

Experimental demonstration of a reconfigurable three-user quantum digital signature network

Jeong Youn-Chang

w31400@gmail.com

The affiliated institute of ETRI

Kim Seok

The affiliated institute of ETRI

Hong Changho

The affiliated institute of ETRI

Ji Se-Wan

The affiliated institute of ETRI

Article

Keywords: quantum digital signature, quantum network, quantum key distribution, time-bin encoding, information-theoretic security

Posted Date: October 13th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10500827/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Experimental demonstration of a reconfigurable three-user quantum digital signature network

Youn-Chang Jeong^{1*}, Seok Kim¹, Changho Hong¹, Se-Wan Ji¹

¹The Affiliated Institute of ETRI, Daejeon, 34044, Korea.

*Corresponding author(s). E-mail(s): w31400@gmail.com;

Abstract

Quantum digital signature (QDS) provides information-theoretic security and enables fundamental cryptographic functionalities, including integrity, non-repudiation, and data origin authentication. Existing QDS implementations, however, assign fixed user roles — signer, authenticator, and verifier — which limits their applicability in practical quantum networks, where role flexibility is essential. In this work, we implement a QDS protocol on a three-user fiber-optic quantum network in which any participant can dynamically assume the role of signer. Every node uses an identical design for encoding and decoding time-bin quantum states, enabling flexible signer assignment without hardware reconfiguration. We evaluate the signature rate and secret key rate for all possible signer configurations and show that valid signatures can be generated even in regimes where quantum key distribution (QKD) fails to produce a secret key. This result highlights a fundamental practical advantage of QDS over QKD at small classical post-processing block sizes, where key distillation is not achievable. Our results establish the feasibility of reconfigurable quantum signature networks and represent an important step toward scalable and robust quantum communication infrastructures.

Keywords: quantum digital signature, quantum network, quantum key distribution, time-bin encoding, information-theoretic security

1 Introduction

Cryptography is designed to ensure four primary security objectives: confidentiality, integrity, authentication, and non-repudiation [1]. Authentication can be further

divided into entity authentication and data origin authentication. As a critical cryptographic primitive, digital signatures provide integrity, non-repudiation, and data origin authentication for digital messages or documents transmitted over the Internet. Unlike entity authentication, which verifies the active presence of a party in real time, digital signatures focus on ensuring the provenance and immutability of the transmitted content.

The security of digital signatures is increasingly threatened by ongoing advances in quantum computing, novel algorithms, and growing computational power [2, 3]. Most widely used digital signature schemes rely on public-key cryptosystems whose security rests on the computational hardness of certain mathematical problems. However, Shor’s algorithm [4] demonstrates that such problems can be solved in polynomial time on a sufficiently powerful quantum computer, thereby undermining the security of modern public-key signature schemes. Digital signatures based on symmetric-key primitives are not immune either: quantum algorithms such as Grover’s algorithm [5] can quadratically reduce their effective security level. Consequently, classical digital signature schemes can no longer be considered robust against potential quantum adversaries.

To remain secure even in the presence of quantum adversaries, digital signature schemes must therefore achieve unconditional security. Unconditional security refers to security that can be proven without imposing any restrictions on the computational power or technological capabilities available to an adversary acting on the transmitted signals [6]. Such schemes provide information-theoretic security (ITS), which does not rely on computational hardness assumptions. Two types of digital signature schemes can achieve unconditional security [7]: unconditionally secure “classical” signature schemes and unconditionally secure “direct” quantum signature schemes. In the unconditionally secure classical signature schemes, a secret key is first established using an ITS method such as quantum key distribution (QKD) [8]. This shared secret key is then used for the signing process and consumed after one-time use. Since the secret key generated by QKD provides ITS, the resulting signature scheme can also achieve ITS. However, this approach requires all participants to behave honestly during the key distribution stage. In contrast, unconditionally secure direct quantum signature schemes use quantum states as signature elements for signing, authentication, and verification, without first distilling a highly secure shared secret key. These schemes assume that no more than half of the participants are dishonest, but they typically require a relatively large number of signature keys. Each approach thus carries its own advantages and disadvantages.

This study focuses on quantum digital signature (QDS), an unconditionally secure direct quantum signature scheme. In contrast to QKD, QDS does not require error correction or privacy amplification to form its signature keys. Instead, it assumes that potential adversaries are legitimate participants in the protocol. QDS protocols require at least three participants and are typically implemented over a quantum network. In a three-participant protocol, security is maintained even if one of the three participants is dishonest. Notably, dishonest participants pose a greater security threat than external eavesdroppers.

