entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Quantum Digital Signature Using Entangled States for Network

Changho Hong, Youn-Chang Jeong, Osung Kwon and Se-Wan Ji

Special Issue

New Advances in Quantum Communications and Quantum Computing

Edited by

Dr. Mariella Minder and Prof. David Lucas

MDPI

https://doi.org/10.3390/e27111179

entropy

MDPI

Article

Quantum Digital Signature Using Entangled States for Network

Changho Hong *, Youn-Chang Jeong, Osung Kwon and Se-Wan Ji

The Affiliated Institute of ETRI, Yuseong-daero 1559, Yuseong-gu, Daejeon 34044, Republic of Korea
* Correspondence: hchc11@nsr.re.kr; Tel.: +82-42-870-4967

Abstract

We propose an entanglement-based quantum digital signature (QDS) protocol optimized for quantum networks. The protocol follows the Lamport-inspired QDS paradigm but eliminates QKD post-processing by signing and verifying with raw conclusive keys, thereby reducing latency and implementation complexity. We provide a finite-size security analysis of robustness, unforgeability, and non-repudiation. Under standard fiber-loss and detector models, simulations show a consistent signature rate advantage over a representative Lamport-inspired QDS baseline across metro-to-regional distances. The proposed protocol is practical for near-term deployment while preserving end-to-end, finite key security guarantees.

Keywords: quantum communication; quantum network; quantum digital signature; one-time signature

Academic Editors: Mariella Minder and David Lucas

Received: 1 October 2025
Revised: 10 November 2025
Accepted: 18 November 2025
Published: 20 November 2025

Citation: Hong, C.; Jeong, Y.-C.; Kwon, O.; Ji, S.-W. Quantum Digital Signature Using Entangled States for Network. *Entropy* **2025**, *27*, 1179. https://doi.org/10.3390/e27111179

1. Introduction

Digital signature (DS) is a cryptographic service that ensures that an important message was created by the legitimate and clearly identified sender (authenticity), that the message was not tampered with (integrity), and that the message transmitter cannot deny having sent the message (non-repudiation). Quantum digital signature (QDS) should also provide these services. The most common DS uses a public key system consisting of a private key and a public key [1]. The signer chooses a message and uses private key to generate a signature sig(m). A verifier of signatures checks whether to accept the message as originating from the legitimate signer or not by using the public key. The security of these schemes is based on the assumption that attackers have limited computational power and that solving mathematical problems such as discrete logarithms or factorization is hard for them. In other words, if an extremely powerful computer is built, it could solve these problems efficiently and break the security of these DS schemes. In 2001, Gottesman and Chuang proposed the first QDS scheme [2]. The protocol uses quantum one-way function, where the inability to invert is not based on computational assumption but assured by the law of quantum mechanics. The quantum one-way function exploits the fact that non-orthogonal quantum states cannot be distinguished perfectly. If we have a quantum state $|g(x)\rangle$, where $g(x)$ represents the classical described state, and the set of possible states are non-orthogonal, nobody should be able to settle the classical description of the state with high probability.

Inspired by Lamport's one-time signature (OTS) scheme [3], which relies solely on the one-wayness of hash functions for security, QDS protocols adopt the same principle of partial key revelation per message while leveraging quantum key distribution (QKD) to provide information theoretically secure key establishment [2,4]. This hybridization

eliminates the need for large classical public keys, enhances forward security, and ensures robustness even against quantum adversaries [5]. Recent advances have produced practical instantiations, notably one-time universal hashing (OTUH) QDS [5], which compresses arbitrary length messages into fixed-size digests and uses QKD-generated keys without privacy amplification, thereby enabling efficient, low-latency signing [5]. Furthermore, measurement device independent (MDI) QDS protocols [6] have removed detector side channel vulnerabilities, while chip-integrated implementations [7] have demonstrated scalable, low-cost deployment over metropolitan-scale fiber networks [7–9]. Experimental work has further pushed these concepts into the field: Yin et al. demonstrated an MDI-QDS protocol over a metropolitan network with security level on the order of 10^{-7}, securing binary messages against all detector side channel attacks [10]; Liu et al. achieved decoy-state QDS over 102 km of fiber, even signing a 32 bit message ("USTC") at 51 km [11]; Clarke et al. additionally showed equivalent QDS performance over ≈134 km (≈43 dB loss) in installed fiber, setting records for transmission distance [7,12–14]. Together, these developments position Lamport-inspired QDS (QS-L) as a promising candidate for securing critical communications in quantum era infrastructure.

In this paper, we propose a QDS protocol based on entangled states. This protocol belongs to the QS-L family of protocols and share several common features. QS-L integrates QKD without post-processing (i.e., omitting full error correction and privacy amplification) and parameters that are standard in QKD are used as pass/fail criteria in the QDS verification phase. The raw key, which is the intermediate data or key of QKD, is used as the signature key. It means that QS-L family has significant advantages in implementation [8,15]. Although quantum secure direct communication (QSDC) may, in the ideal case, dispense with post-processing, the manner in which post-processing is omitted in QSDC differs from what we mean by eliminating post-processing in the proposed QDS. QSDC transmits plaintext directly through quantum states and thereby dispenses with key distillation, typically employing block coding and error correction, and in some variants, device independence techniques [16–20]. In our protocol we do not transmit the message in quantum states and we use the quantum channel only to generate correlated classical strings that are later tested for signature verification, and by "no QKD post-processing", we mean that full error correction and privacy amplification are not applied while decoy-state estimation and thresholding are still performed.

There are some assumptions on the QS-L family as follows.

- Alice–Bob and Alice–Charlie are connected by imperfect quantum channels.
- Alice–Bob and Alice–Charlie are connected by authenticated classical channels.
- Bob–Charlie link is confidential and authenticated, and its content (indices, test positions) is never revealed to Alice. (In our symmetrization-free QDS this assumption is unnecessary, and the reasons will become clear as the protocol is presented.)
- In the key generation step within the distribution phase, participating users all act honestly.

2. Quantum Digital Signature Using Entangled States

The protocol suggested in this paper consists of a distribution phase, estimation phase, and a messaging phase. The distribution phase comprises two steps: key generation and reordering. In the estimation phase, we derive the thresholds necessary to validate the signature. The message phase consists of signature and verification. In the proposed QDS protocol, Alice is the signer, Bob the authenticator, and Charlie the verifier [21].

Our protocol uses the SARG04 [22] encoding/decoding method; a brief description follows. Because our scheme operates with entangled states, the single-photon formulation of the original SARG04 is modified as follows. In the proposed entanglement-based SARG04 protocol, polarization-entangled photon pairs are distributed to Alice and Bob

(Charlie), who each measure every qubit in a randomly chosen x-basis or z-basis and record the outcomes. During sifting, Alice first publicly announces, for every round, a pair of non-orthogonal candidate states that contains the state consistent with her setting and outcome, chosen from $[\{|0\rangle, |+\rangle\}, \{|+\rangle, |1\rangle\}, \{|1\rangle, |-\rangle\}, \{|-\rangle, |0\rangle\}]$. Given this announcement, Bob (Charlie) classifies the round as conclusive if and only if his projective measurement outcome is orthogonal to exactly one of the two candidates; in that case, the other candidate is inferred as the emitted state and the raw bit is set by its basis label ($z \to 0$, $x \to 1$). Otherwise, the round is discarded. No prior disclosure of Bob's basis is required for decoding (basis information is revealed only for parameter estimation samples). The surviving conclusive events are then used for estimation of error. For brevity, we designate the above procedure as the bit assignment process (BAP).

