in the channel and achieves perfect secrecy.[16] This indistinguishability is referred to as ϵ-indistinguishability, defined as follows.

Given a positive constant ϵ, a real-world protocol P_{real} and an ideal protocol P_{ideal} are **ϵ-indistinguishable** if, for any distinguisher, the following condition

$$|\Pr[B = 1|P_{\text{real}}] - \Pr[B = 1|P_{\text{ideal}}]| \leq \epsilon,$$

holds. Here, a **distinguisher** is a virtual entity that attempts to differentiate between the two protocols. On the basis of its evaluation, the distinguisher outputs an estimate B. If the distinguisher identifies the protocol as ideal, it outputs $B = 1$; if it identifies it as real, it outputs $B = 0$. The probability of obtaining an estimate B under a given protocol P is denoted as $\Pr[B|P]$. Satisfying ϵ-indistinguishability for all possible distinguishers ensures security against all possible eavesdropping attempts, forming the basis for the protocol's information-theoretic security.

A protocol that ensures the shared key satisfies this property is referred to as **ϵ-secure**. The positive constant ϵ, which can be set to any desired value by the QKD user, intuitively represents the maximum probability that the real protocol's outcome deviates from that of an ideal protocol.

2. Assumptions for security proofs

The proof of QKD's information-theoretic security (or **unconditional security**[17]) relies on a set of mathematical assumptions about the abilities of the sender, receiver, and eavesdropper, as well as the device models and the QKD protocol itself. These assumptions include the following.

(a) On the quantum channel, the attacker can perform any attack including interception and eavesdropping.

16. This security criterion ensures closeness in terms of the trace distance between the ideal and real states.
17. The term "unconditional" in this context has a limited meaning, indicating that no specific conditions are imposed on the quantum communication channel.

(b) On the classical channel, the attacker can eavesdrop but cannot impersonate either party or tamper with the transmitted data.
(c) Both the sender and receiver can generate genuine random numbers.
(d) The devices function precisely in accordance with the device models.
(e) The eavesdropper has no direct access to the internal components of the devices.

Assumption (a) considers extreme attacks, such as denial of service (DoS) attacks in which the attacker observes all qubits or completely severs the channel. In such cases, the length of the shared key becomes zero. This highlights a fundamental characteristic of QKD: while its security is always guaranteed, the ability to share a key is not.

Assumption (b) indicates that authentication of the parties and messages is securely conducted. Although authentication methods are established for classical communication, it is essential to recognize that the security of authentication is encompassed within the overall security of the QKD protocol. For further details, see Section V.B.

Assumption (c) presumes that the sender and receiver possess secure physical random number generators. These generators can be based on quantum or classical pseudorandom methods, but the associated risk profiles differ. Classical pseudorandom generators are susceptible to backdoor attacks and inherently carry a risk of random number prediction. Quantum random number generators (QRNGs) are believed to have a lower risk of backdoor attacks, but they still have a risk stemming from other types of attacks.[18]

Assumption (d) defines the device model as an abstraction of real-world devices, mathematically described within the framework of quantum mechanics.

Assumption (e) presumes that the attacker cannot directly steal the classical bits of random number sequences stored inside the devices. It is notable that this assumption does not rule out the possibility of remote extraction attacks. Additionally, regarding implementation attacks, the associated risks are inherently tied to the assumptions of the device model.

Under these assumptions, the security of the QKD protocol is established.

3. Relationship between assumptions for security proofs and the threat of implementation attacks

The security of QKD is proven based on the assumption that devices operate in accordance with their device models. However, discrepancies between real-world devices and their theoretical models may be exploited by attackers, enabling eavesdropping or tampering. Such risks pose significant threats of implementation attacks to QKD.

Implementation attacks encompass any attacks that break cryptographic security without relying on design flaws in the protocol or cryptographic weaknesses.[19] In QKD,

.....

18. For example, it is necessary to consider the risk of attacks that replicate random numbers output by a random number generator through some means.
19. For details on implementation attacks, see, for example, Suzuki, Sugawara, and Suzuki (2015). In classical cryptography, implementation attacks are classified into invasive attacks, which involve direct physical access to the internal components of a device, and non-invasive attacks, which do not require such access. Non-invasive attacks can be further divided into side-channel attacks, where the normal operation of a device is passively observed, and fault-injection attacks, where errors are actively induced in the device to observe

these are defined as attacks that compromise the assumptions of the device model. Importantly, such attacks invalidate the security guarantees provided by mathematical proofs.

One example of an implementation attack in QKD involves exploiting vulnerabilities in the photon detectors on the receiving side. If a detector is exposed to extremely intense light, it may become damaged, rendering it unresponsive to light below a certain intensity. An attacker could exploit this phenomenon by ensuring that the receiver detects signals only on specific measurement bases chosen by the attacker. This enables eavesdropping without introducing detectable errors, thereby bypassing the QKD protocol's error-checking mechanisms.

