

Experimental demonstration of a multisigner quantum digital signature system

Wenli Ding,^{1,*} Xi Deng,^{1,*} Chao Li,¹ Yuanhua Li,^{1,†} Jia Lin,^{1,‡} Yuanlin Zheng^{④,2,§} and Xianfeng Chen^{2,||}

¹Department of Physics Shanghai Key Laboratory of Materials Protection and Advanced Materials in Electric Power, Shanghai University of Electric Power, Shanghai 200090, China

²State Key Laboratory of Photonics and Communications, School of Physics and Astronomy, Shanghai Jiao Tong University, Shanghai 200240, China



(Received 24 June 2026; accepted 17 August 2026; published 8 September 2026)

Quantum digital signatures (QDSs) utilize shared keys generated by quantum key distribution, thereby providing information-theoretic security. Most existing QDS schemes, however, only support single-signer scenarios, which limits their applications in large-scale quantum networks. Based on previous studies of multisigner QDSs, we design and experimentally demonstrate a scalable multisigner QDS system. The results show that the designed system enables multiple signers to jointly sign the same message while supporting receiver verification and arbitrated validation. The single-photon count rate used in the experiment was approximately 2.6×10^4 counts/s. The measured coincidence-to-accidental ratio (CAR) was greater than 830, and the second-order correlation function $g^{(2)}(0)$ was less than 0.01. The two-photon interference visibility measured for the polarization-entangled state $|\Phi^+\rangle = (|HH\rangle + |VV\rangle)/\sqrt{2}$ was approximately 99.01%, corresponding to a quantum bit error rate below 0.495%. This work demonstrates a reliable implementation of multisigner QDSs and may provide a practical approach to secure authentication and collaborative authorization in future large-scale quantum networks.

DOI: [10.1103/zpv3-tr68](https://doi.org/10.1103/zpv3-tr68)

I. INTRODUCTION

Quantum information technology can achieve security at the information-theoretic level by exploiting the basic laws of quantum mechanics. Quantum communication [1–5], as an important component of quantum information technology, has attracted extensive attention. Among them, quantum key distribution (QKD) [6,7], quantum secret sharing [8,9], and quantum teleportation [10] are regarded as important components of quantum communication. Quantum digital signatures (QDSs) [11], as an important research direction that has emerged in recent years, can not only verify the origin and authenticity of messages but also provide security properties such as unforgeability and nonrepudiation [12]. Therefore, QDSs have broad application prospects in future quantum network scenarios.

Since the concept of QDSs was proposed, extensive research has been carried out on security analysis, protocol design, and experimental implementation. Gottesman and Chuang laid the theoretical foundation of QDSs in 2001 [11]. Subsequently, Clarke *et al.* presented an early experimental realization, demonstrating the feasibility of QDSs in practical optical systems [13]. With the development of related technologies, Collins *et al.* further proposed and

experimentally demonstrated more practical QDS protocols, promoting the development of QDSs toward real-world applications [14–16]. In 2017, Yin *et al.* implemented a QDS experiment over a 102-km optical fiber link, further verifying the application potential of QDSs in long-distance quantum communication [17]. In recent years, researchers have begun to focus on multireceiver QDSs, networked QDSs, and identity authentication in quantum networks, and various related theoretical protocols have been proposed [18,19]. However, current QDS research is mainly focused on signature tasks involving a single signer [20–23]. Existing QDS protocols still have certain limitations in application scenarios that require joint authorization, collaborative decision-making, and cooperative authentication among multiple participants. Although related technologies such as long-distance and multinode QKD, as well as quantum networks without trusted nodes, have made progress [24–27], the implementation of QDS systems for multiuser scenarios remains relatively limited. Moreover, some multiuser QDS studies remain at the theoretical stage, with limited investigation into practical implementation methods and scalability. This has hindered the application of QDSs in large-scale quantum networks to some extent. Table I provides a quantitative comparison of representative QDS protocols reported in recent years. Existing schemes are primarily designed for single-signer scenarios and often face challenges in simultaneously supporting multiple signers while maintaining low resource consumption and experimental feasibility.

In this work, we design and experimentally demonstrate a QDS system for multisigner scenarios based on an existing multisigner QDS scheme [28]. By establishing pairwise

*These authors contributed equally to this work.

†Contact author: lyhua1984@shiep.edu.cn

‡Contact author: jlin@shiep.edu.cn

§Contact author: ylzhang@sjtu.edu.cn

||Contact author: xfchen@sjtu.edu.cn

TABLE I. Quantitative comparison of the designed scheme with representative QDS protocols. $\checkmark$ ($\times$) indicates whether the corresponding feature is supported (unsupported). N denotes the number of signers.