2.1. The Distribution Phase

The distribution phase can be explained by dividing into the key generation step and the reordering step. Among them, the key generation step corresponds to the post-processing free QKD process.

The purpose of the distribution phase is to create keys for signing and verifying, and to securely share them between legitimate users, thereby providing a non-repudiation service.

2.1.1. Key Generation Step

Alice randomly generates an entangled state of

$$|\psi^z\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \tag{1}$$

$$|\psi^x\rangle_{AB} = \frac{1}{\sqrt{2}}(|++\rangle_{AB} + |--\rangle_{AB}) \tag{2}$$

and shares it with Bob. Similarly, Alice creates an entangled state of

$$|\psi^z\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle_{AC} + |11\rangle_{AC}) \tag{3}$$

$$|\psi^x\rangle_{AC} = \frac{1}{\sqrt{2}}(|++\rangle_{AC} + |--\rangle_{AC}) \tag{4}$$

and shares it with Charlie. Here, the subscripts AB and AC mean that the two-qubit entangled state is shared between Alice and Bob, and Alice and Charlie, respectively. The states $|\psi^z\rangle$ and $|\psi^x\rangle$ represent the z-basis entangled state and the x-basis entangled state, respectively. The rules for Alice's preparation and distribution of quantum states are as follows. For each possible message $m = \{0, 1\}$, Alice prepares two types of entangled quantum state sequences with length n—that is sequence $(A_b)_m$, $(B_a)_m$, $(A_c)_m$ and $(C_a)_m$. The sequence $(A_b)_m$ and $(B_a)_m$ form n entangled states, and similarly, the sequence $(A_c)_m$ and $(C_a)_m$ also form n entangled states. Here, each entangled state constituting sequence is randomly selected and generated from $\{|\psi^z\rangle, |\psi^x\rangle\}$. Each sequence of length N includes the following decoy states. The decoy method is commonly used in QKD implementation for secure communication [23–25]. It is a powerful tool that can be used to improve the security and performance of QKD. The decoy method is also used to set the signature verification threshold in our signature scheme. In the decoy method, Alice uses intensity μ to generate the entangled states used for the signal states, and uses intensity ν and 0 (vacuum) for parameter estimation. When using intensity ν, it is not necessary to generate entangled states, but one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ is randomly selected to create a pair of identical states. For example, a pair of $|1\rangle$ state is generated, and one qubit is stored by Alice herself and the other qubit is transmitted to the opponent. The intensities μ,

ν, and 0 are generated with probabilities p_μ, p_ν, and p_0, respectively. Here, the state generated with intensity μ is an entangled state, and the state generated with ν is one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

1. Alice sends $(B_a)_m$ to Bob and $(C_a)_m$ to Charlie. She measures her states on a randomly chosen basis, thereby forming a sequence of outcomes ((AB_a) and (AC_a)).
2. Bob and Charlie make a measurement on each state of received sequence ($(B_a)_m$ and $(C_a)_m$, respectively) by randomly selecting from the measurement bases, z- or x-basis. They announce all the click (measured) events through an authenticated channel to Alice. Only part of quantum states can be detected due to channel loss and imperfect detection [26–31]. Alice and Bob throw away all the events that have not clicked on either side. It means that they keep the left data of length l ($l < n$), denoted as $(Ab)_m$, kept by Alice and $(Ba)_m$ kept by Bob. Alice and Charlie also repeat the same process to form $(Ac)_m$ kept by Alice and $(Ca)_m$ kept by Charlie. Of course, there is no correlation between the states of sequences of Bob and Charlie at this stage because Alice randomly and independently generated and distributed entangled states.
3. Alice announces the intensity information of all qubits. According to the intensity data, the legitimate three users divide each of their sequence into three strings. For example, Bob divides $(Ba)_m$ into $(Ba)_m^\mu$, $(Ba)_m^\nu$, and $(Ba)_m^o$. In a similar manner, Charlie partitions the $(Ca)_m$ sequence. We describe these three intensities as λ ($\in \{\mu, \nu, 0\}$.

2.1.2. Reordering Step

1. Alice, using the sequence $(Ab)_m^\lambda$ as a reference, reorders the positions of each bit within the sequence $(Ac)_m^\lambda$ to match the bit sequence of the sequence $(Ab)_m^\lambda$. This rearranged sequence is denoted as $\left((Ac)_m^\lambda\right)'$. Alice shares the repositioning information with Charlie, allowing Charlie to transform the sequence $(Ca)_m^\lambda$ to the sequence $\left((Ca)_m^\lambda\right)'$ accordingly. We use parentheses and prime ($'$) to indicate that a sequence has been reordered. This procedure effectively eliminates the canonical symmetrization step in standard QS-L [21].

At this stage, the ownership status of each sequence and the inter-sequence relationships are compiled in Table 1. As a result of the reordering step, $(Ab)_m^\lambda$ and $\left((Ac)_m^\lambda\right)'$ consist of the same bit sequence.

2. They generate new bit strings through the BAP; specifically, Alice obtains $(kA)_m$, Bob obtains $(kB)_m$, and Charlie obtains $(kC)_m$. Note that Bob and Charlie do not reveal which bits are conclusive results.

Table 1. The ownership status of each sequence.

User/Source		**Sequence**
Source	$\left\|\psi^{z(x)}\right\rangle_{AB}$	$\left\|\psi^{z(x)}\right\rangle_{AC}$
Alice	$(Ab)_m^\lambda$	$\left((Ac)_m^\lambda\right)'$ $(=(Ab)_m^\lambda)$
Bob	$(Ba)_m^\lambda$	
Charlie		$\left((Ca)_m^\lambda\right)'$

2.2. Estimation Phase

At this phase, three legitimate users determine the authentication security threshold and the verification security threshold of the signature based on the bit error rate. The detailed process is as follows.