To mitigate such risks, countermeasures can be employed, such as introducing MDI-QKD as described in Section III.C.1., or by actively monitoring the intensity of incoming light to the receiver to detect potential attacks.

In general, however, anticipating and mitigating unknown implementation attacks in advance is challenging. Thus, countermeasures against implementation attacks typically focus on addressing known attack methods. Over the nearly 40-year history of QKD, particularly in the past two decades, knowledge has been accumulated regarding device models tailored to real-world devices and countermeasures against implementation attacks.

In theoretical research, efforts have been made to redesign QKD protocols—especially the processes for privacy amplification—by incorporating device imperfections as assumptions. Such redesign efforts have helped extend security proofs to account for potential risks posed by these imperfections, effectively nullifying certain vulnerabilities.

In practice, verifying whether devices operate in accordance with their theoretical models requires experimental testing of actual devices. This highlights the need for developing standards for device specifications and establishing institutional frameworks for verification and certification. For further details on this topic, see Section V.C.

Finally, even in QKD, once information is converted into classical bits, the devices become vulnerable to implementation attacks as classical systems. Thus, standard countermeasures used in classical systems must also be applied to QKD devices.

B. Advances in QKD Security Proofs

Section IV.B provides an overview of the evolution of research on QKD, focusing on the **security criteria** and the **device imperfections**.

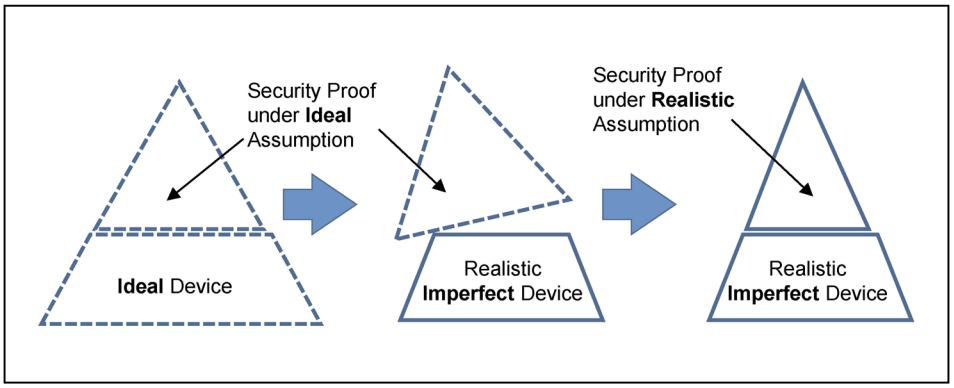
Since the proposal of the BB84 protocol, the theory for proving QKD security has continuously evolved. Typically, QKD security proofs begin by adopting idealized assumptions that are conducive to mathematical analysis. These studies have driven advancements in research on security criteria for QKD protocols.

abnormal behavior.

An example of a side-channel attack includes methods that extract information about plaintext by observing electromagnetic emissions or power consumption from a processing device during encryption or decryption operations.

In the case of QKD, a classification of implementation attacks similar to those for classical cryptography has not been well-established. Furthermore, implementation attacks are sometimes referred to as side-channel attacks, so caution should be taken with the use of terminology.

Figure 3 Device Imperfection and Security Proof



However, a key challenge has been the gap between the assumptions required for theoretical security proofs and the practical constraints of real-world devices. To address this, researchers have developed improved proofs that incorporate device imperfections as explicit assumptions. These advances enable security proofs that preserve QKD performance while accounting for risks posed by implementation attacks and other practical limitations (Figure 3).

The following subsections discuss these two research streams. Section IV.B.1. explains the research on security criteria. Section IV.B.2. explains the research on security proofs incorporating device imperfections.

1. Advances in research on security criteria

The first QKD protocol was the BB84 protocol, in which the sender generates ideal single photons and encodes their polarization in one of four states (0°, 45°, 90°, 135°) before sending them to the receiver. The receiver, using photon detectors, measures the polarization of the photons. The original paper by Bennett and Brassard (1984) claimed that the protocol was information-theoretically secure over an idealized noiseless channel. However, this claim faced criticism, as real-world channels inevitably contain noise, rendering the original security proof incomplete.

In response to these criticisms, Mayers (1996) extended the security proof for the BB84 protocol to account for noisy channels and imperfect measurement devices. This work advanced the field, establishing a broader consensus among researchers that QKD could indeed achieve information-theoretic security. However, the security criterion used in Mayers' proof was fundamentally based on **mutual information**.[20]

Subsequent research by Müller-Quade and Renner (2009) revealed that mutual information was insufficient as a security criterion. Their findings raised the consensus among researchers that ϵ-security, an information-theoretic security criterion, should be adopted (see the definition of ϵ-security in Section IV.A.1.). Today, ϵ-security is the

20. Mutual information is a metric that represents the degree of dependency between two random variables and can be interpreted as the amount of information about one random variable obtained from the other. Intuitively, if the information about the secret key that can be derived from the quantum information processing system executing a QKD protocol (i.e., the values of certain random variables) is small, the protocol could be considered secure.