The first QDS protocol [9], GC-QDS, was proposed by Gottesman and Chuang in 2001 as a quantum analogue of Lamport’s one-time signature scheme. This protocol, however, required demanding resources—including long-term quantum memory, entanglement swapping, and authenticated quantum channels—that made practical implementation difficult. To overcome these limitations, a series of modified protocols [10–15] was proposed and subsequently demonstrated experimentally [16–21], progressively eliminating the need for quantum memory, entanglement swapping, and authenticated quantum channels. Among these, the protocol proposed by Amiri et al. in 2016 [15] is particularly relevant to the present work, as it removes the requirement for authenticated quantum channels and can be implemented using QKD-type systems with modified classical post-processing [22–25].

This protocol further simplifies the security analysis by avoiding a setting in which a dishonest signer distributes quantum states to the recipients. If the signer were permitted to prepare and send the states, unwanted correlations could be introduced between the recipients’ signature data. To prevent this, the protocol is designed so that the recipients, rather than the signer, prepare and send the quantum states during the distribution stage. Beyond these GC-QDS-derived protocols, other QDS families have also been proposed, including entanglement-based [26, 27], measurement-device-independent [28], twin-field-based [29, 30], and OTUH-based schemes [31–33], which extend QDS toward multipartite networking, detector-side-channel resistance, long-distance performance, and improved signing efficiency.

In this work, we implement the QDS protocol in a quantum network in which any participant can act as the signer. To this end, we construct a three-node fiber-optic network in which each node can both transmit and receive quantum states. When a participant assumes the role of signer, it receives quantum states from the other two participants, establishes raw keys, and uses them to generate the signing, authentication, and verification keys for the message. For the secure classical communication required in the symmetrization step, the authenticator and verifier establish a secret key through classical post-processing. Unlike previous implementations with a fixed signer, this architecture enables flexible signer assignment in a general quantum network, demonstrating that any node can serve as the signer.

2 Results

We first summarize the network architecture underlying the measurements; the QDS protocol, security analysis, and optical setup are provided in the Methods (see Fig. 3). The three nodes—Alice, Bob, and Charlie—are linked through a network switch, and because every node uses an identical optical design, any participant can be assigned the role of signer. When a node acts as the signer, the network switch routes quantum states to it from the other two participants, with the ON/OFF state of the switch selecting which link is active. The signer then forms its signature keys from the resulting raw keys, while the authenticator and verifier additionally perform QKD to share the secret key used in the symmetrization step.

We evaluated the generated keys and their associated security parameters for all three possible signer assignments in the three-user QDS network. When Alice acted as

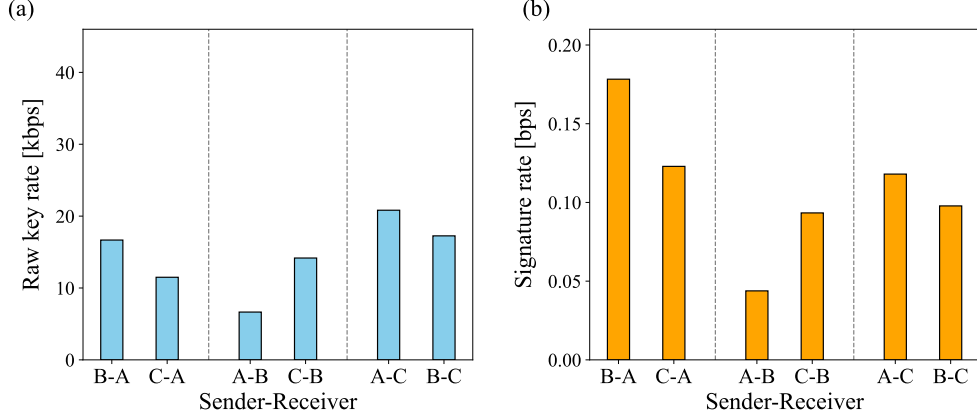


Fig. 1 Experimental results of (a) raw key rate and (b) signature rate for all sender–receiver pairs in the three-user QDS network. A, B, and C denote Alice, Bob, and Charlie, respectively. Each pair indicates the direction of quantum state transmission.

the signer, with Bob and Charlie serving as the authenticator and verifier, respectively, she received quantum states from Bob with the switch set to OFF and from Charlie with the switch set to ON, thereby generating the raw keys used for signature generation and verification. When Bob acted as the signer, he received quantum states from Alice with the switch set to OFF and from Charlie with the switch set to ON. When Charlie acted as the signer, he received quantum states from Alice with the switch set to OFF and from Bob with the switch set to ON. In each case, the signer generated raw keys with the other two participants through quantum state exchange, while the authenticator and verifier performed QKD to establish a secret key via classical post-processing.

Figure 1(a) shows the raw key rates for all sender–receiver pairs. Here, A, B, and C denote Alice, Bob, and Charlie, respectively; for example, B-A represents quantum state transmission from Bob to Alice. The raw key rate of the B-A link is higher than that of the A-B link, despite identical quantum channel transmittance in both directions. This asymmetry is attributed to the difference in detection efficiency at the receiving node [34]. Furthermore, the raw key rates of the authenticator–signer and verifier–signer links are similar even when the corresponding quantum channel transmittance differs. This indicates that, in our system, detection efficiency has a more significant effect on the raw key rate than channel transmittance.