1. The signer Alice chooses the authenticator from among Bob and Charlie; the remaining user naturally becomes the verifier of the signature. In this protocol, the authenticator serves as a kind of intermediary for non-repudiation services. The verifier plays the role of validator, verifying Alice's signature. For the description of the protocol, we suppose that Bob is the authenticator and Charlie is the verifier.
2. Alice, Bob, and Charlie publicly announce all data about ν-, and 0-sequences: Alice's candidate pair announcements and the measurement outcomes of Bob and Charlie.
3. They estimate the bit error rate of entangled pairs in μ sequences (between $(kA)_m^\mu$ and $(kB)_m^\mu$, and $(kA)_m^\mu$ and $(kC)_m^\mu$) using the all data of ν sequence (between $(kA)_m^\nu$ and $(kB)_m^\nu$, and $(kA)_m^\nu$ and $(kC)_m^\nu$) and 0 sequence (between $(kA)_m^0$ and $(kB)_m^0$, and $(kA)_m^0$ and $(kC)_m^0$). In other words, the bit error rate for the central sequence (μ sequence) is calculated by the decoy method commonly used in QKD.
4. Charlie randomly selects a proportion of u in the μ sequence $(kC)_m^\mu$ to use as test bits, then requests Alice to announce the bit values at those locations. We describe test bit sequences as $\left((kA)_m^\mu\right)_T$, $\left((kB)_m^\mu\right)_T$, and $\left((kC)_m^\mu\right)_T$. Also, let us denote $e_{ab,T}$ and $e_{ac,T}$ as the mismatch rate of conclusive results between $\left((kA)_m^\mu\right)_T$ and $\left((kB)_m^\mu\right)_T$, and $\left((kA)_m^\mu\right)_T$ and $\left((kC)_m^\mu\right)_T$, respectively. In QKD, just as in the method used to determine post-processing based on the bit error rate, if $e_{ab,T}$ and $e_{ac,T}$ are too high, the subsequent steps are not performed.
5. Bob and Charlie estimate the conclusive event rates on $(kB)_m$ and $(kC)_m$. These are denoted as P_b and P_c, respectively. Under ideal statistics, P_b and P_c are expected to approach $1/4$. If they deviate substantially from this nominal value, the protocol is aborted.
6. Based on $e_{ab,T}$, $e_{ac,T}$, P_b, and P_c, Alice, Bob, and Charlie set the authentication security threshold T_a and verification security thresholds T_v. Set $T_a = e_{ab,T} + \Delta_A$, $T_v = e_{ac,T} - \Delta_V$ where Δ_A, $\Delta_V > 0$ are one-sided finite-size margins derived from the conclusive sample sizes [32,33]. The thresholds are required to satisfy $0 < T_a < T_v < 1/2$. In other words, by excluding the post-processing procedures that are essential, in general, QKD when setting up T_a and T_v, the comprehensive effects of losses and errors included in the shared key are reflected.
7. The three legitimate users discard the test bits and keep the remaining bits in μ strings with length L_k. We denote these remaining bit sequences as $(K_a)_m$, $(K_b)_m$, and $(K_c)_m$.

2.3. Message Phase

1. Alice sends the message and the corresponding signature $\{m, (K_a)_m\}$ to the authenticator Bob to sign message m.
2. Bob receives $\{m, (K_a)_m\}$ and estimates the error rate e'_{ab} between $(K_a)_m$ and $(K_b)_m$. If $e'_{ab} < T_a$, Bob accepts the signature and transmits $\{m, (K_a)_m\}$ to the verifier Charlie; otherwise, he aborts the signature and announces the failure result.
3. In a similar way to Bob, Charlie calculates the error rate e'_{ac} between $(K_a)_m$ and $(K_c)_m$. Charlie accepts the signature if $e'_{ac} < T_v$. As a result, Charlie accepts $\{m, (K_a)_m\}$ as Alice's signature for message m with signature verification using T_a and T_v.

3. Security Analysis

This section provides a comprehensive and rigorous security analysis of the proposed QDS protocol utilizing entangled states. We address robustness, unforgeability, and non-repudiation by systematically applying methods from the established literature [21]. Taken together, these results establish that the signature scheme achieves information theoretic security while supporting efficient message authentication. Here, we discuss the security of the proposed protocol from these three perspectives.

3.1. Robustness

Robustness is defined as the probability of honest participants successfully completing the protocol without aborting due to unexpected discrepancies. Although robustness pertains to honest run completeness rather than adversarial security, it is standard to report it alongside security parameters. Thus, including robustness in the security section is appropriate. In this protocol, robustness is achieved by setting an error rate threshold that distinguishes acceptable noise (due to channel imperfections) from adversarial interference (indicative of an attack). We compute the probability ϵ_{rob} that the protocol fails because of noise or errors by using Chernoff bound [10]. The Chernoff bound yields a tail probability for deviations in the empirical error from its expectation. Through the estimation step of our QDS, legitimate users calculate the error rate between transmitted and received qubit sequences. By leveraging random sampling without replacement, the probability of an honest abort, ϵ_{rob}, can be defined as

$$\epsilon_{rob} = exp\left[-2n^{cu}(T_a - E_B^{cu})^2\right], \text{ for } E_B^{cu} < T_a \tag{5}$$

where T_a is the acceptance authentication threshold, E_B^{cu} is the measured bit error rate between Alice and Bob for the conclusive bits, and n^{cu} is the length of the conclusive bit sequence used for authentication. From a robustness perspective, Equation (5) indicates that the probability of protocol abortion exponentially decreases as the difference between the measured bit error rate E_B^{cu} and the threshold T_a increases. Hence, to ensure high robustness, the threshold T_a should be appropriately selected, considering the expected system imperfections and channel conditions.

3.2. Unforgeability

The protocol's unforgeability is maintained by ensuring that an adversarial party (e.g., an internal forger such as Bob) cannot replicate or manipulate Alice's signature to deceive other participants. The forgery probability ϵ_{for} quantifies the chance that an adversary (e.g., authenticator Bob) successfully forges the signature to deceive the verifier Charlie. Let us explain unforgeability based on our QDS protocol.

(1) Estimate the lower bound of the secure single-photon pair events s_{11}^{AC} between Alice and Charlie by decoy-state analysis:

$$s_{11}^{AC*} \geq \frac{p_\mu^2 e^{2\mu}}{v^2(\mu-\nu)^2 n_p^{AC}} \left(\mu^2 e^{\nu} \frac{n_\nu^{AC}}{p_\nu} - \mu^2 e^{\mu} \frac{n_\mu^{AC}}{p_\mu} + \left(\nu^2 - \mu^2\right) \frac{n_0^{AC}}{p_0}\right)^2 \tag{6}$$

The meaning of each variable is specified below.

- n_p^{AC}: Observed number of conclusive detection events on the Alice–Charlie link when the source intensity is $p \in \{\mu, \nu, 0\}$.
- n_μ^{AC}, n_ν^{AC}, n_0^{AC}: Shorthand for the above counts at the signal (μ), weak decoy (ν), and vacuum (0) settings, respectively.
- $e^{2\mu}$, $e^{2\nu}$: Poisson weight factors appearing in the decoy linear relations for pair sources when isolating the single-photon contribution from n_p^{AC}.

(2) Compute the maximum number of single-photon error events t_{11}^{AC}:

$$t_{11}^{AC*} \leq \frac{p_\mu^2 \mu^2 e^{2\mu}}{v^2 n_p^{AC}} \left(e^{\nu} \frac{n_\nu^{AC}}{p_\nu} - \frac{n_0^{AC}}{2p_0}\right)\left(e^{\nu} \frac{n_\nu^{AC}}{p_\nu} - \frac{n_0^{AC}}{p_0}\right) \tag{7}$$

(3) Calculate minimum expected mismatch rate E^*_{BF11}:

$$E^*_{BF11} = \frac{t^{AC*}_{11}}{s^{AC*}_{11}} \tag{8}$$

(4) Bound the forgery success probability using Chernoff bound [10]:

$$\epsilon_{for} = \exp\left[-\frac{\left(E^*_{BF11} - T_{\nu 11}\right)^2}{2E^*_{BF11}} s^{AC*}_{11}\right] \tag{9}$$

Here, $T_{\nu\,11}$ represents the verification threshold specifically for single-photon entangled pairs.