Ref.	Multisigner	Link scaling	Key scaling	Experiment
Clarke <i>et al.</i> [13]	$\times$	$O(N)$	$O(N)$	$\checkmark$
Yin <i>et al.</i> [17]	$\times$	$O(N)$	$O(N)$	$\checkmark$
Weng <i>et al.</i> [18]	$\times$	$O(N^2)$	$O(N^2)$	$\times$
This work	$\checkmark$	$O(N)$	$O(N)$	$\checkmark$

shared keys among the signers, the receiver, and the arbitrator, the designed system enables multiple signers to jointly sign the same message. We further analyze the key resource requirements and scalability of the system and derive the communication link overhead and key overhead as functions of the number of signers. Experimentally, we generate polarization-entangled photon pairs in the telecommunications band based on a periodically poled lithium niobate (PPLN) waveguide-entangled photon source. The performance of the entangled photon source is characterized by the spontaneous parametric down-conversion (SPDC) spectrum, the coincidence-to-accidental ratio (CAR), the second-order correlation function $g^{(2)}(0)$, and the two-photon interference visibility. The measurements indicate that the entangled source exhibits a high photon-pair generation rate, excellent quantum correlation properties, and a low quantum bit error rate (QBER), meeting the requirements of QDS systems for high-quality key generation. On this basis, we further demonstrate a QDS process in which four signers independently generate signatures for the same message, verifying the feasibility of the designed scheme. The designed scheme exhibits good scalability and can be extended to support more users by adding additional nodes in the future, providing technical support for identity authentication in quantum networks. Combined with the demand for highly secure identity authentication in smart grids and new power systems, the designed scheme may also find applications in dispatch instruction authorization, multiagent collaborative control, and device identity authentication.

II. SYSTEM ARCHITECTURE AND COMMUNICATION MODEL

A. System roles and network architecture

We consider a multisigner QDS system consisting of N signers S_i ($i = 1, \dots, N$), a receiver R , and an arbitrator A . The objective of the system is to enable the receiver to verify the authenticity of signed messages from multiple signers in an open communication environment with potential adversaries. In the event of a dispute, the arbitrator performs dispute resolution to ensure the nonrepudiation of signatures and the trustworthiness of the system.

To support collaborative signing by multiple signers, the system establishes shared keys through a pairwise key distribution mechanism. These shared keys enable subsequent functional modules, including signature generation, signature verification, and arbitrated validation. This architecture exhibits good scalability and is compatible with existing fiber-based quantum communication platforms.

The communication model consists of quantum and classical channels. Quantum channels are employed to transmit and measure quantum states, producing correlated data for key extraction or source characterization. Classical channels are used for public discussion, control signaling, and the transmission of signature-related data. We assume that the classical channels may be subject to eavesdropping or tampering by adversaries. Therefore, authentication mechanisms are required to ensure the security of classical communications.

B. Resource allocation for point-to-point key establishment

To support the multisigner signature process, the system establishes shared keys among different entities through a point-to-point key distribution mechanism, as shown in Fig. 1(a). For N signers S_i ($i = 1, \dots, N$), each signer shares a $2n$ -bit key $K_{S,R}$ with the receiver R and an n -bit key $K_{S,A}$ with the arbitrator A . The receiver R and the arbitrator A share an $n(N + 1)$ -bit key K_{RA} . These keys are used to support functional modules including signature generation, receiver verification, signature aggregation, and arbitrated verification. Specifically, $K_{S,R}$ is mainly used for signature encryption, message authentication, and receiver verification. $K_{S,A}$ is used for digest-matrix generation and arbitrated verification by the arbitrator. K_{RA} is used for authentication and masking when the receiver forwards the aggregated signature data to the arbitrator.

Owing to the use of aggregate signatures and consistency verification mechanisms, the overhead of the arbitration stage scales linearly with the number of signers N , resulting in a complexity of $O(N)$. This design enables the arbitrator to determine the validity of signatures, in the event of a dispute, based on independently shared keys established with each signer. As a result, the nonrepudiation of signatures and the robustness of the system are enhanced. It is worth noting that the designed multisigner QDS system performs signature verification and arbitration based on pairwise shared keys held by different participants. System consistency is ensured by the verification architecture itself. This feature enables the system to support collaborative authentication among multiple parties while preserving the pairwise key-sharing model.

We establish a key resource model for the system. As summarized in Table II, the key resource requirements can be explicitly quantified. For a scenario involving N signers, each signer S_i establishes pairwise shared keys $K_{S,R}$ and $K_{S,A}$ with the receiver R and the arbitrator A , respectively. In addition, the receiver and the arbitrator share a key K_{RA} for authentication during the arbitration process. Therefore, the total number of pairwise key links required by the system is given by $N_{\text{link}} = 2N + 1$. This linear scaling relationship