The signature rates between the signer and the authenticator or verifier are shown in Fig. 1(b). The signature rate is defined as the number of signatures generated per second for a one-bit message, given by $r_{QDS} = \frac{qQf}{L}$, where q is the key sifting efficiency corresponding to the protocol efficiency of QKD, Q is the overall gain, f is the system repetition rate, and L is the signature length required per one-bit message. In our system, the repetition rate is $f = 10$ MHz. Since the raw key rates vary across different sender–receiver pairs, the corresponding signature rates also differ. When Alice acts as the signer, a relatively higher signature rate is observed compared with the other

Signer	Alice	Bob	Charlie
L	8.5×10^4	1.38×10^5	1.604×10^5
Q_{auth}	0.0103	0.0092	0.0130
Q_{ver}	0.0128	0.0228	0.0199
E^U	0.0361	0.0410	0.0368
s_a	0.0577	0.0580	0.0526
s_v	0.0793	0.0749	0.0683
p_E	0.1009	0.0919	0.0840
$P(\text{repudiation})$	9.84×10^{-5}	9.95×10^{-5}	9.94×10^{-5}

Table 1 Summary of the signature length L , QBERs for the authenticator and verifier (Q_{auth} , Q_{ver}), upper-bound error rate E^U , authentication and verification threshold error rates (s_a , s_v), and repudiation failure probability $P(\text{repudiation})$ for each signer configuration, obtained from the finite-key security analysis. The robustness and forging failure probabilities were set to 2×10^{-5} and 1×10^{-4} , respectively.

configurations, primarily because the required signature length L is smaller in this case.

Since the signature rate is inversely proportional to the signature length L , determining L under the given experimental conditions is essential. The required signature length for a one-bit message is determined through finite-key security analysis, as it depends on the QBERs, raw key rate, and security parameters associated with unforgeability, non-repudiation, and transferability. Using the security parameters $\epsilon_{PE} = 10^{-5}$, $\alpha = 10^{-5}$, and $\epsilon = 10^{-10}$, we calculated the required signature length L for each signer configuration. In this analysis, the test key size was set to 10% of the corresponding signature length.

The experimental results are summarized in Table 1, including the QBERs for the authenticator and verifier, the upper-bound error rate E^U , the authentication and verification threshold error rates (s_a , s_v), the minimum forger mismatch rate p_E , and repudiation failure probability $P(\text{repudiation})$ for each signer configuration; these security quantities and the finite-key relations among them are defined in the Methods. The robustness failure probability is bounded by 2×10^{-5} according to Eq. (1) (Methods), and the forging probability is obtained as 1×10^{-4} . The required signature length L differs across the three signer configurations because the quantum channel transmittance and detector performance vary along each transmission path, leading to different error characteristics and security bounds.

The authentication and verification threshold error rates serve as criteria for validating the transmitted message and signature during the messaging stage. These thresholds are determined from the upper bound error rate E^U and the minimum mismatch rate p_E that can be introduced by a dishonest party. In our analysis, the repudiation failure probability was set to be no greater than the forging probability in order to balance the dominant failure contributions, as the individual failure probabilities contribute to the overall security parameter P_{sec} , which is constrained by Eqs. (1) and (2) in the Methods.

The upper bound error rate E^U is estimated from the observed QBERs of the relevant links. For example, when Alice is the signer, E^U is determined from the

Bob-Alice and Charlie-Alice links. Consequently, E^U varies depending on the signer assignment, which leads to different threshold error rates. However, exchanging the roles of the authenticator and verifier does not affect these thresholds, since the upper bound is determined by the worst-case (maximum) error rate.