From the perspective of forgery attacks, Equation (9) explicitly shows that the probability of a successful forgery by the adversary decreases exponentially with the number of secure single-photon events s^{AC*}_{11} and the squared difference between the expected mismatch rate and the verification threshold. Thus, our QDS protocol ensures strong security against forgery attacks as long as proper thresholds are established and verified. The threshold effectively limits an adversary's chances of successful forgery.

3.3. Repudiation Resistance

Repudiation resistance ensures that Alice cannot deny having signed a message once it is authenticated by Bob and verified by Charlie. To rigorously quantify the security against repudiation, we evaluate the probability ϵ_{rep} that Alice successfully repudiates her signature. This probability is carefully bounded by statistical methods involving relative Hamming distances and threshold parameters, as explained below in detail.

First, we compute the relative Hamming distance between the bit sequences held by the authenticator Bob and verifier Charlie after the reordering step:

$$\Delta^{cu}_{BC} = \frac{\sum_{i=1}^{n^{cu}} |B_i - C_i|}{n^{cu}} \tag{10}$$

Here, B_i and C_i denote the ith bit in Bob's and Charlie's conclusive bit sequence, respectively. n^{cu} is the total length of the conclusive bit sequences shared between Bob and Charlie after discarding inconclusive and test bits. This relative Hamming distance (Δ^{cu}_{BC}) physically represents the proportion of differing bits between Bob's and Charlie's conclusive sequences, reflecting discrepancies arising primarily from quantum channel noise and potential adversarial actions.

Next, we solve the following transcendental equation to determine the critical parameter A:

$$\frac{\left[P^c_C T_\nu - P^c_C\left(\frac{\Delta^{cu}_{BC}}{n^{cu}} + \frac{A}{P^c_B}\right)\right]^2}{3P^c_C\left(\frac{\Delta^{cu}_{BC}}{n^{cu}} + \frac{A}{P^c_B}\right)} = \frac{\left(A - P^c_B T_a\right)^2}{2A} \tag{11}$$

The parameters in the above equation are explicitly defined as follows. P^c_B is the proportion of conclusive measurement results in Bob's bit sequence, reflecting the ratio of bits for which Bob obtained unambiguous measurement outcomes. P^c_C is the proportion of conclusive measurement results in Charlie's bit sequence, analogously defined for Charlie. Δ^{cu}_{BC} is the relative hamming distance between Bob's and Charlie's conclusive bit strings after the reordering step. T_ν is the verification threshold used in the repudiation analysis, i.e., the admissible mismatch limit for Charlie's acceptance test in the messaging phase. T_a is the authentication threshold used by Bob. It is fixed in the estimation phase from conclusive test statistics. A is an auxiliary parameter representing the critical error limit necessary

to balance and bound Alice's potential repudiation probability effectively. Equation (11) essentially quantifies the boundary conditions under which the legitimate users (Bob and Charlie) can confidently reject Alice's repudiation attempt.

Finally, with A fixed, the repudiation probability can be evaluated as follows:

$$\epsilon_{rep} = exp\left(-\frac{\left(A - P_B^c T_a\right)^2}{2A} n^u\right) \tag{12}$$

Here, the parameter n^u denotes the length of the bit sequence retained after removing test bits, effectively representing the available sample size for verification. Equation (12) indicates that Alice's probability of successfully repudiating her signature is exponentially suppressed by two factors. The first factor is that a greater difference between the parameter A and the product $P_B^c\ T_a$ strengthens security by making repudiation significantly more improbable. The second factor is that increasing the number of retained verification bits (n^u) drastically reduces the likelihood of successful repudiation, thereby strongly ensuring protocol security. Thus, the derived equation clearly emphasizes the protocol's ability to securely prevent repudiation, provided thresholds are properly selected and a sufficiently large verification dataset is utilized.

3.4. Overall Security Discussion

The overall security of the protocol against forging, repudiation, and robustness failures can thus be given by

$$\epsilon_{tot} = \epsilon_{rob} + \epsilon_{for} + \epsilon_{rep} + \epsilon_{stat} \tag{13}$$

Here, ϵ_{stat} encompasses additional statistical variations from finite-size effects and experimental inaccuracies.

3.5. Conclusion of Security Analysis

Our finite-size security analysis demonstrates end-to-end protection of the proposed QDS against the three standard failure modes—honest aborts, forgery, and repudiation—using statistics obtained in the estimation phase and applied during the message phase.

The honest abort event is controlled by a Chernoff-type tail bound whose tightness improves as the authentication sample size increases and as the observed conclusive bit error remains further below the authentication threshold, yielding rapidly improving robustness under realistic margins. For unforgeability, a decoy-state procedure isolates the single-photon component on the Alice–Charlie link; by lower bounding secure single-photon events, upper bounding single-photon errors, and forming the corresponding minimum expected mismatch, comparison with a single-photon verification threshold yields an exponentially small forgery probability that decreases with both the effective single-photon sample size and the squared gap to that threshold. Repudiation is addressed after the reordering step by measuring the relative Hamming distance between Bob's and Charlie's conclusive strings and solving a transcendental relation that combines their conclusive rates with the authentication and verification thresholds to obtain a critical parameter; the resulting repudiation bound decays exponentially with the verification sample size and strengthens as this parameter separates from the acceptance boundary. Finally, the overall failure probability is the sum of the three contributions above together with a residual finite-size term that captures additional statistical and experimental effects, enabling explicit budgeting of security parameters for implementation.

4. Realization Discussion

The proposed QDS protocol was deliberately designed for experimental feasibility and practical deployment. To assess the feasibility under realistic conditions, we compare our protocol with a canonical QS-L scheme implemented over insecure channels [34] using a common channel detector model and finite-size security budgets. The resulting distance-dependent signature rates are plotted in Figure 1, where two curves are shown (the proposed protocol and the QS-L baseline) in accordance with our intended comparison. In brief, the proposed design maintains a consistent rate advantage over the QS-L baseline across the metro-to-regional distance range because it (i) eliminates the data-discard cost of the symmetrization step and (ii) retains conclusive event statistics comparable to prepare-and-measure schemes under the same channel and detector parameters.