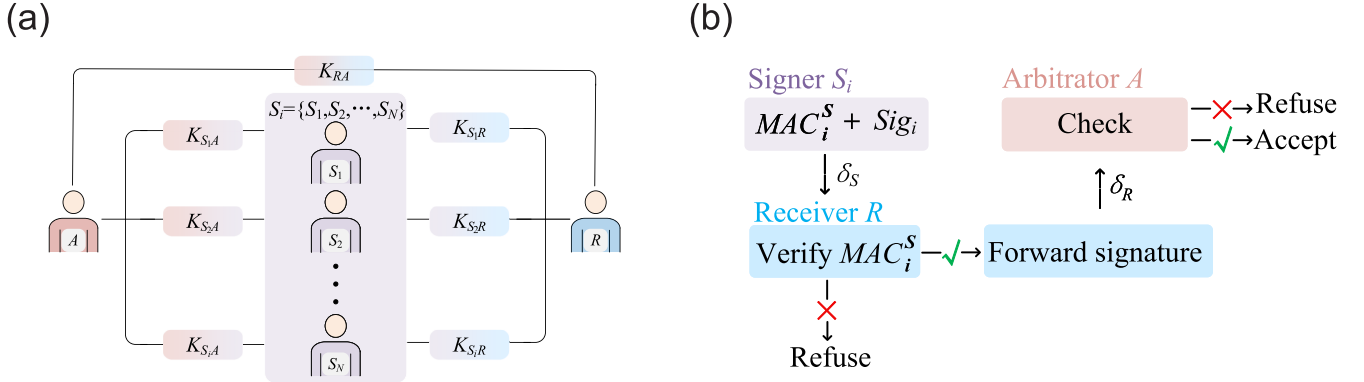


FIG. 1. Shared-key resource allocation and signing workflow of the designed multisigner quantum digital signatures system. (a) Pairwise shared-key distribution among the set of signers S , the receiver R , and the arbitrator A . $K_{S_i R}$, $K_{S_i A}$, and K_{RA} denote the shared keys between the corresponding participants. (b) Signing, verification, and arbitration procedures.

indicates that the key resource overhead grows in a predictable manner as the number of signers increases, providing a basis for evaluating the system scale and throughput. The multisigner capability can be extended by adding signer nodes and establishing the corresponding key links, without requiring structural modifications to the core verification mechanisms of the receiver and the arbitrator.

III. MULTISIGNER QUANTUM DIGITAL SIGNATURE PROCEDURE

In this section, based on the concepts introduced in the multisigner QDS study in Ref. [28] and combined with a pairwise shared-key architecture, we design a multisigner QDS procedure suitable for experimental implementation, as shown in Fig. 1(b). The signing mechanism can be applied to different types of information carriers, including text, images, and video. Let the message to be signed be denoted by Mes . The system consists of a set of signers $S = \{S_1, S_2, \dots, S_N\}$, a receiver R , and an arbitrator A . After establishing pairwise shared keys through QKD, the communication entities use these keys for multisigner signature generation, receiver verification, and arbitrator-assisted validation. For clarity, the multisigner signing task considered in this work is defined as follows. Multiple signers independently generate their signatures for the same message Mes . The receiver verifies the validity of each signature and decides whether to accept it. In

the event of a dispute, the arbitrator performs arbitration based on independently shared key information.

A. Signature generation by signers

During the signature generation stage, each signer independently performs the signing operation. First, signer S_i generates a message authentication code MAC_i^S for the message Mes based on the shared key $K_{S_i R}$ established with the receiver. Specifically, HMAC – SHA256 is employed to construct the message authentication tag, and an n -bit message authentication code is generated [29,30]:

$$MAC_i^S(K_{S_i R}, Mes) = \text{Hash}((K_{S_i R} \oplus T_2) \parallel \text{Hash}((K_{S_i R} \oplus T_1) \parallel Mes)), \quad (1)$$

where T_1 and T_2 denote the inner and outer padding constants used in HMAC – SHA256, respectively. The message authentication code is mainly used to resist active tampering attacks on the classical channel, and its security is based on standard computational security assumptions.

Subsequently, signer S_i uses an n -bit quantum random number R_i to construct the feedback polynomial of the linear feedback shift register [31,32]. Taking $K_{S_i A}$ as the seed, signer S_i generates an $n \times m$ Toeplitz matrix H_i^S and performs a matrix-vector operation over GF(2) to obtain an n -bit message digest [33,34]:

$$\text{Dig}_i = H_i^S \times Mes. \quad (2)$$

Finally, the signer encrypts the digest and the random number with the shared key $K_{S_i R}$ to generate an individual signature:

$$\text{Sig}_i = K_{S_i R} \oplus (\text{Dig}_i \parallel R_i). \quad (3)$$

The signer then packages the message and the corresponding signature data as $\delta_i = (Mes, \text{Sig}_i, MAC_i^S)$, and sends it to the receiver.

In the above process, for the i th signer S_i , the generated signature data consist of three parts: the message authentication tag MAC_i^S based on the shared key, the digest bit string Dig_i generated from the random seed, and the corresponding signature tag Sig_i . For a given key-length parameter n , the length of Dig_i is n bits, and the length of Sig_i is $2n$ bits.

TABLE II. Key resource requirements and scalability of the designed multisigner QDS system. N denotes the number of signers, and n denotes the key length required for a single signing operation. The receiver and arbitrator key overheads scale linearly with N .

Resource item	Exact value
Number of signers	N
Number of pairwise key links	$2N + 1$
Key requirement per signer	$3n$
Key requirement for receiver	$n(3N + 1)$
Key requirement for arbitrator	$n(2N + 1)$

During the verification stage, the receiver and the arbitrator only perform consistency checks and threshold judgments on the structured data described above. They do not need to recover or reconstruct the original keys. This allows the system to maintain low computational and storage complexity when extended to multiple signers.

