PHOTONICS Research

Experimental demonstration of complete quantum e-commerce based on an efficient quantum digital payment

Shuaishuai Liu,[1,2] Yu Zhang,[1,2] Shaobo Ren,[1,2] Si Qiu,[1,2] Zhenguo Lu,[1,2] Xuyang Wang,[1,2,3] and Yongmin Li[1,2,3,*]

[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
[2]Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China
[3]Hefei National Laboratory, Hefei 230088, China
*Corresponding author: yongmin@sxu.edu.cn

Received 21 August 2024; revised 24 November 2024; accepted 5 December 2024; posted 6 December 2024 (Doc. ID 540123); published 18 February 2025

With the rapid spread of Internet technology, e-commerce is gradually becoming an integral part of the modern business models. The e-commerce transactions should obey integrity, authentication, nonrepudiation, traceability, and impartiality. Here, we propose and demonstrate a complete continuous-variable quantum e-commerce scheme, which involves subscription, payment, transport, and reception protocols among five parties. To this end, a simple, efficient quantum digital payment scheme is proposed. Furthermore, we streamline the entire e-commerce process by eliminating the private amplification step in the pre-distribution of keys. We achieve a contract signing rate of 1.51×10^3 times per second for a 33 kilobits contract, and a payment rate of 2.70×10^3 times per second over 80 km of single-mode fiber. Our results can support 411 times complete transactions per second, including three contract signings and two separate monetary payments. The proposed scheme takes into account the compatibility with existing e-commerce platforms to ensure a smooth transition and provides a practical solution for quantum e-commerce at metropolitan distances.

https://doi.org/10.1364/PRJ.540123

1. INTRODUCTION

The rapid development of quantum computing heralds a potential impact on the existing encryption systems [1–3]. Classic e-commerce usually uses security mechanisms such as public key cryptographic algorithms, digital signatures, and authentication for secure transactions [4–6]. Such protocols may be vulnerable to the powerful computational capabilities of quantum computing. In the face of the challenges posed by quantum computing, quantum key distribution (QKD) shows its unique advantages [7–12]. Its information-theoretic security (i.t.-security) is guaranteed by the theorems of quantum mechanics. It enables secure distribution of keys without limiting the ability of the adversary, and when combined with a one-time pad, can ensure secure transmission of private information. QKD is one of the most mature quantum technologies available and its proof-of-principle demonstration has been achieved at the thousand-kilometer level in both free space and fiber-optic links [13–15].

In modern society, e-commerce is indispensable for a merchant and client. A complete e-commerce covers business information flow, financial flow, and logistics, which require collaboration among banks (trusted), trading platforms (trusted third parties), merchants, clients, and logistics companies (LCs) to complete the transaction of goods. During e-commerce transaction, security that mainly consists of authentication, nonrepudiation, and traceability is critical. QKD itself is an effective approach for secure key distribution; however, it can only guarantee the confidentiality of messages and cannot directly perform other cryptographic tasks required by e-commerce.

Quantum digital signatures (QDSs), as an important primitive in cryptography, provide effective solutions for five cryptographic tasks (integrity, authentication, nonrepudiation, traceability, and impartiality) in e-commerce. Since the first proposal of QDS [16], it has seen great progress in the past two decades. The initial requirements of secure quantum channels [17–21] and quantum memory [22–24] that are difficult to operate have been removed. A number of theoretical [25–30] and experimental [31–38] studies have been carried out, among which the QDS based on one-time universal hashing (OTUH) improves the contract signing rate by 10^8 orders of magnitude [38]. Recently, quantum e-commerce that can provide i.t.-security was proposed [39]. The original scheme mainly focuses on the issue of subscription protocols between merchants, clients,

and third-party platforms, while the protocols on payment, logistics, and reception of goods that are essential parts of the quantum e-commerce are lacking.

A banknote, with its advantages of being difficult to reproduce and portable, has replaced traditional physical money such as copper, silver, and gold as an efficient proof of transaction. Although banknotes are relatively difficult to forge, they are not completely impossible to forge. It is in this context that the concept of "quantum money" was introduced [40], whose unforgeable properties are guaranteed by the no-cloning theorem of quantum mechanics, which has stimulated extensive interests [41–48], especially in the prevention of counterfeiting [41–43]. The anti-counterfeiting features of quantum money bode well for their potential to replace traditional banknotes as a new type of currency in the future. However, banks need to pre-prepare and store quantum money with a trusted verifier [41] or the holder's credit card [43], waiting for the holder to redeem it for payment or waiting to spend it. Quantum storage is a major challenge limiting the quantum money to be stored for long periods of time awaiting payment [49]. With the popularity of smartphones and the Internet, digital payments are showing a tendency to replace monetary payments. The appealing and original quantum digital payment (QDP) scheme, which uses a combination of QKD and quantum payment token preparation, transmission, and measurement effectively solves the security problem of digital payments [50]. However, banks and clients need to wait to prepare or measure quantum payment tokens at any time. Furthermore, the quantum tokens should consume around 10^6 quantum states in order to achieve an honest success probability close to one and a negligible dishonest success probability. A QDP solution that is both efficient and simple is desired.