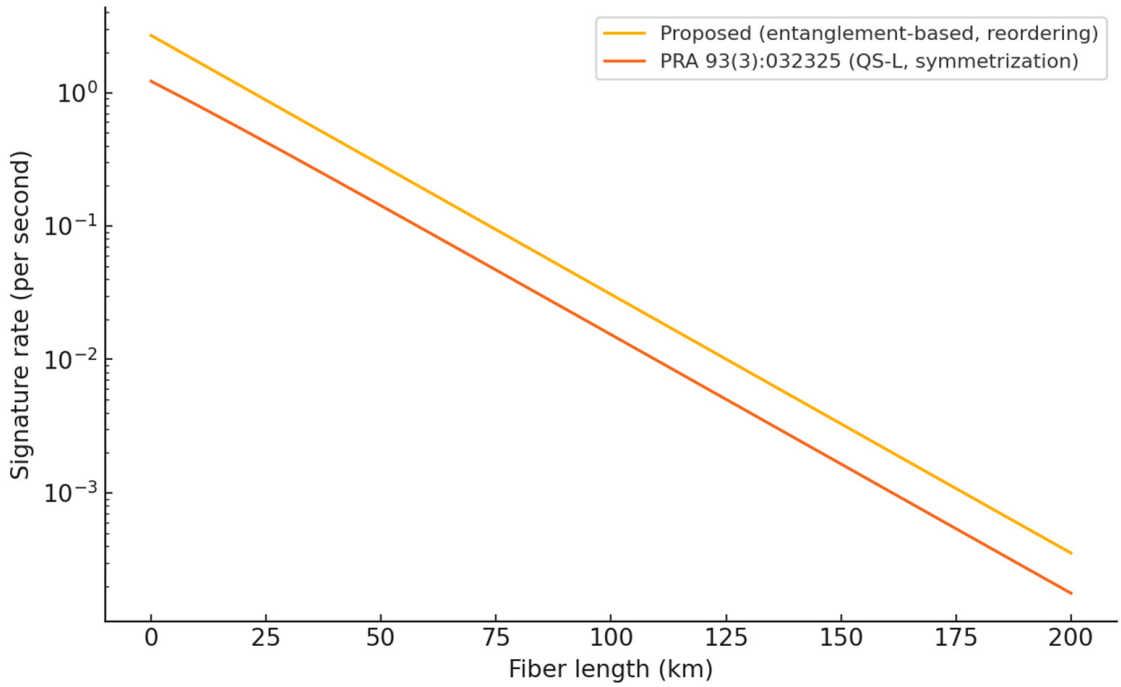

Figure 1. Comparison of our QDS protocol and general QS-L protocol [34].

The parameter values used in the simulations are as follows. All parameters are given per time slot unless otherwise noted. Channel and detection: detection efficiency 52%; dark-count probability 1.3×10^{-7}; basis misalignment 0.15%; insertion loss 1.2 dB; fiber attenuation 0.194 dB/km. Security budgets: ϵ_{rob}, ϵ_{for}, $\epsilon_{rep} \leq 10^{-10}$. Clocking and sifting: repetition rate 100 MHz (typical value in contemporary fiber-based systems); SARG04-style conclusive fraction was fixed to 0.25 (nominal expectation used consistently across both curves). Threshold margins (finite-size): authentication margin $\Delta_A = 0.005$ (absolute), verification margin $\Delta_V = 0.01$; single-photon mismatch threshold gap $\Delta_{11} = 0.012$ was used to instantiate the forging bound. Tail calibration: Chernoff constant is set to 2 with natural-log tail; the required signature length for each failure event is computed as $2\ln\left(\frac{1}{\epsilon_x}\right)/\Delta_x^2$, and the effective length is the maximum of the three. We plot n_x versus Δ for the security budget used here and mark the three operating margins; see Appendix A, Figure A2. Source models: for our protocol, entanglement pair generation probability per clock is fixed at 0.5; for the QS-L baseline (prepare and measure with weak coherent pulses), the mean photon number is set to 0.5 (typical operating point). All "typical" values are standard choices for comparative studies; if device-specific calibrations are available, the curves translate accordingly without changing the qualitative separation.

With identical security budgets (ϵ_{rob}, ϵ_{for}, ϵ_{rep}) and device parameters, the elimination of the symmetrization step nearly doubles the number of usable conclusive events, which directly translates into a higher signature rate at short and intermediate distances; the gap persists at longer distances until channel loss dominates both curves. Because the bounds in Section 3 scale exponentially with the product of the effective sample size and the squared threshold gap, modest improvements in margins (via calibration) or in conclusive fractions (via collection optics) yield disproportionate gains in rate in practice.

Given that our QDS targets quantum network applications, we utilize entangled states [7,13,14]. This raises a natural question of practical feasibility.

5. Integration with Quantum Networks and Deployment Considerations

5.1. Network Native Rationale

Our protocol is entanglement-centric by construction: the signing and verification criteria are calibrated from decoy-state statistics. This aligns with the vision of quantum internet in which entanglement is the network service and applications consume it via higher-layer protocols [35]. In particular, the ITU-T Y.3800 framework and related Y.38xx series decompose quantum key distribution networks (QKDNs) into the user, key management, control, and transport strata; entanglement distribution (via fiber or free space) is the primitive that these strata orchestrate [36]. Our use of entangled states as the resource therefore maps naturally onto network operations in which entanglement is generated, routed, or swapped across multiple domains.

5.2. Topologies and Relay Placement

The protocol supports (i) endpoint-sourced entanglement, where Alice's source feeds Bob and Charlie directly (as in our baseline), (ii) network-sourced entanglement, where an entanglement server (ES) injects Bell pairs into a metro network (star or mesh) for multi-tenant consumption, and (iii) an MDI-hub realization, where a central untrusted relay performs Bell-state measurements (BSMs). Metro-scale analyses and field concepts using an ES that streams entanglement to users over line of sight, free space, or fiber links have been reported, validating (ii) at city scale [37]. Option (iii) inherits the MDI advantages and is consistent with our symmetrization step, which equalizes recipients' evidence even under hub-routed traffic.

5.3. Interoperability with Control/Management Planes

Our decoy derived authentication and verification threshold functions as physical layer telemetry that can be surfaced to network controllers. ETSI GS QKD 014 [38] defines a REST key delivery API between QKDNs and applications, while ETSI GS QKD 015 [39] standardizes SDN control interfaces for provisioning, monitoring, and policy enforcement in disaggregated networks. Exposing the measured error rates and threshold margins ($e_{obs} - \{T_{auth}, T_{ver}\}$) as metrics allows controllers to (a) select routes/relays with adequate quantum signal quality, (b) adjust intensity probabilities (p_μ, p_ν, p_0) under congestion or weather dynamics, and (c) schedule QDS signing windows when decoy inferred yields are optimal—without changing the security model.

5.4. Empirical Evidence from Network Trials

A three-party MDI-QDS field test over a ~200 km^2 metropolitan network demonstrated successful binary message signing with security level ~10^{-7}, removing detector side channels via an untrusted relay—directly supporting our (iii) deployment mode [10]. This complements long-running QKD network trials that have integrated heterogeneous

links and centralized key management (e.g., Tokyo QKD Network, SECOQC Vienna), establishing operational practices for multi-vendor, SDN-assisted quantum networks [40,41].