B. Verification by the receiver

In the receiving stage, the receiver obtains δ_i from N signers. The receiver first computes MAC_i^R using $K_{S_i,R}$ and Mes , and checks whether the following condition is satisfied: $\text{MAC}_i^R = \text{MAC}_i^S$. If this condition holds, the message authentication tag of signer S_i is regarded as valid. If the authentication of any signer fails, the corresponding signature is rejected.

For the authenticated signatures, the receiver decrypts each signature using the shared key $K_{S_i,R}$ and recovers the digest and the random number:

$$\text{Dig}_{R,i} \| R_{R,i} = K_{S_i,R} \oplus \text{Sig}_i. \quad (4)$$

The receiver then aggregates all digests and random numbers as follows:

$$\text{Sig}_R = (\text{Dig}_{R,1} \oplus \cdots \oplus \text{Dig}_{R,N} \| R_{R,1} \| \cdots \| R_{R,N}) \oplus K_{RA}. \quad (5)$$

Finally, the receiver packages the aggregated signature data as $\delta_R = (\text{Mes}, \text{Sig}_R)$, and sends them to the arbitrator A for subsequent arbitration.

From the perspective of verification, the design converts the task of individually verifying the validity of each signature in a multisigner scenario into the verification of consistency relations among multiple signatures. While preserving the pairwise key-sharing model, this approach reduces the verification complexity and communication overhead in the arbitration stage. This design is particularly suitable for scenarios in which the number of signers increases.

C. Arbitration by the arbitrator

To improve the auditability and reliability of the system in dispute scenarios, this work adopts a two-layer verification structure consisting of receiver verification and arbitrated validation. The receiver R first independently verifies the signatures from each signer based on the shared key $K_{S_i,R}$. When further confirmation is required or a dispute occurs, the arbitrator A performs arbitrated consistency verification using the independent key $K_{S_i,A}$ shared with the signer.

The arbitration process is as follows. First, the arbitrator un.masks the aggregated signature sent by the receiver using the shared key K_{RA} :

$$K_{RA} \oplus \text{Sig}_R = \text{Dig}_{A,O} \| R_{R,1} \| R_{R,2} \| \cdots \| R_{R,N}. \quad (6)$$

Then, the arbitrator regenerates the Toeplitz matrix H_i^c using $K_{S_i,A}$ and the corresponding random number $R_{R,i}$. The matrices are applied to Mes over GF(2) to perform the matrix-vector operation:

$$\text{Dig}_{A,T} = (H_1^c \oplus \cdots \oplus H_N^c) \times \text{Mes}. \quad (7)$$

Finally, the arbitrator compares the two digest results: $\text{Dig}_{A,O} = \text{Dig}_{A,T}$. If this condition holds, the arbitrated verification is successful; otherwise, the signature is rejected.

Since receiver verification and arbitrated verification are based on different key views, this structure can reduce the potential risk introduced by a single verification node and provides an auditable decision mechanism for multisigner scenarios. In addition, the signing process is built on the shared-key relationships established among the entities, and its overall security is guaranteed by the underlying key-establishment mechanism.

This work focuses on the architecture and experimental realization of a multisigner QDS system. Therefore, we do not provide a rigorous security proof of the designed scheme. Instead, we discuss its security from the design perspective. First, the designed scheme is secured by keys generated through QKD. According to the no-cloning theorem and the measurement-disturbance principle, an external attacker cannot obtain valid key information without being detected. Second, the designed scheme provides a certain degree of unforgeability. The signature generation process requires both the key shared between the signer and the receiver and the key shared between the signer and the arbitrator. Even if an attacker obtains the public message, it is difficult to construct a valid signature without access to all the required key information. Finally, for an individual signer, the designed scheme provides nonrepudiation. When a dispute occurs between the receiver and the signer, the arbitrator can review the signature result, thereby reducing the possibility that the signer denies having sent the message. In addition, if the message content is modified, the corresponding digest result and authentication tag will also change. Therefore, the receiver can detect message tampering in a timely manner. It should be noted that this work does not yet consider practical issues such as collusion among malicious internal nodes or device imperfections. These issues require further investigation in connection with specific application scenarios. Overall, under the combined action of quantum key distribution, secure digest generation, and the arbitration mechanism, the designed scheme can meet the basic requirements of identity authentication, message integrity, and accountability in multiparty joint signing scenarios.

IV. MULTISIGNER QUANTUM DIGITAL SIGNATURE SYSTEM BASED ON A HIGH-QUALITY ENTANGLED PHOTON SOURCE

In this section, the PPLN ridge-waveguide entangled photon source used in the multisigner QDS system is experimentally characterized (Fig. 2). The pump seed is provided by a continuous-wave laser centered at 1550.65 nm and then amplified with an erbium-doped fiber amplifier (EDFA). The amplified light is filtered to suppress noise. Subsequently, pump light is generated through second-harmonic generation and coupled into a Sagnac interferometer. A PPLN ridge waveguide employing type-0 quasi phase matching is integrated into the interferometer. Polarization-entangled photon pairs are produced via the SPDC process, with the waveguide temperature stabilized at 62.72°C. The generated entangled photon pairs are routed to different users by a