    On the basis of this intuition, a security criterion using mutual information was developed. However, counterexamples have demonstrated that a protocol is not necessarily secure despite this intuitive reasoning.

de facto standard security criterion for QKD protocols.[21]

2. Advances in research incorporating device imperfections

Even when ϵ-security is guaranteed, the significance of the security heavily depends on the underlying assumptions. For device models, several critical aspects must be considered, including the feasibility of procuring devices that meet the model's requirements, the extent of losses and noises in the devices, the accuracy of performance metrics, and the methods for verifying these metrics.

One challenge involves the light source used in the BB84 protocol. The original security proof assumed the availability of an ideal single-photon source. However, realizing such an ideal source is technically difficult, so practical implementations typically use laser sources with average photon intensities reduced to the single-photon level.

Nonetheless, laser sources inherently emit **multiple photons** with a certain probability, violating the assumptions of the original security proof. This discrepancy introduces vulnerabilities that can be exploited by attackers. For instance, when multiple photons with identical quantum states are emitted, an eavesdropper could intercept one photon while forwarding the remaining photons to the receiver. Since the eavesdropper leaves no trace of their interference, the attack compromises the security of the protocol without introducing detectable errors. Thus, regardless of analysis, it is fundamentally impossible to derive a secure key from signals containing multiple photons under the BB84 protocol.

Furthermore, laser light in reality exists as a **superposition of single-photon and multi-photon states**, creating additional risks of efficient eavesdropping via implementation attacks. To mitigate these risks, countermeasures involving phase randomization of the laser light have been developed. This randomization—achieved using laser oscillation instability or phase modulators—transforms the laser light into a probabilistic mixture of classical states corresponding to various photon numbers, neutralizing attacks that exploit its quantum superposition nature.

The methodology for proving security under such conditions was established by Gottesman *et al.* (2004). However, this approach introduced a drawback: long-distance communication performance was substantially lower compared with systems using ideal single-photon sources.

To address the performance decline, **decoy-state QKD** (Hwang [2003], Lo, Ma, and Chen [2005], Wang [2005]) was proposed. In this protocol, the sender probabilistically varies the intensity of laser pulses, and the receiver analyzes the corresponding detection rates. If an attacker selectively targets multi-photon states, changes in detection rate ratios reveal the attack's presence.

Decoy-state QKD offers the following benefits. First, the average key generation rate per pulse improves to levels comparable with those achievable with ideal single-photon sources, even over long distances. Second, laser sources with high pulse repetition rates outperform single-photon sources in average key generation rate per unit time.

Decoy-state QKD exemplifies advancements in QKD protocols and security proofs addressing device imperfections, as illustrated in Figure 3. Beyond this study, Sajeed *et*

21. For the approach in security proofs based on ϵ-security, please refer to the appendix.

al. (2021) provide a comprehensive survey of other device imperfections.[22] For many known implementation attacks exploiting such imperfections, basic countermeasures have been devised. For unknown implementation attacks and device imperfections with unclear security implications, Pereira *et al.* (2020) proposed a methodology to handle discrepancies between adopted device models and idealized models. Their framework quantifies these differences using fidelity-like metrics, ensuring QKD system security if discrepancies remain sufficiently small.

Many frameworks addressing device imperfections include provisions for verifying noise levels in devices as part of their security guarantees. Thus, simplifying device property testing and ensuring high QKD protocol performance remain key challenges in the field.

V. Discussion

This section examines the challenges toward the widespread adoption of QKD.

Section V.A. reviews position papers on QKD published by national information security organizations and agencies. Section V.B. discusses authentication in QKD. Section V.C. summarizes the standardization of QKD protocols and technologies. Finally, Section V.D. explores the key challenges toward the adoption of QKD, on the basis of the preceding discussions.

A. International Assessments of QKD

Information security agencies and related authorities from various countries have published documents evaluating QKD. Many of these assessments express skepticism regarding the practicality and cost-effectiveness of QKD. However, note that these evaluations often assume a comparative context with PQC, specifically focusing on general-purpose encryption used in Internet communications.

Reviewing these documents, QKD is not currently viewed as a viable alternative to PQC in terms of performance and cost. Its primary advantage lies in its information-theoretic security, which is particularly beneficial for scenarios requiring ultra-long-term confidentiality or for addressing risks such as the secret compromise of PQC or the threat of HNDL attacks. Thus, the value of QKD depends on its application context.