5.5. Scalability via Integrated Photonics

Large scale adoption hinges on cost, footprint, and stability of quantum transceivers. Silicon photonic QKD has achieved metropolitan field rates with monolithically integrated encoders and receivers, demonstrating stability and manufacturability compatible with carrier-grade deployment [42]. Recent work reports gigabit class secret key rates on chip at 10 km, while integrated CV-QKD receivers have operated over tens of kilometers, suggesting a path to compact, low-cost entanglement distribution and detection hardware for QDS overlays [43,44]. Although our protocol uses DV entanglement, the same integration ecosystem (PICs, packaging, and classical DSP) applies to entanglement sources, BSM nodes, and time/frequency multiplexed distribution.

5.6. Extending Reach with Repeaters and Swapping

For backbone scale deployment, entanglement swapping and quantum repeaters extend feasible distances by composing high-fidelity pairs across segments [45,46]. Our entanglement-based signing naturally composes with repeater chains: the distribution phase operates over swapped Bell pairs, while the decoy analysis and thresholding continue to bound single pair yields and error events end-to-end. This is consistent with recent continental scale QKD network reports (e.g., China's carrier-grade CN-QCN over 10,000 km with multi-type hybrid networking) and with space to ground entanglement/QKD progress that anticipates global integration [47,48].

5.7. Operational Mapping of Protocol Steps

In networks, (a) key generation maps to entanglement provisioning (ES or repeater chain) with decoy scheduling per path; (b) symmetrization becomes a control plane function that publishes index maps (or PRNG seeds) to verifiers over authenticated classical channels; and (c) estimation act as link state measurements, feeding SDN policies for route selection and admission control. The Messaging phase can be executed at the network edge or via an MDI hub: in the latter case, our verifier's acceptance thresholds are evaluated using keys derived from BSM outcomes, preserving non-repudiation while improving device independence [10].

5.8. Summary

Entangled states are not merely a resource used by our scheme—they are the core service envisioned for future quantum networks, where entanglement distribution is orchestrated much like bandwidth provisioning in classical networks [35,36]. Our protocol is therefore "network native": it consumes entanglement directly as the signing key material, relies on decoy-state statistics that can be interpreted as physical layer quality metrics, and exposes clear acceptance thresholds that network controllers can monitor for routing and scheduling. This alignment allows the protocol to plug seamlessly into standardized interfaces (e.g., ITU-T Y.3800, ETSI GS QKD 014/015) and benefit from network-level optimizations such as path selection, load balancing, and adaptive intensity control. Furthermore, its reliance on raw keys and minimal post-processing makes it latency-efficient and well-suited for time sensitive applications such as distributed ledgers or control signaling. Finally, because entanglement swapping and repeaters extend network reach, the same distribution phase naturally scales to metro to backbone deployments while preserving finite key, decoy-calibrated security guarantees. In this way, the proposed QDS is positioned not as a standalone cryptographic primitive but as an integral quantum

network application layer, bridging rigorous information theoretic security with practical, carrier-grade deployment.

6. Conclusions

We have presented an entanglement-based QDS that organizes distribution, estimation, and the messaging phase centered on a reordering step that replaces the symmetrization in conventional QS-L variants. The protocol determines authentication and verification thresholds from decoy-state and conclusive event statistics and operates without assuming a secure Bob–Charlie classical link, while preserving the balance of evidence required for signature verification.

Our finite-size analysis provides explicit bounds for robustness, unforgeability, and repudiation. These bounds are governed by the effective sample sizes and by the gaps between observed mismatch rates and the thresholds T_a and T_v derived from decoy-state statistics, which yield exponential suppression of all three failure probabilities under practical parameter choices. Overall security is followed by composition, with a residual statistical term to account for finite-size effects.

To gauge feasibility, we compared the distance-dependent signature rates of our protocol with a QS-L baseline under a common channel and detector model and the same security budget. Across the metro-to-regional distance range considered in Figure 1, the proposed design maintains a consistent advantage, and the simulation parameters align with the device and channel assumptions stated in the main text. Together with the network-integration options outlined in Section 5, these results indicate readiness for near-term deployment on quantum network testbeds.

Future work. We will implement a laboratory prototype based on the present protocol and validate end-to-end signing under calibrated device settings. Building on this prototype, we plan a field trial on a campus- or metro-scale fiber network to verify signature generation and verification under real-network conditions and to exercise the reordering workflow alongside the network-integration options discussed in Section 5.

Author Contributions: Conceptualization, C.H. and Y.-C.J.; Methodology, C.H.; Validation, C.H., Y.-C.J., O.K. and S.-W.J.; Formal analysis, C.H. and S.-W.J.; Investigation, C.H. and O.K.; Resources, O.K.; Data curation, Y.-C.J.; Writing—original draft, C.H.; Writing—review and editing, C.H., Y.-C.J., O.K. and S.-W.J.; Visualization, C.H.; Supervision, C.H.; Project administration, C.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Council of Science & Technology (NST) grant by the Korea government (MSIT) (No. CAP22053-200).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Finite-Size Calibration Examples

We instantiate the finite-size bounds with the parameterization used in this work. First, the robustness bound in Equation (5) reads

$$\epsilon_{rob} = exp\Big[-2n^{cu}(T_a - E_B^{cu})^2\Big],$$

so that, for a fixed acceptance margin $\Delta_A \equiv T_a - E_B^{cu}$, the honest-abort probability decays exponentially with the conclusive sample size n^{cu}.

Next, adopting the tail-calibration rule used in Section 4, the required conclusive sample size for a target failure budget ϵ_x and margin Δ is as follows:

$$n_x = \frac{2\ln\left(\frac{1}{\epsilon_x}\right)}{\Delta^2}$$

For the common budget $\epsilon_{rob} = \epsilon_{for} = \epsilon_{rep} = 10^{-10}$ and the margins employed in our simulations (Section 4), the resulting sizes are as follows:

$$\Delta_A = 0.005 \rightarrow \; n_A \approx 1.842 \times 10^6$$

$$\Delta_V = 0.01 \rightarrow \; n_V \approx 4.605 \times 10^5$$

$$\Delta_{11} = 0.012 \rightarrow \; n_{11} \approx 3.20 \times 10^5$$

Accordingly, the effective signature length is $n_{eff} = max\{n_A, n_V, n_{11}\} = n_A$, which is consistent with our rate–distance evaluation. Figure A1 visualizes ϵ_{rob} versus n_{cu} for $\Delta_A = 0.005$, directly exhibiting the exponential suppression predicted by Equation (5). Figure A2 plots n_x versus Δ under $\epsilon_x = 10^{-10}$ and marks the three operating margins used in our study. The $1/\Delta^2$ dependence highlights the benefit of modest calibration improvements to Δ.