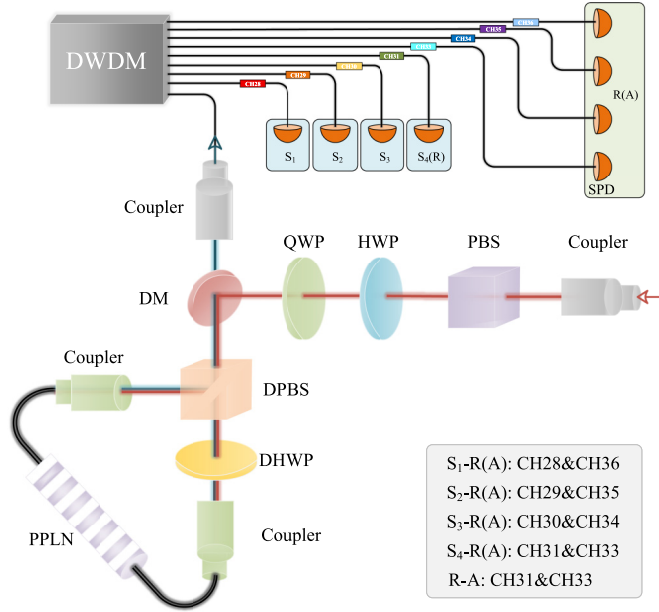


FIG. 2. Experimental setup of the multisigner QDS system based on a PPLN ridge-waveguide entangled photon source. The PPLN ridge waveguide is embedded in a Sagnac interferometer for the generation of polarization-entangled photon pairs. The entangled photon pairs are distributed through DWDM channels to construct pairwise shared keys among the signers, the receiver, and the arbitrator. DM, dichroic mirror; QWP, quarter-wave plate; HWP, half-wave plate; PBS, polarizing beam splitter; DPBS, dual-polarization beam splitter; DHWP, dual half-wave plate; Coupler, fiber coupler; DWDM, dense wavelength division multiplexer; PPLN, periodically poled lithium niobate.

dense wavelength division multiplexer (DWDM) according to the selected channels. Each user is equipped with a polarization analysis module and can choose either the Z or the X basis for polarization analysis. Photons are detected by superconducting nanowire single-photon detectors, whose detection efficiency is approximately 80% and whose dark count rates are 40–110 cps. The fiber attenuation coefficient of the quantum channel is approximately 0.2 dB/km. Finally, a time-to-digital converter (ID900) acquires the photon arrival-time tags, from which the coincidence counts are extracted.

To characterize the spectral coverage provided by the PPLN waveguide, the fitted normalized SPDC conversion efficiency spectrum is shown in Fig. 3(c). The spectrum is obtained by fitting the experimentally measured SPDC conversion efficiency data of the PPLN waveguide. The SPDC process is governed by energy conservation and the quasi-phase-matching condition, and its spectral distribution is mainly determined by the waveguide length and phase mismatch [35–37]. The measured SPDC spectrum is centered in the telecommunication band and covers multiple DWDM channels, indicating that the PPLN waveguide can stably generate high-quality entangled photon pairs. In the experiment, the CH31-CH33 channel pair was selected to measure the photon count rate, the CAR, and the second-order correlation function $g^{(2)}(0)$ under different EDFA power levels. The CAR is defined as $CAR = C_{\text{true}}/C_{\text{acc}}$, where C_{true} and C_{acc} denote the true and accidental coincidence counts,

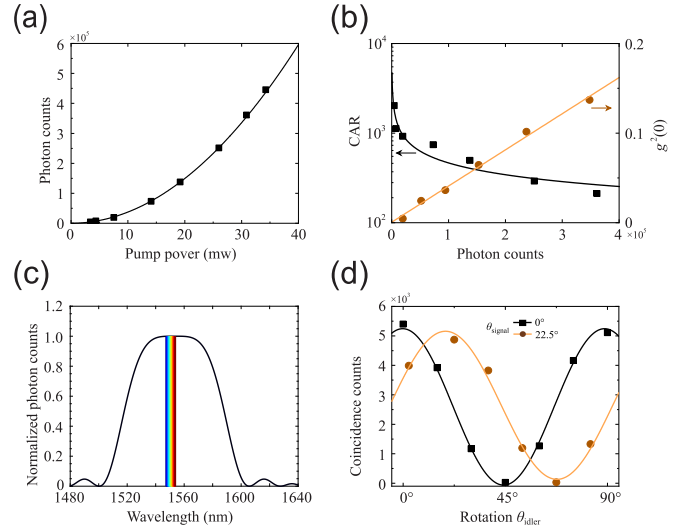


FIG. 3. Experimental characterization of the PPLN ridge-waveguide entangled photon source. (a) Single-photon counting rate vs pump power. (b) CAR and second-order correlation function $g^{(2)}(0)$ as functions of the photon count rate. (c) Experimentally measured normalized SPDC conversion-efficiency spectrum and the fitted curve. The colored region indicates the CH28 to CH36 DWDM channels used in the experiment. (d) Two-photon interference fringes measured in the Z and X basis settings, with interference visibilities of 99.01% and 98.73%, respectively.