Here, we propose a complete quantum e-commerce scheme based on a simple and efficient QDP method. Our QDP scheme, with only one QKD link and bank verifying the signature, can achieve secure and efficient digital payments at any time and from any location. This solution eliminates the reliance on quantum memory in the traditional quantum money payment process and removes the need to wait for the preparation and measurement of quantum payment tokens. By employing a continuous-variable QKD (CV-QKD) system that eliminates the private amplification step, and two programmable optical switches, the complete quantum e-commerce transaction involving five parties is implemented. It achieves 411 times per second complete transactions in a trading network connected by five 80 km single-mode fibers, including the signing of three contracts and two independent currency payments. The involved CV-QKD has good compatibility with the coherent optical communication components and technology. The presented scheme paves the way for the practical application of quantum e-commerce and QDP.

2. QUANTUM E-COMMERCE AND QUANTUM-DIGITAL PAYMENTS

In quantum e-commerce, trusted third-party trading platforms (TTP-TPs) play a crucial role in the transaction process, such as the Amazon trading platform [51] and Taobao trading platform [52]. The merchants employ the TTP-TP to display and sell their goods. The clients browse and shop for their favorite items on them. During the transaction process, the bank serves as a trusted party to guarantee the security of payment for goods. The LC takes on the responsibility of transporting goods to ensure they reach the clients safely and on time. Ensuring the security of each step in the transaction process is the cornerstone of maintaining the security of the quantum e-commerce. The TTP-TP not only ensures the validity of the transaction between the merchant, the client, and the LC, but also provides nonrepudiation evidence to resolve any disputes that may arise among the three parties, i.e., traceability. For example, if clients find that the parameters or performances of the goods they receive do not match the description in the contract, they are entitled to request the merchant to provide a return or exchange service. The TTP-TP will monitor and guarantee the transaction items based on the appropriate evidences it obtains during the execution of the protocol.

The implementation process of the complete quantum e-commerce can be divided into six steps as shown in Fig. 1. Step 1: pre-distribution of keys; Step 2: the TTP-TP signs a subscription protocol with the merchant and the client; Step 3: the client pays the TTP-TP; Step 4: the TTP-TP signs a transport protocol with the merchant and the LC; Step 5: the TTP-TP signs a reception protocol with the LC and the client; Step 6: the TTP-TP deducts the commission as agreed and pays the remaining payment to the merchant. The specific procedure for each step is as follows.

(i) Pre-distribution of keys.

We use the quadrature phase shift keying (QPSK) discrete-modulation CV-QKD system to distribute the key. The TTP-TP and the bank exploit the uniformly distributed binary quantum random number generator (QRNG) to generate two sets of modulation signals. The generated modulation

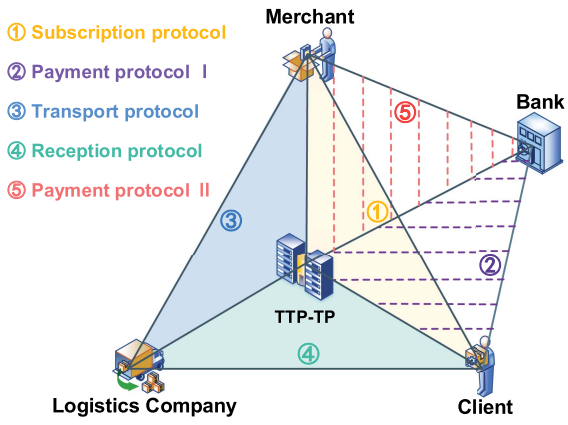

Fig. 1. Schematic diagram of the quantum e-commerce. TTP-TP acts as a bridge among the merchant, the client, the LC, and the bank, with pre-distributed keys among all parties. It is necessary to pre-distribute keys among the bank and the client in order to safeguard the security of the payment. Firstly, the merchant and the client sign a subscription protocol. Next, the client and TTP-TP execute the payment protocol I. The merchant and the LC sign a transport protocol, and the goods are delivered to the clients. Finally, the LC and the client sign a reception protocol, and the TTP-TP takes a commission and executes payment protocol II.