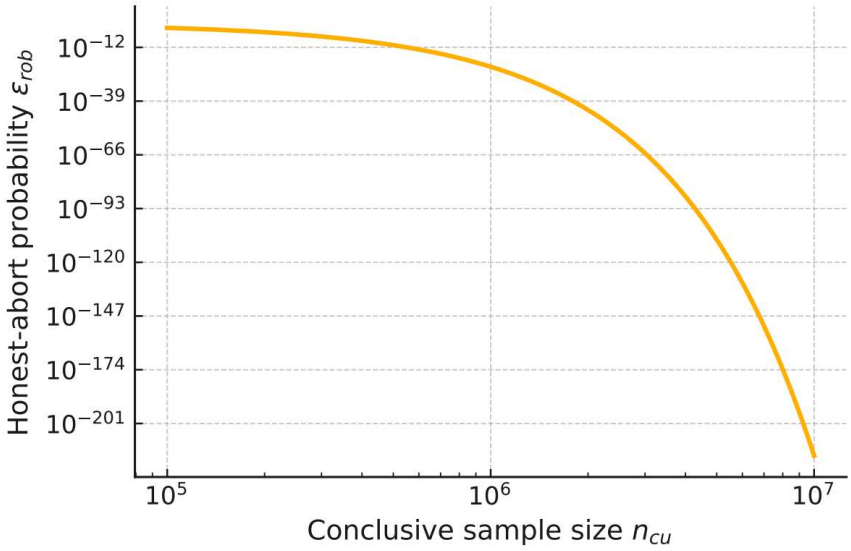

Figure A1. ϵ_{rob} versus n_{cu} for $\Delta_A = 0.005$.

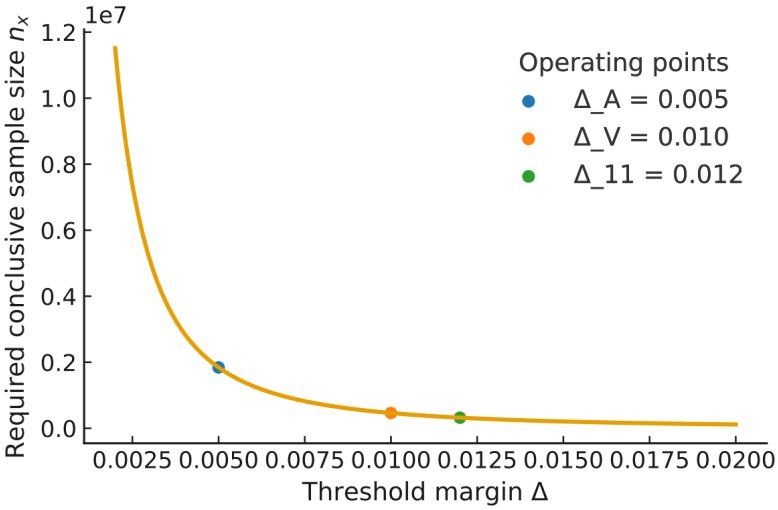

Figure A2. n_x versus Δ under $\epsilon_x = 10^{-10}$.

References

1. NIST. *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process*; NIST IR 8545; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025.
2. Gottesman, D.; Chuang, I. Quantum Digital Signatures. *arXiv* **2001**, arXiv:quant-ph/0105032. [CrossRef]
3. Lamport, L. *Constructing Digital Signatures from a One-Way Function*; Technical Report SRI-CSL-98; SRI International: Menlo Park, CA, USA, 1979.
4. Dunjko, V.; Wallden, P.; Andersson, E. Quantum Digital Signatures without Quantum Memory. *Phys. Rev. Lett.* **2014**, *112*, 040502. [CrossRef]
5. Li, B.-H.; Xie, Y.-M.; Cao, X.-Y.; Li, C.-L.; Fu, Y.; Yin, H.-L.; Chen, Z.-B. One-Time Universal Hashing Quantum Digital Signatures without Perfect Keys. *Phys. Rev. Appl.* **2023**, *20*, 044011. [CrossRef]
6. Puthoor, I.V.; Amiri, R.; Wallden, P.; Lucamarini, M.; Andersson, E. Measurement-Device-Independent Quantum Digital Signatures. *Phys. Rev. A* **2016**, *94*, 022328. [CrossRef]
7. Du, Y.; Li, B.-H.; Hua, X.; Cao, X.-Y.; Zhao, Z.; Xie, F.; Zhang, Z.; Yin, H.-L.; Xiao, X.; Wei, K. Chip-Integrated Quantum Signature Network over 200 km. *Light Sci. Appl.* **2025**, *14*, 108. [CrossRef]
8. Bian, J.-W.; Li, B.-H.; Xie, Y.-M.; Yin, H.-L.; Chen, Z.-B. Asynchronous Measurement-Device-Independent Quantum Digital Signatures. *Phys. Rev. A* **2024**, *110*, 012609. [CrossRef]
9. Zhu, J.-L.; Zhang, C.-H.; Wang, Q. Improved Finite-Size Analysis for Measurement-Device-Independent Quantum Digital Signatures. *Opt. Lett.* **2025**, *50*, 6245–6248. [CrossRef]
10. Yin, H.-L.; Wang, W.-L.; Tang, Y.-L.; Zhao, Q.; Liu, H.; Sun, X.-X.; Zhang, W.-J.; Li, H.; Puthoor, I.V.; You, L.-X.; et al. Experimental Measurement-Device-Independent Quantum Digital Signatures over a Metropolitan Network. *Phys. Rev. A* **2017**, *95*, 042338. [CrossRef]
11. Yin, H.-L.; Fu, Y.; Liu, H.; Tang, Q.-J.; Wang, J.; You, L.-X.; Zhang, W.-J.; Chen, S.-J.; Wang, Z.; Zhang, Q.; et al. Experimental Quantum Digital Signature over 102 km. *Phys. Rev. A* **2017**, *95*, 032334. [CrossRef]
12. Clarke, P.J.; Donaldson, W.; Collins, R.J.; Amiri, R.; Fujiwara, M.; Honjo, T.; Shimizu, K.; Takeoka, M.; Andersson, E.; Sasaki, M. Quantum Digital Signatures over 134 km Equivalent Installed Fiber. *Sci. Rep.* **2017**, *7*, 4635.
13. Chapman, J.C.; Alshowkan, M.; Qi, B.; Peters, N.A. Entanglement-Based Quantum Digital Signatures over a Deployed Campus Network. *Opt. Express* **2024**, *32*, 7521–7539. [CrossRef]
14. Yin, H.-L.; Fu, Y.; Li, C.-L.; Weng, C.-X.; Li, B.-H.; Gu, J.; Lu, Y.-S.; Huang, S.; Chen, Z.-B. Experimental Quantum Secure Network with Digital Signatures and Encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef] [PubMed]
15. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
16. Pan, D.; Liu, Y.-C.; Niu, P.; Zhang, H.; Zhang, F.; Wang, M.; Song, X.-T.; Chen, X.; Zheng, C.; Long, G.-L. Simultaneous Transmission of Information and Key Exchange Using the Same Photonic Quantum States. *Sci. Adv.* **2025**, *11*, eadt4627. [CrossRef]
17. Wang, M.; Long, G.-L. Quantum Secure Direct Communication: Whispering with Photons. *Natl. Sci. Rev.* **2025**, *12*, nwaf096. [CrossRef]
18. Zhou, L.; Sheng, Y.-B.; Long, G.L. Device-Independent Quantum Secure Direct Communication against Collective Attacks. *Sci. Bull.* **2020**, *65*, 12–20. [CrossRef] [PubMed]
19. Liu, C.; Zhang, C.; Gu, S.-P.; Wang, X.-F.; Zhou, L.; Sheng, Y.-B. Receiver-Device-Independent Quantum Secure Direct Communication. *Sci. China Phys. Mech. Astron.* **2025**, *68*, 250311. [CrossRef]
20. Ding, C.-W.; Wang, W.-Y.; Zhang, W.-D.; Zhou, L.; Sheng, Y.-B. Quantum Secure Direct Communication Based on Quantum Error Correction Code. *Appl. Phys. Lett.* **2025**, *126*, 024002. [CrossRef]
21. Lu, Y.-S.; Cao, X.-Y.; Weng, C.-X.; Gu, J.; Xie, Y.-M.; Zhou, M.-G.; Yin, H.-L.; Chen, Z.-B. Efficient Quantum Digital Signature without Symmetrization Step. *Opt. Express* **2021**, *29*, 10162–10171. [CrossRef]
22. Scarani, V.; Acín, A.; Ribordy, G.; Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]
23. Wei, Z.; Wang, W.; Zhang, Z.; Gao, M.; Ma, Z.; Ma, X. Decoy-State Quantum Key Distribution with Biased Basis Choice. *Sci. Rep.* **2013**, *3*, 2453. [CrossRef]
24. Grasselli, F.; Curty, M. Practical Decoy-State Method for Twin-Field Quantum Key Distribution. *New J. Phys.* **2019**, *21*, 073001. [CrossRef]
25. Tsurumaru, T.; Tamaki, K. Security Proof for Quantum-Key-Distribution System with Threshold Detectors. *Phys. Rev. A* **2008**, *78*, 032302. [CrossRef]
26. Ekert, A.K. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
27. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-Field Implementation of a Perfect Eavesdropper on a Quantum Cryptography System. *Nat. Commun.* **2011**, *2*, 349. [CrossRef]