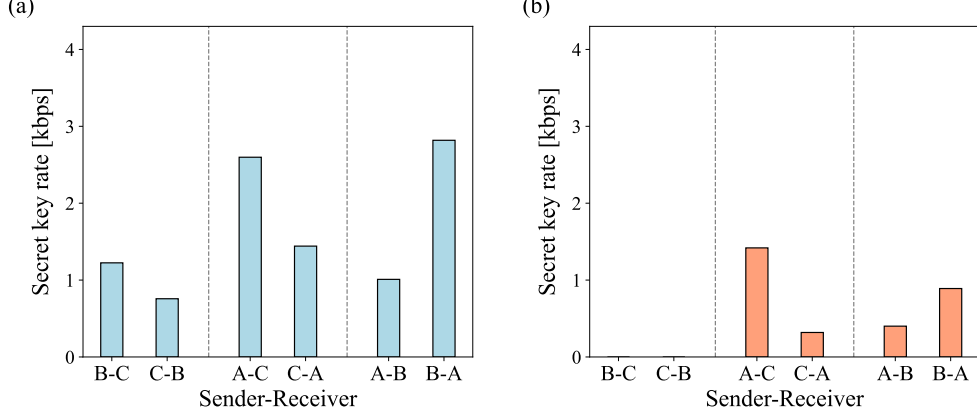


Fig. 2 Secret key rates between the authenticator and verifier for all signer configurations in the three-user QDS network, obtained using two classical post-processing block sizes: (a) a fixed block size of 10^6 bits, corresponding to the secret key actually used for the symmetrization step, and (b) a block size corresponding to the signature length, $(L+k)$ bits, shown as a contrast to illustrate QKD performance at the short block used for signature generation. A, B, and C denote Alice, Bob, and Charlie, respectively, and each pair indicates the direction of quantum state transmission used for secret key generation. In (b), no secret key is generated for the B-C and C-B directions, since the information disclosed during error correction exceeds the secret information shared between the two nodes.

To implement the QDS network, secure classical communication between the authenticator and verifier is required, which necessitates a shared secret key with unconditional security. In our system, this secret key is generated via QKD, and the finite-key analysis is performed for two different post-processing block sizes [34, 35]. For example, when Alice is the signer, the raw key shared between Bob and Charlie is processed through classical post-processing to generate a secret key. This post-processing consists of error correction and privacy amplification, where the Winnow protocol was employed for error correction and a Toeplitz matrix was used for privacy amplification.

The resulting secret key rates after classical post-processing are shown in Fig. 2. In the Winnow protocol, a block configuration of $[16, 32, 64, 128]$ was used for a QBER of approximately 2% or higher, while a configuration $[32, 64, 128, 256, 512]$ was used for a QBER of approximately 2% or lower. The secret key rate corresponds to the length of secret keys generated per second. Although raw keys must be accumulated over a period corresponding to the classical post-processing block size, we define the secret key rate here as the secret key length divided by the time required to accumulate one block.

As shown in Fig. 2 (a), the authenticator and verifier generate the secret key using a classical post-processing block size of 10^6 bits. The secret key is used in the symmetrization step during the signing process between the authenticator and verifier. Even for the same quantum channel, the secret key rates differ depending on the transmission direction, since the secret key rate depends not only on the channel transmittance but also on the detection efficiency and detector characteristics at the receiver.

Notably, a link with a relatively high signature rate (e.g., B-A) does not necessarily yield a higher secret key rate. This is because the signature rate depends on the raw key generation and the required signature length, which is affected by both the authenticator-signer and verifier-signer links, whereas the secret key rate is obtained from classical post-processing over a single sender-receiver link. In other words, the signature involves two links among three nodes, while the secret key involves only one link between two nodes.

We also generated a secret key using a classical post-processing block size corresponding to the signature length L and sample size k . The classical post-processing was carried out in the same manner as described above. As shown in Fig. 2 (b), no secret key can be generated between Bob and Charlie or between Charlie and Bob. This is because the amount of information disclosed during error correction exceeds the amount of secret information shared between the two nodes.

3 Discussion

For the short block size of $(L + k)$ bits actually used for signature, QKD fails while QDS succeeds, owing to statistical fluctuations. QKD typically requires a large block size, generally 10^5 to 10^6 bits or more, during parameter estimation in order to tightly bound the information available to an eavesdropper. In contrast, the goal of QDS is not to keep the message confidential but to prevent forgery and repudiation; its security can therefore be established using correlated data of a relatively short length $(L + k)$. This difference reflects the distinct objectives of the two protocols: QKD aims to establish a shared secret key through error correction and privacy amplification, whereas QDS relies on correlated raw keys to provide message integrity, non-repudiation, and data origin authentication. Moreover, the ability to operate with small block sizes implies lower latency between network nodes and reduced memory buffer requirements. This supports the view that QDS can operate more lightly and rapidly than QKD in future quantum network environments.

In this work, we constructed a three-user QDS network in which any participant can act as the signer and experimentally demonstrated the QDS protocol for all possible signer configurations. In contrast to previous implementations where the signer role was fixed, our system enables flexible signer assignment, yielding valid signatures and threshold error rates for each configuration. In addition, secret keys were generated via QKD to support secure classical communication between the authenticator and verifier.

Importantly, we demonstrated that QDS can generate valid signatures even at small classical post-processing block sizes where QKD fails to produce a final secret

key, highlighting a fundamental practical advantage of QDS over QKD. This advantage stems from QDS requiring only short correlated data rather than a fully distilled secret key, which in turn implies lower latency and reduced memory requirements between network nodes. These results establish the feasibility of reconfigurable quantum signature networks and represent an important step toward scalable and robust quantum communication systems. Our work paves the way for integrating QDS into future quantum network infrastructures.

4 Methods

4.1 Protocol and security analysis

QDS provides three fundamental security properties: unforgeability, non-repudiation, and transferability. Unforgeability ensures that no dishonest party can generate a valid signature for a message on behalf of the signer. Non-repudiation ensures that the signer cannot later deny having signed a message that has been accepted by a recipient. Transferability guarantees that if one recipient accepts a signature, all other honest recipients will also accept it when it is forwarded to them.