As discussed in Section II.D., QKD is best suited for the transmission of highly confidential information with restricted applications. Thus, its most appropriate comparison is likely with trusted courier systems rather than PQC. In any case, constructive discussions about the appropriate use cases for QKD and its differentiation from PQC should consider evaluations from cryptographic experts.

The following provides a summary of the evaluations of QKD by national authorities.

The U.S. National Security Agency (2021) has stated that it does not recommend the use of QKD in National Security Systems unless the following technical limitations are addressed.

22. For example, the uncertainty in the sender's ability to perfectly prepare qubits in the desired states is taken into consideration.

(a) QKD does not provide authentication mechanisms equivalent to digital signatures.
(b) QKD requires dedicated communication devices.
(c) QKD relies on trusted relays, which increases infrastructure costs.
(d) The actual security guaranteed by QKD depends on the implementation of the communication devices.

The authors consider these constraints, highlighted in the discussions by the NSA and other nations, as follows.[23] Limitation (a) does not significantly undermine the utility of QKD. For further details, please refer to Section V.B. Limitations (b) and (c) primarily relate to the issue of initial implementation costs. In scenarios requiring ultra-long-term confidentiality, QKD remains a promising option even with such costs. Additionally, studies have proposed cost-effective approaches that integrate existing communication lines with QKD-based systems, providing further support for its adoption. Regarding limitation (d), similar constraints apply to classical cryptographic systems, including PQC. Nevertheless, for QKD, the establishment of institutional frameworks to certify device security remains a challenge. For further discussion, see Section V.C.

The United Kingdom's National Cyber Security Centre (NCSC) also expressed its position on QKD in a white paper on cryptographic transition published in November 2020 (National Cyber Security Centre [2020b]). Citing reasons similar to the aforementioned limitations (a) and (b), the NCSC recommended against the use of QKD in all government and military institutions. Further details on these reasons were elaborated in another white paper on QKD and quantum random number generation, released in March of the same year (National Cyber Security Centre [2020a]).

The Netherlands National Communications Security Agency (2022) has similarly criticized QKD, citing limitation (a) as a vulnerability to man-in-the-middle attacks. A man-in-the-middle attack occurs when an attacker intercepts and manipulates communication between a sender and receiver, who mistakenly believe they are directly communicating with each other, thereby enabling an attacker to eavesdrop or alter the transmitted information. To address this vulnerability, the use of PQC for authentication has been proposed; however, doing so would undermine the relative advantages of QKD to PQC. Additionally, the agency noted that the security proofs for QKD are incomplete because they fail to account for the entire application environment in which QKD is implemented. Many of the assumptions regarding the devices are unrealistic. Moreover, QKD suffers from limitations in communication distance, the necessity of numerous trusted points, and poor scalability. On the basis of these considerations, the agency concluded that QKD cannot serve as a viable substitute for PQC.

A position paper ANSSI (2023) published by France's National Agency for the Security of Information Systems (Agence Nationale de la Sécurité des Systèmes d'Information: ANSSI) highlighted the challenges of large-scale deployment of QKD, emphasizing that the risks posed by universal quantum computers are already

23. Additionally, Renner and Wolf (2023) have reviewed and countered the NSA's evaluation. Their paper concludes that many of the issues raised by the NSA regarding QKD will be resolved in the medium- to long-term future. Here, the medium-term future refers to an era when affordable optical devices and quantum repeaters become available, while the long-term future refers to a time when quantum computers are interconnected via quantum networks.

addressed within PQC. While the paper acknowledged the potential niche applications of QKD, such as secure communication between critical sites, it also pointed out that QKD fails to meet many of the functional requirements demanded by modern communication systems, including scalability, high transmission speed, and end-to-end encryption. Thus, the agency concluded that PQC is a more suitable option for long-term data protection.

In a joint position paper released by the information security authorities of France, Germany, the Netherlands, and Sweden (ANSSI *et al.* [2024]), additional limitations of QKD, as outlined by the U.S. NSA, were reiterated. The paper notes that QKD's constraints on transmission speed preclude its use for encrypting data payloads. Instead, the data must be encrypted using symmetric cryptography rather than OTPs, meaning that QKD cannot guarantee information-theoretic security for the data itself. Moreover, it is argued that the theoretical security assurances of QKD are not directly applicable to its practical implementations in real-world devices. On the basis of these considerations, the paper concluded that QKD remains an immature technology and, for the time being, is limited to niche applications.

However, in the authors' view, QKD holds the potential to be effectively combined with OTPs by continuously running the QKD protocol to accumulate keys even during periods of non-use. This approach enables the practical encryption of data payloads using OTPs. Furthermore, as discussed in Section IV., security proofs now increasingly account for device imperfections, thereby narrowing the gap between theoretical guarantees and practical implementations.