28. Sajeed, S.; Huang, A.; Sun, S.; Xu, F.; Makarov, V.; Curty, M. Insecurity of Detector-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2016**, *117*, 250505. [CrossRef]
29. Liu, Y.; Chen, T.-Y.; Wang, L.-J.; Liang, H.; Shentu, G.-L.; Wang, J.; Cui, K.; Yin, H.; Liu, N.-L.; Li, L.; et al. Experimental Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2013**, *111*, 130502. [CrossRef] [PubMed]
30. Zhao, Y.; Zhou, Y.; Zhang, C.; Wang, X.; Xu, F.; Lo, H.-K. Security of Quantum Key Distribution with Source and Detector Imperfections through Combined Analysis. *arXiv* **2025**, arXiv:2507.03549.
31. Chen, X.; Li, Z.; Liu, Y.; Zhang, Q.; Pan, J.-W. Automatically Identifying Imperfections and Attacks in Practical Quantum Key Distribution Using Machine Learning. *Sci. China Inf. Sci.* **2023**, *66*, 180503. [CrossRef]
32. Scarani, V.; Renner, R. Quantum Cryptography with Finite Resources. *Phys. Rev. Lett.* **2008**, *100*, 200501. [CrossRef]
33. Li, M.-Y.; Cao, X.-Y.; Xie, Y.-M.; Yin, H.-L.; Chen, Z.-B. Finite-Key Analysis for Coherent One-Way Quantum Key Distribution. *Phys. Rev. Res.* **2024**, *6*, 013022. [CrossRef]
34. Amiri, R.; Wallden, P.; Kent, A.; Andersson, E. Secure Quantum Signatures Using Insecure Quantum Channels. *Phys. Rev. A* **2016**, *93*, 032325. [CrossRef]
35. Wehner, S.; Elkouss, D.; Hanson, R. Quantum Internet: A Vision for the Road Ahead. *Science* **2018**, *362*, eaam9288. [CrossRef]
36. *Recommendation Y.3800 (10/2019)*; Overview on Networks Supporting Quantum Key Distribution (QKD). ITU-T: Geneva, Switzerland, 2019. Available online: https://www.itu.int/rec/T-REC-Y.3800 (accessed on 17 November 2025).
37. Kržič, A.; Sharma, S.; Spiess, C.; Chandrashekara, U.; Töpfer, S.; Sauer, G.; del Campo, L.J.G.-M.; Kopf, T.; Petscharnig, S.; Grafenauer, T.; et al. Towards Metropolitan Free-Space Quantum Networks. *npj Quantum Inf.* **2023**, *9*, 59. [CrossRef]
38. *ETSI GS QKD 014 V1.1.1 (2019-02)*; Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API. ETSI: Sophia Antipolis, France, 2019. Available online: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf (accessed on 17 November 2025).
39. *ETSI GS QKD 015 (2022-04)*; Quantum Key Distribution (QKD); Control Interface for Software-Defined Networks. ETSI: Sophia Antipolis, France, 2022. Available online: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_qkd015v020101p.pdf (accessed on 17 November 2025).
40. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field Test of Quantum Key Distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef] [PubMed]
41. Poppe, A.; Peev, M.; Maurhart, O. Outline of the SECOQC Quantum-Key-Distribution Network in Vienna. *Int. J. Quantum Inf.* **2008**, *6*, 209–218. [CrossRef]
42. Bunandar, D.; Lentine, A.; Lee, C.; Cai, H.; Long, C.M.; Boynton, N.; Martinez, N.; DeRose, C.; Chen, C.; Grein, M.; et al. Metropolitan Quantum Key Distribution with Silicon Photonics. *Phys. Rev. X* **2018**, *8*, 021009. [CrossRef]
43. Ng, S.Q.; Kanitschar, F.; Zhang, G.; Wang, C. Gigabit-Rate Quantum Key Distribution on Integrated Photonic Chips. *arXiv* **2025**, arXiv:2504.08298. [CrossRef]
44. Bian, Y.; Pan, Y.; Xu, X.; Zhao, L.; Li, Y.; Huang, W.; Zhang, L.; Yu, S.; Zhang, Y.; Xu, B. Continuous-Variable Quantum Key Distribution over 28.6 km Fiber with an Integrated Silicon Photonic Receiver Chip. *Appl. Phys. Lett.* **2024**, *124*, 174001. [CrossRef]
45. Briegel, H.-J.; Dür, W.; Cirac, J.I.; Zoller, P. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.* **1998**, *81*, 5932–5935. [CrossRef]
46. Żukowski, M.; Zeilinger, A.; Horne, M.A.; Ekert, A.K. "Event-Ready-Detectors" Bell Experiment via Entanglement Swapping. *Phys. Rev. Lett.* **1993**, *71*, 4287–4290. [CrossRef] [PubMed]
47. CN-QCN Consortium. Implementation of Carrier-Grade Quantum Communication Networks over 10,000 km. *npj Quantum Inf.* **2025**, *11*, 89. [CrossRef]
48. Li, Y.; Cai, W.-Q.; Ren, J.-G.; Wang, C.-Z.; Yang, M.; Zhang, L.; Wu, H.-Y.; Chang, L.; Wu, J.-C.; Jin, B.; et al. Microsatellite-Based Real-Time Quantum Key Distribution. *Nature* **2025**, *640*, 47–54. [CrossRef] [PubMed]