In the QDS protocol proposed by Amiri et al. [15], authenticated classical channels are assumed between the signer and the authenticator, and between the signer and the verifier. In addition, a secret classical channel is assumed between the authenticator and the verifier, which can be established via QKD.

The QDS protocol consists of two stages: the distribution stage and the messaging stage. In the distribution stage, participants generate and exchange keys used for signature generation and verification through quantum and classical communication. During this stage, a secure classical channel must exist between the authenticator and the verifier that is inaccessible to the signer. In the messaging stage, messages are signed and verified using classical communication.

If Alice is the signer, Bob is the authenticator, and Charlie is the verifier, the protocol proceeds as follows. In the distribution stage, Alice generates raw keys A_m^B and A_m^C with Bob and Charlie, respectively, for each message bit $m \in \{0, 1\}$. The corresponding raw keys held by Bob and Charlie are denoted K_m^B and K_m^C , respectively, where each raw key has length L . Alice's signature for message m is then defined as $\text{Sig}_m = (A_m^B, A_m^C)$. Bob and Charlie then symmetrize their raw keys by randomly forwarding half of their bits to each other through a secure classical channel. After symmetrization, Bob and Charlie obtain $S_m^B = (K_{m,keep}^B, K_{m,forward}^C)$ and $S_m^C = (K_{m,keep}^C, K_{m,forward}^B)$, respectively, while the retained portions remain private.

Since the generated keys may contain errors, the upper bound on the observed error rate $E_{B,A}^U$ is estimated using the Serfling inequality [36]. Specifically, following the sender-receiver convention, the upper bound for the Bob-to-Alice link is given by

$$E_{B,A}^U = E_{B,A} + \sqrt{\frac{\ln(1/\epsilon_{PE})}{2k} \left(1 - \frac{2(k-1)}{L}\right)},$$

where ϵ_{PE} denotes the failure probability of parameter estimation and k is the sample size. When Alice is the signer, the overall upper bound on error rate is defined as

$E^U = \max(E_{B,A}^U, E_{C,A}^U)$. In addition, the minimum mismatch rate p_E for a forging attacker is determined by

$$h(p_E) = \frac{2s_{X,0}^L}{L} + \frac{2s_{X,1}^L}{L}[1 - h(\phi_{X,1}^U)],$$

as derived in Ref. [15, 34]. Here, $h(x)$ denotes the binary Shannon entropy, $s_{X,0}^L$ and $s_{X,1}^L$ represent the lower bounds on the number of vacuum events and single-photon events, respectively. $\phi_{X,1}^U$ is the upper bound of the phase error rate associated with the single-photon events in the X basis.

In the messaging stage, Alice signs a one-bit message m and sends (m, Sig_m) to the desired recipient, Bob, who acts as the authenticator. Bob compares Sig_m with his symmetrized key S_m^B and counts the mismatches in the retained and forwarded parts separately. If both mismatch counts are below $s_a \frac{L}{2}$, Bob accepts the message and then forwards (m, Sig_m) to Charlie, where s_a is the authentication threshold error rate. Charlie similarly compares Sig_m with his symmetrized key S_m^C , and if both mismatch counts are below $s_v \frac{L}{2}$, Charlie accepts the forwarded message, where s_v is the verification threshold error rate. The threshold error rates satisfy $0 < s_a < s_v < 1/2$ and are given by $s_a = E^U + \frac{p_E - E^U}{3}$ and $s_v = E^U + \frac{2(p_E - E^U)}{3}$. A message accepted under these conditions is thus guaranteed to have originated from the signer and cannot be repudiated.

For the security analysis of the QDS protocol, three failure probabilities must be considered: robustness $P(\text{robust})$, repudiation $P(\text{repudiation})$, and forging $P(\text{forge})$. Their upper bounds are given by

$$\begin{aligned} P(\text{robust}) &\leq 2\epsilon_{PE}, \\ P(\text{repudiation}) &\leq 2 \exp \left[-\frac{1}{4}(s_v - s_a)^2 L \right] \\ P(\text{forge}) &\leq \alpha + \epsilon_F + 8\epsilon_{PE} \end{aligned} \tag{1}$$

Here, α is a free optimization parameter used in the forging bound, and ϵ_F denotes the failure probability associated with the estimation of the forger's information based on smooth min-entropy analysis. In the bound on the forging probability, the term $8\epsilon_{PE}$ accounts for the failure probabilities arising from finite-size estimation of quantum channel parameters:

$$\epsilon_F = \frac{1}{\alpha} \left[2^{-\{s_{X,0}^L + s_{X,1}^L[1 - h(\phi_{X,1}^U)] - \frac{L}{2} h(s_v)\}} + \epsilon \right],$$

where ϵ denotes the smoothing parameter of the smooth min-entropy, which enters the min-entropy bound as an additive term proportional to $\log_2(\frac{1}{\epsilon})$ and appears as the additive term in the expression for ϵ_F above. The overall security parameter P_{sec} is then defined as an upper bound on QDS protocol failure probabilities and satisfies

$$P_{sec} \geq \max\{P(\text{robust}), P(\text{forge}), P(\text{repudiation})\}. \tag{2}$$