B. Discussion on Authentication

As noted in Section V.A. with reference to the evaluation of the U.S. NSA, QKD has been criticized for not providing an inherent authentication mechanism. Without mutual authentication, QKD becomes vulnerable to man-in-the-middle attacks. However, since QKD utilizes both quantum and classical channels, integrating any desired authentication mechanism is feasible through the classical channel. Ideally, mutual authentication should be conducted before initiating key sharing to verify the legitimacy of the communication partner.

This section discusses how the choice of authentication mechanism integrated with QKD impacts the assumptions and security evaluations of the entire QKD protocol, including authentication. In particular, as explained later, even if the authentication mechanism is based on computational security, this does not necessarily undermine the overall utility of QKD.

Many QKD protocols aim to achieve information-theoretic security not only for the key distribution process but also for authentication. To this end, they often incorporate the **Wegman-Carter authentication** scheme (Wegman and Carter [1981]), designed to ensure information-theoretic security. This scheme assumes that the sender and receiver share a small number of secure random numbers in advance—no more than the logarithmic scale of the classical communication volume. Under the use of Wegman-Carter authentication, QKD should more accurately be described as "key growing" rather than "key distribution." In this sense, QKD can be viewed as a mechanism for prolonging the secure random number sequence pre-shared for Wegman-Carter authen-

tication.

If information-theoretic security is not required for mutual authentication, computationally secure authentication may also be employed. For instance, digital signatures based on elliptic curve cryptography can be used. However, because it does not guarantee security against quantum computers, there remains a risk of impersonation.

Digital signatures based on PQC provide security against quantum computers. In this case, as discussed in Section II.D., this leads to criticisms that QKD offers little relative advantage over PQC. Nonetheless, the importance of information-theoretic security for authentication is generally lower than that for data confidentiality.

In authentication, it is sufficient to ensure the authenticity of the communication partner only during the limited timeframe in which message exchange occurs. Even if the authentication mechanism is based on computational security and could potentially be compromised in the future, impersonation of the partner would have no practical impact once the exchange is completed. Thus, in practice, as long as computationally secure authentication mechanisms cannot be broken within the short timeframe, the utility of QKD in ensuring the confidentiality of the data payload remains largely intact.

C. Standardization of QKD

A challenge of QKD is to establish an institutional framework to verify and certify the security of its communication devices. Toward this goal, international standardization is being promoted. Such frameworks are expected to promote the adoption of QKD by providing formal certification of cryptographic products' security on the basis of international standards.

To provide context, the following provides an overview of the institutional frameworks for classical cryptographic products. Institutional frameworks for third-party evaluation and certification have been established and are currently in operation. In Japan, the **Japan Information Technology Security Evaluation and Certification Scheme (JISEC)**[24] provides a framework under which the security functions of products and systems are defined and assessed on the basis of the Common Criteria (CC) established by the International Organization for Standardization (ISO/IEC 15408). These assessments certify whether the security functions are appropriately implemented. Additionally, the **Japan Cryptographic Module Validation Program (JCMVP)**[25] provides a framework to test and certify cryptographic modules on the basis of standards such as the U.S. Federal Information Processing Standards (FIPS 140-3) or its international equivalent, ISO/IEC 19790. Cryptographic modules implementing algorithms listed in the **e-Government Recommended Ciphers List**[26] are tested and certified by third-party organizations under Japan's national standard, JIS X 19790, which aligns with ISO/IEC 19790. The historical context of these frameworks is thoroughly discussed in Tamura and Une (2008).

.....

24. For an overview of JISEC, please refer to the following webpage provided by the Information-technology Promotion Agency (IPA) (https://www.ipa.go.jp/security/jisec/about/index.html).
25. For an overview of JCMVP, please refer to the following IPA webpage (https://www.ipa.go.jp/security/jcmvp/index.html).
26. Cryptography Research and Evaluation Committees (CRYPTREC) has established a list of recommended cryptographic algorithms for procurement in e-government systems, commonly referred to as the CRYPTREC Cryptographic List.

For QKD, the standardization of cryptographic protocols as well as the institutional frameworks for evaluation and certification of QKD products will be essential for its broader adoption. Specifically, for the deployment of QKD products, security evaluation standards certified by a third-party organization for compliance with international standards and implemented using methods recommended by public authorities will serve as critical benchmarks for decision-making.