respectively. The second-order correlation is calculated as $g^{(2)}(0) = (n_{123}n_1)/(n_{12}n_{13})$, where n_{123} denotes the threefold coincidence counts, n_{12} and n_{13} denote the twofold coincidence counts, and n_1 denotes the single-channel photon counts. The experimental results show that the single-photon count rate increases approximately linearly with increasing pump power, while the multiphoton component is enhanced, resulting in a reduced CAR and an increased $g^{(2)}(0)$, as presented in Fig. 3(b). In addition, as shown in Fig. 3(d), two-photon interference measurements were performed on the CH31-CH33 channel pair to verify the polarization coherence and stability of the entangled photon source. By adjusting the polarization analysis angle and fitting the coincidence counts with a sinusoidal function, a two-photon interference visibility of 99.01% was obtained, corresponding to a link QBER of 0.495%. These results demonstrate the excellent polarization coherence of the PPLN ridge-waveguide entangled photon source. The other experimental channels also exhibited similar coincidence response characteristics, indicating good consistency of the entangled photon source within the selected communication channels. The high CAR, low $g^{(2)}(0)$, high two-photon interference visibility, and low QBER measured for the CH31-CH33 channel pair indicate that the entangled photon source can reliably supply high-quality quantum resources.

In this work, we demonstrate a QDS process involving four signers. According to the requirements of the designed scheme, nine sets of pairwise shared keys are required. In the experimental demonstration, the shared keys between the signers and the receiver, between the signers and the arbitrator, and between the receiver and the arbitrator are all generated

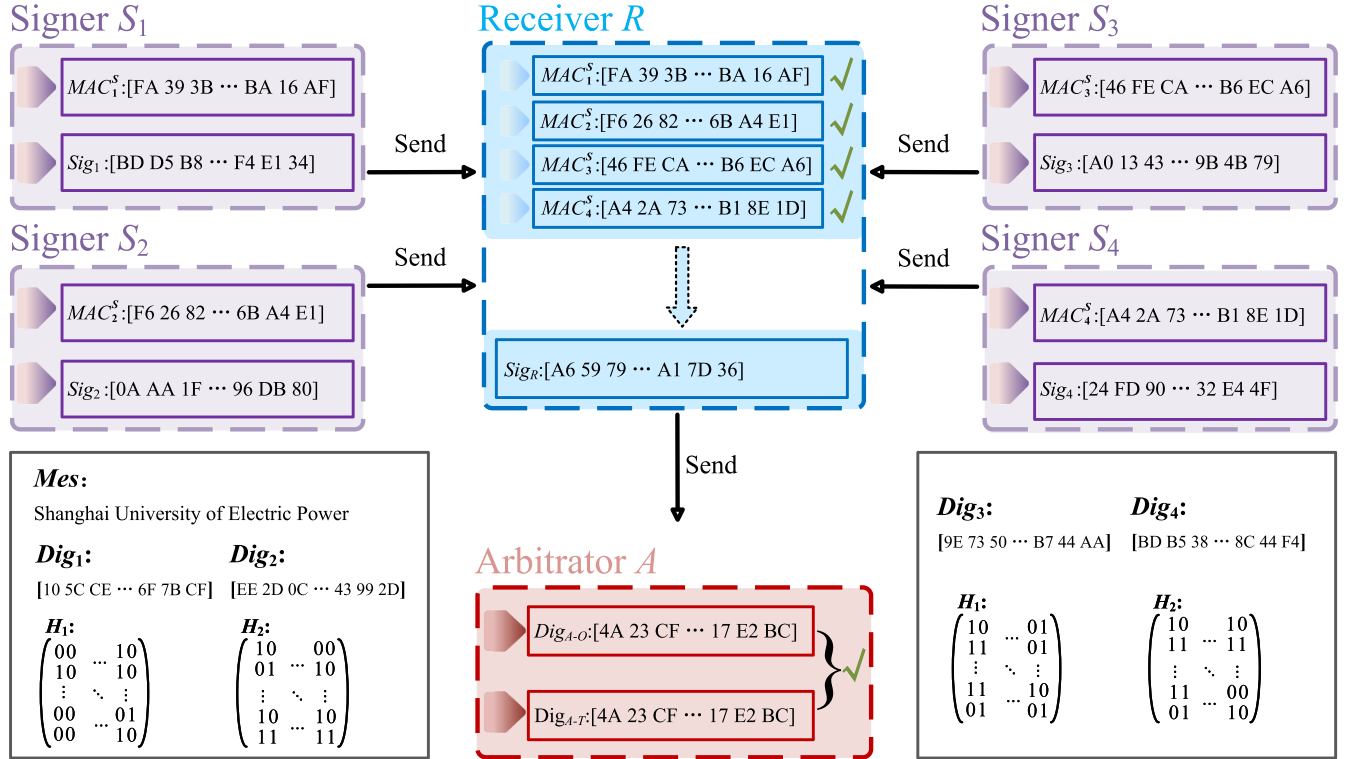


FIG. 4. Experimental demonstration of the multisigner quantum digital signatures process. Four signers independently generate signatures for the same message, “Shanghai University of Electric Power.” The receiver verifies each signature and aggregates the verified signatures, and then sends the aggregated result to the arbitrator for arbitration. In this experiment, $m = 296$ and $n = 256$, with Mes, MAC, Dig, and Sig lengths of 296 bits, 256, 256, and 512 bits, respectively.