4.2 Experimental setup

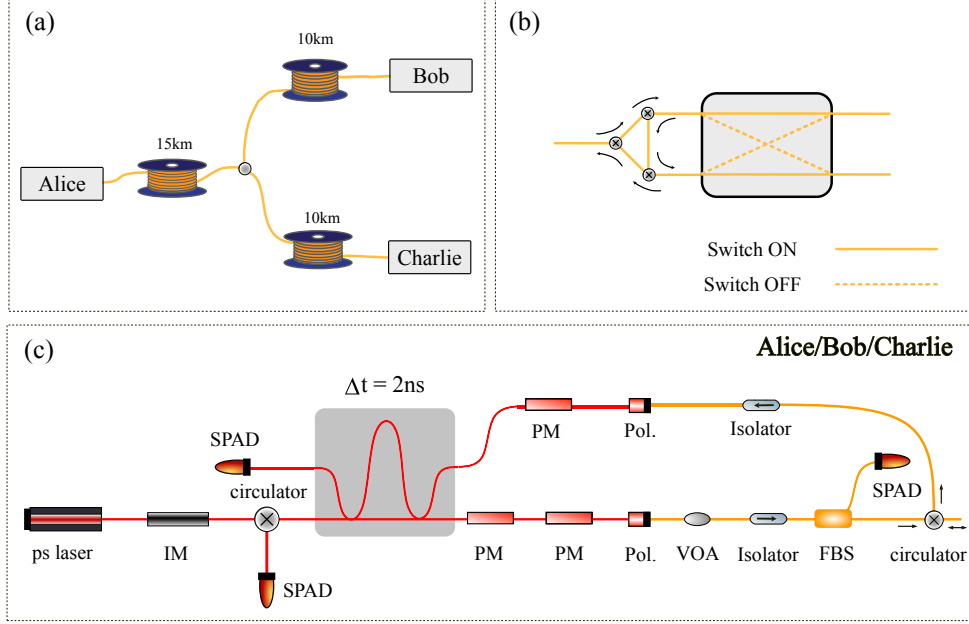


Fig. 3 (a) QDS network composed of three nodes (Alice, Bob, and Charlie), quantum channels, and a network switch. (b) Architecture of the network switch, consisting of three 3-port optical circulators and a 2×2 optical switch. (c) Experimental optical setup implemented at each node of the QDS network. All nodes are identically designed to encode and decode time-bin quantum states. Each node consists of a picosecond pulsed laser (ps laser), an intensity modulator (IM), an asymmetric Mach-Zehnder interferometer, phase modulators (PMs), a polarizer (Pol.), a variable optical attenuator (VOA), isolators, a fiber beam splitter (FBS), telecom-wavelength single-photon avalanche detectors (SPADs), and optical circulators.

Our QDS network is configured as shown in Fig. 3(a). Three participants, Alice, Bob, and Charlie, are connected to a network switch via quantum channels of approximate lengths 15 km, 10 km, and 10 km, respectively. In the protocol, each participant can dynamically assume any of the three roles: signer, authenticator, or verifier. When Alice acts as the signer, for instance, she first sends a message and its corresponding signature to the desired recipient, who serves as the authenticator. The remaining participant, who receives the forwarded message and signature, becomes the verifier.

As shown in Fig. 3(b), the network switch controls the routing of quantum state transmission in the QDS network. It comprises three 3-port optical circulators interconnected with a 2×2 optical switch. These circulators form an effective three-port routing device that enables quantum state transmission among the three nodes. In a standard 3-port optical circulator, light entering port 1 exits from port 2, and light entering port 2 exits from port 3; however, light entering port 3 does not exit from port 1. To overcome this limitation, the circulators are interconnected such that port

3 of each circulator is connected to port 2 of another, thereby enabling bidirectional routing among all three ports [34]. This configuration can be generalized to construct an N -port optical routing device.

One output port of the composed circulator is connected to Alice, while the remaining two output ports are connected to a 2×2 optical switch, whose outputs are connected to Bob and Charlie, respectively. By toggling the optical paths between Bob and Charlie, the sender and receiver of the transmitted quantum states can be dynamically selected.

In our quantum network, any participant can assume the role of signer. The signer must receive quantum states from the other participants, who transmit their states to it. For instance, when Alice is the signer, she receives quantum states from both Bob and Charlie. The network switch is configured such that Alice receives quantum states from Bob when the switch is OFF and from Charlie when the switch is ON. Since all participants have identical setups, each node can both transmit and receive quantum states.