In recent years, the development of security evaluation standards for QKD has been progressing in Europe and other regions. In Europe, the European Telecommunication Standards Institute (ETSI) published a Protection Profile (ETSI GS QKD 016) in April 2023. This document defines security requirements for CC-based evaluations, with contributions from Japan's National Institute of Information and Communications Technology (NICT).[27]

Furthermore, significant advances have been made in the international standardization of security evaluation criteria. The **ITU-T Recommendations**,[28] which are international standards for telecommunications, already include numerous standards for QKD within the Y.3800 series. As of the time of writing (February 2024), 20 standards ranging from Y.3800 to Y.3819 have been established. ITU-T Recommendations are recognized as one of the enforceable de jure standards[29] under the WTO/TBT Agreement.[30] Additionally, the Agreement on Government Procurement within the WTO agreements mandates that technical specifications in government procurement be based on international standards wherever appropriate, giving ITU-T Recommendations significant influence over public procurement.

In the field of information security, **ISO/IEC JTC 1/SC 27** is also working on standards related to QKD security. For example, the draft standard ISO/IEC CD 23837-1/2 defines security requirements and specifies testing and evaluation methods for QKD. Similarly, an Industry Specification Group (ISG) under ETSI has advanced the standardization of QKD. Japanese researchers have significantly contributed their expertise to the development of these standards. For the effective implementation of these standards after their establishment, it is also crucial to cultivate domestic testing and certification bodies.

D. Challenges for the Adoption of QKD

The adoption of QKD faces four key challenges as follows.

The **first challenge** lies in improving communication performance by advancing

27. For further details, refer to the NICT webpage (https://www2.nict.go.jp/qictcc/social/standard.html).
28. The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for developing international standards for telecommunications. Among the three sectors of the ITU, the ITU-T (ITU Telecommunication Standardization Sector) focuses on telecommunication standardization. The international standards developed by ITU-T are published as ITU-T Recommendations.
29. The TBT Agreement, included in the WTO Agreement, establishes principles to ensure that national standards for industrial products and their conformity assessment procedures do not create unnecessary obstacles to international trade (Technical Barriers to Trade). It emphasizes the development of standards on the basis of international norms.
30. A **de jure standard** refers to an official standard that has been formally documented and developed through publicly available procedures by a standardization body. In contrast, a **forum standard** is a standard established through the consensus of companies and experts interested in standardization within a specific field. A **de facto standard** refers to a standard created by an individual company or other entity that has become dominant in the market through selection and competition.

the theory of protocols and their security proofs, as well as communication devices. These elements are not independent; instead, there is a reciprocal relationship where improvements to protocols and devices necessitate corresponding updates to security proofs.

The **second challenge** involves developing institutional frameworks for evaluating and certifying the security of QKD devices. For QKD systems manufactured by various vendors to operate seamlessly on the same network, it is essential to standardize protocol specifications. Additionally, accumulating and validating expertise in implementation practices is crucial to prevent implementation attacks.

In Japan, it would be worth considering the option of including QKD-related cryptographic technologies in the e-Government Recommended Ciphers List, which provides guidelines for government procurement.

The **third challenge** is the development of quantum relay technology. In QKD systems that rely on classical relays, trust in the relay devices is a prerequisite, which significantly diminishes the inherent value of QKD. As of February 2024, there have been no successful demonstrations of quantum relays. However, the realization of quantum relay technology is a critical milestone for maintaining QKD's relative advantage over other encryption schemes. For detailed discussions on proposed approaches and challenges related to quantum relays, refer to Azuma *et al.* (2023).

The **fourth challenge** involves lowering the costs associated with deploying and operating QKD systems. The need for specialized devices makes the initial setup expensive, making it impractical for individual companies to establish proprietary QKD networks. Thus, public initiatives to develop and support communication infrastructure are essential. In this regard, Japan's efforts—led by NICT to demonstrate QKD networks—are a step in the right direction. Additionally, advancements in technologies that integrate QKD with existing networks could further reduce operational costs, enhancing its feasibility for broader adoption.

VI. Concluding Remarks

While progresses have been made in QKD demonstration experiments across major countries and regions, QKD remains a developing technology. Its societal utility heavily depends on uncertain future technological advancements. At present, QKD is not a replacement for the general-purpose encryption schemes used in Internet communications. Instead, it is best suited for transmitting highly confidential information between limited, secure endpoints.

The unique strength of QKD lies in its information-theoretic security, a robust property that cannot be guaranteed by PQC. For transmitting highly confidential information with exceptionally long retention periods, QKD could become a valuable option. Moreover, the advent of quantum computers capable of breaking conventional cryptography and the potential development of new cryptanalysis algorithms targeting PQC are unpredictable. Considering these tail risks, QKD provides a societally valuable option.

Beyond the scope of this paper, QKD could contribute to future innovations such as **quantum-secure clouds**, enabling the information-theoretically secure distribution

and storage of data by combining QKD networks with existing cryptographic technologies (e.g., secret sharing). Additionally, the development of a **quantum Internet**, which could interconnect quantum information processing devices on a global scale, might emerge in the distant future. The research and development of QKD are likely to proceed with these societal implications and potential applications.