by the same entangled photon source. As shown in Fig. 2, quantum keys are extracted from the coincidence-event data obtained from four DWDM channel pairs, namely, CH31-CH33, CH30-CH34, CH29-CH35, and CH28-CH36. These keys are then used to construct the shared keys among the nodes according to the requirements of the designed scheme. All four channel pairs participate in the multi-signer QDS system demonstration. Since these DWDM channels use the same entangled photon source and experimental configuration and exhibit similar coincidence response characteristics, the CH31-CH33 channel pair is selected as a representative channel for detailed characterization of the entangled photon source. The nine sets of shared keys required for the operation of the designed scheme are all generated from experimentally measured coincidence-event data.

V. EXPERIMENTAL DEMONSTRATION OF MULTISIGNER QUANTUM DIGITAL SIGNATURES

Here, we experimentally demonstrate the designed multisigner QDS system, as shown in Fig. 4. In the experiment, four signers, S_1 , S_2 , S_3 and S_4 , independently generate signatures for the same message. After independently verifying the signatures from the four signers, the receiver R aggregates the signatures and sends the aggregated result to the arbitrator A for arbitration. During the demonstration, all key resources are derived from DWDM channel data. The signers, receiver, and arbitrator complete the demonstration based on actually generated point-to-point quantum keys, realizing a closed-loop verification process from quantum key distribution to digital

signatures and demonstrating the capability of extending the system to support more signers.

VI. DISCUSSION

Taking a four-signer scenario as an example, we experimentally verify the designed multisigner QDS system using the keys extracted from the experiment. It should be noted that the designed scheme is not limited to the four-signer scenario. Since the designed scheme adopts a point-to-point quantum key architecture, no additional modifications to the signature process or verification mechanism are required when new signers are added to the system. A new signer only needs to establish the corresponding quantum keys with the receiver and the arbitrator to participate in the joint signing process. Therefore, the extension from four signers to an arbitrary number of signers essentially corresponds to an increase in key distribution resources and does not require additional functional modules or structural changes to the signing and verification procedures. The designed system employs a polarization-entangled photon source based on a PPLN ridge waveguide, which is compatible with existing wavelength-division multiplexing technologies and quantum key distribution networks, providing a hardware foundation for the deployment of the designed scheme in practical quantum communication networks.

The designed multisigner QDS system can be applied to scenarios involving multiparty collaborative authentication and joint authorization. Future work will focus on the experimental validation of larger-scale signer scenarios to further

improve the applicability of the system in practical complex network environments.

VII. CONCLUSION

Based on previous studies of multisigner QDSs, this work implements and experimentally verifies a system for multisigner scenarios. The system enables multiple signers to jointly sign the same message. The obtained results indicate that the designed multisigner QDS system can simultaneously accomplish joint signing, receiver verification, and arbitrated validation, thereby verifying its feasibility and effectiveness. The experimental demonstration in the four-signer scenario further confirms the good scalability of the designed scheme. By adding signer nodes and establishing the corresponding point-to-point quantum links, the designed scheme can be readily scaled to tasks with more signers. Combined with large-scale quantum key distribution networks, the designed scheme may provide a feasible technical solution for applications such as multiuser secure authentication, multiparty authorization, and dispatch

instruction management in smart grids within future quantum networks.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 12574360 and No. 62375164), the Shuguang Program of Shanghai Education Development Foundation, the Shanghai Municipal Education Commission (Grant No. 24SG53), the Shanghai Oriental Talent Plan Youth Project (Grant No. QNKJ2025013), and Guangdong Provincial Quantum Science Strategic Initiative (Grant No. GDZX2403003).

DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

-
- [1] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, *et al.*, Implementation of a 46-node quantum metropolitan area network, *npj Quantum Inf.* **7**, 134 (2021).
 - [2] X.-Y. Cao, B.-H. Li, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Experimental quantum e-commerce, *Sci. Adv.* **10**, eadk3258 (2024).
 - [3] C.-X. Weng, R.-Q. Gao, Y. Bao, B.-H. Li, W.-B. Liu, Y.-M. Xie, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, Beating the fault-tolerance bound and security loopholes for Byzantine agreement with a quantum solution, *Research* **6**, 0272 (2023).
 - [4] D. Pan, G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, The evolution of quantum secure direct communication: On the road to the qinternet, *IEEE Commun. Surv. Tutorials* **26**, 1898 (2024).
 - [5] X.-B. An, H. Zhang, C.-M. Zhang, W. Chen, S. Wang, Z.-Q. Yin, Q. Wang, D.-Y. He, P.-L. Hao, S.-F. Liu, *et al.*, Practical quantum digital signature with a gigahertz BB84 quantum key distribution system, *Opt. Lett.* **44**, 139 (2019).
 - [6] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
 - [7] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* **8**, 595 (2014).
 - [8] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, *Phys. Rev. A* **59**, 1829 (1999).
 - [9] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent multiparty quantum communication, *Phys. Rev. Lett.* **114**, 090501 (2015).
 - [10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).
 - [11] D. Gottesman and I. Chuang, Quantum digital signatures, [arXiv:quant-ph/0105032](https://arxiv.org/abs/quant-ph/0105032).
 - [12] W. Diffie and M. E. Hellman, New directions in cryptography, in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman* (Association for Computing Machinery (ACM), New York, NY, 2022), pp. 365–390.
 - [13] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light, *Nat. Commun.* **3**, 1174 (2012).
 - [14] V. Dunjko, P. Wallden, and E. Andersson, Quantum digital signatures without quantum memory, *Phys. Rev. Lett.* **112**, 040502 (2014).
 - [15] C.-H. Zhang, X.-Y. Zhou, H.-J. Ding, C.-M. Zhang, G.-C. Guo, and Q. Wang, Proof-of-principle demonstration of passive decoy-state quantum digital signatures over 200 km, *Phys. Rev. Appl.* **10**, 034033 (2018).
 - [16] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, Measurement-device-independent quantum digital signatures, *Phys. Rev. A* **94**, 022328 (2016).
 - [17] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, *et al.*, Experimental quantum digital signature over 102 km, *Phys. Rev. A* **95**, 032334 (2017).
 - [18] C.-X. Weng, Y.-S. Lu, R.-Q. Gao, Y.-M. Xie, J. Gu, C.-L. Li, B.-H. Li, H.-L. Yin, and Z.-B. Chen, Secure and practical multiparty quantum digital signatures, *Opt. Express* **29**, 27661 (2021).
 - [19] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, Experimental quantum secure network with digital signatures and encryption, *Natl. Sci. Rev.* **10**, nwac228 (2023).
 - [20] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty,

- I. V. Puthoor, and E. Andersson, Experimental measurement-device-independent quantum digital signatures, *Nat. Commun.* **8**, 1098 (2017).
- [21] H.-J. Ding, J.-J. Chen, L. Ji, X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, 280-km experimental demonstration of a quantum digital signature with one decoy state, *Opt. Lett.* **45**, 1711 (2020).
- [22] J. C. Chapman, M. Alshowkan, B. Qi, and N. A. Peters, Entanglement-based quantum digital signatures over a deployed campus network, *Opt. Express* **32**, 7521 (2024).
- [23] Y. Du, B.-H. Li, X. Hua, X.-Y. Cao, Z. Zhao, F. Xie, Z. Zhang, H.-L. Yin, X. Xiao, and K. Wei, Chip-integrated quantum signature network over 200 km, *Light Sci. Appl.* **14**, 108 (2025).
- [24] Y.-H. Li, S.-L. Li, X.-L. Hu, C. Jiang, Z.-W. Yu, W. Li, W.-Y. Liu, S.-K. Liao, J.-G. Ren, H. Li, *et al.*, Free-space and fiber-integrated measurement-device-independent quantum key distribution under high background noise, *Phys. Rev. Lett.* **131**, 100802 (2023).
- [25] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, *et al.*, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [26] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, *et al.*, Experimental twin-field quantum key distribution over 1000 km fiber distance, *Phys. Rev. Lett.* **130**, 210801 (2023).
- [27] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, *et al.*, Robust and adaptable quantum key distribution network without trusted nodes, *Optica* **9**, 812 (2022).
- [28] S. Xiong, Research on key technologies of multiparty secure quantum digital signatures, Ph.D. thesis, Sichuan Normal University, Chengdu, China, 2025.
- [29] H. Yu, Y. Hao, and D. Bai, Evaluate the security margins of SHA-512, SHA-256 and DHA-256 against the boomerang attack, *Sci. China Inf. Sci.* **59**, 052110 (2016).
- [30] H. Krawczyk, M. Bellare, and R. Canetti, HMAC: Keyed-hashing for message authentication, Technical Report No. RFC 2104 (Internet Engineering Task Force (IETF), 1997).
- [31] M. Goresky and A. Klapper, *Algebraic Shift Register Sequences* (Cambridge University Press, Cambridge, UK, 2012).
- [32] S. W. Golomb, *Shift Register Sequences*, revised ed. (Aegean Park Press, Laguna Hills, California, 1982).
- [33] J. L. Carter and M. N. Wegman, Universal classes of hash functions, in *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery (ACM), New York, NY, 1977), pp. 106–112.
- [34] M. Hayashi and T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, *IEEE Trans. Inf. Theory* **62**, 2213 (2016).
- [35] R. W. Boyd, A. L. Gaeta, and E. Giese, Nonlinear optics, in *Springer Handbook of Atomic, Molecular, and Optical Physics*, edited by G. Drake (Springer, New York, 2008), pp. 1097–1110.
- [36] D. H. Jundt, Temperature-dependent Sellmeier equation for the index of refraction, n_e , in congruent lithium niobate, *Opt. Lett.* **22**, 1553 (1997).
- [37] O. Gayer, Z. Sacks, E. Galun, and A. Arie, Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric LiNbO₃, *Appl. Phys. B* **91**, 343 (2008).