The participants encode information in four time-bin quantum states and employ the two-decoy-state method, which uses three intensity levels: a signal state, a decoy 1 state, and a decoy 2 state. Specifically, the decoy 2 state for Alice and Bob is set to the vacuum state. As shown in Fig. 3(c), each participant employs an identical optical setup that enables both the encoding and decoding of time-bin quantum states. In the encoding process, a picosecond pulsed laser with a pulse width of less than 500 ps is used. The ps laser wavelengths are 1548.06 nm for Alice, 1547.86 nm for Bob, and 1549.32 nm for Charlie. The laser generates optical pulses, whose intensities are modulated by an intensity modulator (IM) to prepare the signal, decoy 1, and decoy 2 states. To generate the vacuum state for Alice and Bob, the laser is turned off to create an empty pulse; conversely, a pulse is always generated in Charlie's setup to create his decoy 2 state.

The pulses are then injected into an asymmetric Mach-Zehnder interferometer implemented on a planar lightwave circuit (PLC), with a path delay of 2 ns between the long and short arms. After passing through the PLC, each pulse is prepared in the time-bin state $\frac{1}{\sqrt{2}}(|e\rangle + |l\rangle)$, where $|e\rangle$ and $|l\rangle$ denote the early and late time-bin states, respectively. This state is further converted into one of the four states, $\frac{1}{\sqrt{2}}(|e\rangle + |l\rangle)$, $\frac{1}{\sqrt{2}}(|e\rangle - |l\rangle)$, $\frac{1}{\sqrt{2}}(|e\rangle + i|l\rangle)$, and $\frac{1}{\sqrt{2}}(|e\rangle - i|l\rangle)$, by two phase modulators (PMs), according to the sender's bit value (0 or 1) and basis choice (X or Y).

The optical pulses are then strongly attenuated by a variable optical attenuator (VOA) to reduce the average photon number per pulse to below 1. The attenuated pulses are divided into two paths by a fiber beam splitter (FBS). One path leads to the output port connected to the network switch, while the other path is directed to a single-photon avalanche detector (SPAD). The SPAD monitors the presence or absence of photons in each pulse, and the measurement results are used to estimate the average photon number per pulse for the signal and decoy states. In the experiment, the average photon numbers were set to approximately 0.5 for the signal state and 0.15 for the weak decoy state. The actual average photon numbers of signal and decoy states are summarized in Table 2. The emission probabilities of the signal, weak decoy, and vacuum decoy states are set in the ratio 0.502 : 0.207 : 0.291.

Signer	Alice		Bob		Charlie	
Sender	Bob	Charlie	Alice	Charlie	Alice	Bob
μ_1	0.5771	0.5342	0.5297	0.5016	0.5239	0.6022
μ_2	0.1320	0.1496	0.1088	0.0996	0.1331	0.1412
μ_3	0.0025	0.0107	0.0075	0.0247	0.0078	0.0026

Table 2 Average photon numbers (μ_1 , μ_2 , μ_3) of the signal, decoy 1, and decoy 2 states for each quantum channel link. The signer denotes the receiver. For Alice and Bob, the average photon number of decoy 2 (μ_3) corresponds to the dark count rate of the sender’s monitoring detector.

In the decoding process, the quantum state transmitted by the sender enters a circulator, which directs the incoming signal to the upper path. The measurement basis (X or Y) is randomly selected via a PM, and the state is decoded using an asymmetric Mach-Zehnder interferometer shared with the encoding optical setup, followed by detection with two SPADs operating with a gating window of approximately 1.5 ns. The selected basis and detection outcomes are recorded by a field-programmable gate array (FPGA) at each node. All devices are synchronized via a 10 MHz TTL signal.

At the start of the distribution stage, the participants assign the roles of signer, authenticator, and verifier. The signer then receives quantum states from the authenticator and verifier, and all participants exchange their measurement results and basis information to generate raw keys. Throughout this work, the term raw key refers to the correlated key obtained after basis reconciliation, which corresponds to the sifted key in conventional QKD terminology; unlike in QKD, these keys are used directly for signing without further error correction or privacy amplification. From these raw keys, the participants derive the signature, authentication, verification, and secret keys used in the subsequent messaging stage.

The signer generates a signature key corresponding to the message data bit, where the signature length for one-bit data is L . In addition, the signer randomly samples k test keys from the raw key for parameter estimation. These test keys are used to evaluate the security parameters associated with unforgeability, non-repudiation, and transferability. The authentication and verification threshold error rates are determined from the QBER and gain of the raw key.

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

Data availability

The datasets generated and analyzed during the current study, including raw detection logs, raw keys, signature data, and QBER data, are available from the corresponding author upon reasonable request.

Code availability

The custom code used to generate and analyze the results reported in this study is available from the corresponding author upon reasonable request.