For now, it is crucial for the financial sector requiring high-security solutions to gain a precise understanding of the technical capabilities of QKD, the security services it provides, and the level of security it guarantees.

References

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), "Should Quantum Key Distribution be Used for Secure Communications?" Technical Position Paper, ANSSI, 2023 (available at https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications).

———, Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces, "Position Paper on Quantum Key Distribution," BSI, 2024 (available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html).

Azuma, Koji, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin, "Quantum Repeaters: From Quantum Networks to the Quantum Internet," arXiv: 2212.10820, 2023.

Barrett, Jonathan, Roger Colbeck, and Adrian Kent, "Memory Attacks on Device-Independent Quantum Cryptography," *Physical Review Letters*, 110, 2013, 010503.

Bennett, Charles H., and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 1984.

———, ———, and N. David Mermin, "Quantum Cryptography without Bell's Theorem," *Physical Review Letters*, 68(5), 1992, pp. 557–559.

Ekert, Artur K., "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, 67, 1991, pp. 661–663.

Fujiwara, Mikio, "Ryoushi Angou Gijyutu: Kakujyuu Sareta Toukyo QKD Netowa-ku (Quantum Cryptography Technology: Expanded Tokyo QKD Network)," paper presented at Ryoushi ICT Foramu Semina (Quantum ICT Forum Seminar), on December 20, 2023, Quantum ICT Forum, 2023 (in Japanese).

Goto, Hitoshi, "Ryoushi Angou Tushin No Shikumi To Kaihatu Doukou (Mechanisms and Development Trends of Quantum Cryptographic Communication)," *Kin'yu Kenkyu* (Monetary and Economic Studies), 28(3), Institute for Monetary and Economic Studies, Bank of Japan, 2009, pp. 107–150 (in Japanese).

Gottesman, Daniel, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill, "Security of Quantum Key Distribution with Imperfect Devices," *Quantum Information and Computation*, 4(5), 2004, pp. 325–360.

Grosshans, Frédéric, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, 421, 2003, pp. 238–241.

Hwang, Won-Young, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, 91(5), 2003, 057901.

Kanno, Satoru, "Tai Ryoushi Keisanki Angou Heno Angou Ikou Ni Muketa Gijyutu Doukou (Technological Trends for the Migration to Post-Quantum Cryptography)," paper presented at Joho Security Semina (Information Security Seminar) sponsored by the Institute for Monetary and Economic Studies, Bank of Japan, 2023 (in Japanese).

Koashi, Masato, "Simple Security Proof of Quantum Key Distribution Based on Complementarity," *New Journal of Physics*, 11(4), 2009, 045018.

———, and Takeshi Koshiba, *Ryoushi Angou Riron No Tenkai* (Development of Quantum Cryptography Theory), Tokyo: Saiensu Sha, 2008 (in Japanese).

Lo, Hoi-Kwong, Marcos Curty, and Bing Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, 108(13), 2012, 130503.

———, and F. H. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, 283(5410), 1999, pp. 2050–2056.

———, Xiongfeng Ma, and Kai Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, 94(23), 2005, 230504.

Lucamarini, Marco, Zhiliang Yuan, James F. Dynes, and Andrew J. Shields, "Overcoming the Rate-

Distance Limit of Quantum Key Distribution without Quantum Repeaters," *Nature*, 557, 2018, pp. 400–403.

Matsuura, Takaya, Kento Maeda, Toshihiko Sasaki, and Masato Koashi, "Finite-Size Security of Continuous-Variable Quantum Key Distribution with Digital Signal Processing," *Nature Communications*, 12, 2021, 252.

Mayers, Dominic, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels," *Advances in Cryptology—CRYPTO '96*, Lecture Notes in Computer Science, 1109, Berlin, Heidelberg: Springer, 1996, pp. 343–357.

Müller-Quade, Jörn, and Renato Renner, "Composability in Quantum Cryptography," *New Journal of Physics*, 11, 2009, 085006.

National Cyber Security Centre, "Quantum Security Technologies," White Paper, 2020a (available at https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies).

———, "Preparing for Quantum-Safe Cryptography," White Paper, 2020b (available at https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf).

National Institute of Standards and Technology (NIST), "Status Report on the Third Round of the NIST Post-Quantum Cryptography," 2022 (available at https://doi.org/10.6028/NIST.IR.8413-upd1).

National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," 2021 (available at https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/).

Netherlands National Communications Security Agency (NLNCSA), "Prepare for the Threat of Quantum Computers," 2022 (available at https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers).

Nielsen, Michael A., and Isaac L. Chuang, *Quantum Computation and Quantum Information (10th Anniversary Edition)*, Cambridge: Cambridge University Press, 2010.

Pereira, Margarida, Go Kato, Akihiro Mizutani, Marcos Curty, and Kiyoshi Tamaki, "Quantum Key Distribution with Correlated Sources," *Science Advances*, 6(37), 2020, eaaz4487.