Author contributions

Y.C.J. conceived the experiment(s); Y.C.J. and S.K. conducted the experiment(s); Y.C.J. performed data analysis; and Y.C.J., C.H., and S.W.J. analyzed the results. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

References

- [1] Katz, J. & Lindell, Y. Introduction to Modern Cryptography: Principles and Protocols (Chapman and Hall/CRC, 2007).
- [2] Buchmann, J. et al. Post-quantum signatures. Cryptology ePrint Archive, Paper 2004/297 (2004). URL <https://eprint.iacr.org/2004/297>.
- [3] Bozzio, M., Crépeau, C., Wallden, P. & Walther, P. Quantum cryptography beyond key distribution: Theory and experiment. *Rev. Mod. Phys.* **97**, 045006 (2025).
- [4] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484—1509 (1997).
- [5] Grover, L. K. A fast quantum mechanical algorithm for database search, *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96* 212—219 (1996).
- [6] Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301—1350 (2009).
- [7] Amiri, R. & Andersson, E. Unconditionally secure quantum signatures. *Entropy* **17**, 5635—5659 (2015).
- [8] Portmann, C. & Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).
- [9] Gottesman, D. & Chuang, I. Quantum digital signatures (2001). [quant-ph/0105032](#).
- [10] Andersson, E., Curty, M. & Jex, I. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev. A* **74**, 022304 (2006).

- [11] Dunjko, V., Wallden, P. & Andersson, E. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.* **112**, 040502 (2014).
- [12] Wallden, P., Dunjko, V., Kent, A. & Andersson, E. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A* **91**, 042304 (2015).
- [13] Yin, H.-L., Fu, Y. & Chen, Z.-B. Practical quantum digital signature. *Phys. Rev. A* **93**, 032316 (2016).
- [14] Lu, Y.-S. et al. Efficient quantum digital signatures without symmetrization step. *Opt. Express* **29**, 10162 (2021).
- [15] Amiri, R., Wallden, P., Kent, A. & Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **93**, 032325 (2016).
- [16] Clarke, P. J. et al. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.* **3**, 1174 (2012).
- [17] Collins, R. J. et al. Realization of quantum digital signatures without the requirement of quantum memory. *Phys. Rev. Lett.* **113**, 040502 (2014).
- [18] Croal, C. et al. Free-space quantum signatures using heterodyne measurements. *Phys. Rev. Lett.* **117**, 100503 (2016).
- [19] Donaldson, R. J. et al. Experimental demonstration of kilometer-range quantum digital signatures. *Phys. Rev. A* **93**, 012329 (2016).
- [20] Zhang, C.-H. et al. Proof-of-principle demonstration of passive decoy-state quantum digital signatures over 200 km. *Phys. Rev. Appl.* **10**, 034033 (2018).
- [21] Yin, H.-L. et al. Experimental quantum digital signature over 102 km. *Phys. Rev. A* **95**, 032334 (2017).
- [22] Collins, R. J. et al. Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. *Opt. Lett.* **41**, 4883 (2016).
- [23] Collins, R. J. et al. Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution. *Sci. Rep.* **7**, 3235 (2017).
- [24] An, X.-B. et al. Practical quantum digital signature with a gigahertz BB84 quantum key distribution system. *Opt. Lett.* **44**, 139 (2018).
- [25] Ding, H.-J. et al. 280-km experimental demonstration of a quantum digital signature with one decoy state. *Opt. Lett.* **45**, 1711 (2020).

- [26] Zeng, G. & Keitel, C. H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **65**, 042312 (2002).
- [27] Chapman, J. C., Alshowkan, M., Qi, B. & Peters, N. A. Entanglement-based quantum digital signatures over a deployed campus network. *Opt. Express* **32**, 7521 (2024).
- [28] Puthoor, I. V., Amiri, R., Wallden, P., Curty, M. & Andersson, E. Measurement-device-independent quantum digital signatures. *Phys. Rev. A* **94**, 022328 (2016).
- [29] Zhang, C.-H., Zhou, X., Zhang, C.-M., Li, J. & Wang, Q. Twin-field quantum digital signatures. *Opt. Lett.* **46**, 3757 (2021).
- [30] Zhang, M.-H. et al. Practical long-distance twin-field quantum digital signatures. *Quantum Inf. Process.* **21**, 150 (2022).
- [31] Yin, H.-L. et al. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **10**, nwac228 (2022).
- [32] Li, B.-H. et al. One-time universal hashing quantum digital signatures without perfect keys. *Phys. Rev. Appl.* **20**, 044011 (2023).
- [33] Cao, X.-Y. et al. Experimental quantum e-commerce. *Sci. Adv.* **10**, eadk3258 (2024).
- [34] Jeong, Y.-C. et al. Quantum key distribution over a three-user fiber network with passive optical circulator. Research Square preprint (2025). URL <https://www.researchsquare.com/article/rs-7767711/v1>. Under review at Sci. Rep.
- [35] Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
- [36] Serfling, R. J. Probability inequalities for the sum in sampling without replacement. *Ann. Stat.* **2**, 39—48 (1974).