Pirandola, Stefano, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, "Fundamental Limits of Repeaterless Quantum Communications," *Nature Communications*, 8, 2017, 15043.

Renner, Renato, "Security of Quantum Key Distribution," PhD thesis, ETH Zürich, 2005.

———, and Ramona Wolf, "The Debate over QKD: A Rebuttal to The NSA's Objections," arXiv: 2307.15116, 2023.

Sajeed, Shihan, Poompong Chaiwongkhot, Anqi Huang, Hao Qin, Vladimir Egorov, Anton Kozubov, Andrei Gaidash, Artur Vasiliev, Artur Gleim, and Vadim Makarov, "An Approach for Security Evaluation and Certification of a Complete Quantum Communication System," *Scientific Reports*, 11, 2021, 5110.

Shor, Peter W., and John Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, 85(2), 2000, pp. 441–444.

Suzuki, Masataka, Ken Sugawara, and Daisuke Suzuki, "Saido Chaneru Kougeki Ni Taisuru Anzensei Hyouka No Kenkyu Doukou To EMV Ka-do Koyuu No Ryuuiten (Research Trends in the Security Evaluation Against Side-Channel Attacks and Considerations for EMV Cards)," *Kin'yu Kenkyu* (Monetary and Economic Studies), 34(4), Institute for Monetary and Economic Studies, Bank of Japan, 2015, pp. 107–134 (in Japanese).

Tamura, Yuko and Masashi Une, "Joho Sekyuritei Seihin Shisutemu No Daisansya Hyouka Ninshou Seido Ni Tsuite: Kinyu Bunya Ni Oite Riyou Shite Iku Tame Ni (Third-Party Evaluation and Certification Systems for Information Security Products and Systems: For Application in the Financial Sector)," *Kin'yu Kenkyu* (Monetary and Economic Studies), 27, Special Issue No. 1, Institute for Monetary and Economic Studies, Bank of Japan, 2008, pp. 79–114 (in Japanese).

Tomamichel, Marco, Christian Schaffner, Adam Smith, and Renato Renner, "Leftover Hashing Against Quantum Side Information," *IEEE Transactions on Information Theory*, 57(8), 2011, pp. 5524–5535.

Une, Masashi, "Ryoushi Konpyuta Ga Angou Ni Oyobosu Eikyou Ni Dou Taisyo Suruka: Kaigai Ni Okeru Torikumi (How to Address the Impact of Quantum Computers on Cryptography:

Overseas Initiatives)," Discussion Paper No. 2023-J-13, Institute for Monetary and Economic Studies, Bank of Japan, 2023a (in Japanese).

———, "Ryoushi Konpyuta Ni Taisei Wo Motu Angou Heno Ikou (Transition to Cryptography Resilient to Quantum Computers: Trends in Financial Sector Discussions)," paper presented at Ryoushi ICT Foramu Semina (Quantum ICT Forum Seminar), on December 20, 2023, Quantum ICT Forum, 2023b (in Japanese).

Wang, Xiang-Bin, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Physical Review Letters*, 94(23), 2005, 230503.

Wegman, Mark N., and J. Lawrence Carter, "New Hash Functions and Their Use in Authentication and Set Equality," *Journal of Computer and System Sciences*, 22(3), 1981, pp. 265–279.

Wengerowsky, Sören, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, and Rupert Ursin, "An Entanglement-Based Wavelength-Multiplexed Quantum Communication Network," *Nature*, 564, 2018, pp. 225–228.

APPENDIX: APPROACHES TO PROVING ϵ-SECURITY

There are two major approaches to proving ϵ-security.

The first approach employs the quantum version of the leftover hash lemma (Renner [2005], Tomamichel *et al.* [2011]). The hash values of the sifted key are compared between the sender and the receiver. For legitimate senders and receivers, who share an identical sifted key, the hash values will match. However, for an eavesdropper who possesses only partial information about the sifted key, the presence of unknown elements prevents the hash values from matching. If the hash values are sufficiently consistent between the sender and receiver, the final key can be considered secure.

The second approach involves virtual error correction (Lo and Chau [1999], Shor and Preskill [2000], Koashi [2009]). This approach treats the changes in the key caused by eavesdropping as errors induced by the eavesdropper obtaining key information. It then verifies whether these errors can be corrected. If correction is possible, it indicates that the eavesdropper does not possess sufficient information about the key, and the final key is secure. This technique is termed virtual error correction because it determines the correctability of errors theoretically from the error rate, without performing the experimentally challenging quantum error correction.

Following these proofs, further discussions have developed to evaluate more rigorously the characteristic quantities (e.g., min-entropy, phase error rate) that demonstrate the security of the final key in protocols guaranteeing ϵ-security.