signals are used to drive the in-phase quadrature (IQ) modulator that is operated in carrier suppressed single-sideband (CS-SSB) mode. The prepared sidemode coherent state can be represented as $|\alpha_k\rangle = |\alpha \exp(ik\pi/2)\rangle, k \in \{0,1,2,3\}$. The modulation variance of the quantum signal is $V_M = 2\alpha^2$ [normalized to the shot noise units (SNUs)]. The TTP-TP employs a 1×4 programmable optical switch to route the quantum signals to different quantum channels in a time-division manner and distributes the keys to the merchant, client, LC, and bank, respectively. The bank sends the quantum signals directly to the client through an insecure quantum channel. For the receiving end, the client differs from the other participants in that it uses an additional 1×2 programmable optical switch to alternately receive the quantum signals from the TTP-TP and the bank. After receiving the quantum signals, the receivers independently perform heterodyne detection to extract the information in pilot tones for frequency and phase recovery. Based on this information, the raw keys are distilled. Subsequently, the TTP-TP performs a secure key rate estimation process and data reconciliation with all receivers except the bank (the private amplification step is removed here). Notice that the standard QPSK CV-QKD procedure including secure key rate estimation, data reconciliation, and private amplification is still performed between the bank and the client or TTP-TP.

The process of the key pre-distribution involves five CV-QKD links. The links between the bank & client, and the TTP-TP & bank are intended for the execution of payment protocol I and payment protocol II, respectively. The links between the TTP-TP & merchant, the TTP-TP & client, and the TTP-TP & LC are used for the execution of the subscription, transport, and reception protocols. This design ensures that every step of the quantum e-commerce transaction is encrypted and verified with i.t.-security.

(ii) Subscription protocol.

a. Merchant signature. In Fig. 2(a), the merchant uses the local QRNG to generate a random irreducible polynomial $p(x)$. The merchant and TTP-TP extract a $3n$-bit raw key string K_X^{S}, and use n-bit of it $K_{X_1}^{\mathrm{S}}$ to acquire a random initial column vector s. The n-bit irreducible polynomial's coefficients p_a and the initial vector construct a random linear feedback shift register (LFSR)-based Toeplitz matrix H_{nm}, where n and m are the numbers of rows and columns [53] (see further details in Appendix A). The merchant uses the matrix H_{nm} to perform a hash operation on the subscription contract to obtain the hash value $\mathrm{Hash}^{\mathrm{S}} = H_{nm} \times W$, where W is the subscription contract, which includes the contract number, the basic information of both parties, merchant and client, the details of the goods, the liability for breach of contract, and other relevant information. The length of the subscription contract is m. The merchant constructs the $2n$-bit digest $\mathrm{Dig}^{\mathrm{S}} = (\mathrm{Hash}^{\mathrm{S}} || p_a)$ by concatenating the hash value and the coefficients of irreducible polynomial [38]. The signature is generated by encrypting the digest $S^{\mathrm{S}} = \mathrm{Dig}^{\mathrm{S}} \oplus K_{X_{2,3}}^{\mathrm{S}}$ with a $2n$-bit key $K_{X_{2,3}}^{\mathrm{S}}$. Subsequently, the merchant sends the contract and the signature $\{W, S^{\mathrm{S}}\}$ to the client over an authenticated classical channel.

b. The client verifies the signature. Once the client receives the contract and signature, the information on the contract is checked. If the client does not agree with the content of the contract, the round of subscription is cancelled. Otherwise, they send the contract and signature to the TTP-TP through the authenticated classical channel. When TTP-TP receives the contract, it publishes the key $K_Z^{\mathrm{S}} = K_X^{\mathrm{S}} \oplus K_Y^{\mathrm{S}}$, where K_Y^{S} is the key distributed between the TTP-TP and the client. The client recovers the $3n$-bit key string K_X^{S}, an expected digest, and irreducible polynomial's coefficients by the XOR operation $K_X^{\mathrm{S}} = K_Y^{\mathrm{S}} \oplus K_Z^{\mathrm{S}}$, $\mathrm{Dig}^{\mathrm{S}} = S^{\mathrm{S}} \oplus K_{X_{2,3}}^{\mathrm{S}}$, and then performs the same steps as the merchant signature to verify the consistency of the signature. If the validation passes, they inform TTP-TP of their result; otherwise they declare the round of subscription null and void.

c. The TTP-TP verifies the signature. Once the TTP-TP receives the client's validation result, they verify the consistency of the signature with the $3n$-bit key K_X^{S}. This process is implemented in the same way as the client's validation. If the verification passes, the subscription protocol takes effect. Subsequently, the client pays the TTP-TP to execute the payment protocol I.

(iii) Payment protocol I.

During the payment process, the client must prevent malicious parties from attacking their bankroll, including the TTP-TP, which may illegally use the payment information provided by the client. To this end, we propose an efficient and simple QDP scheme that requires just one QKD link between the bank and the client and only the bank needs to verify the signature, as shown in Fig. 2(b). The detailed procedures are as follows.

a. The bank creates accounts and provides tokens. A secure e-account is a prerequisite for the client to make digital payments; the client applies for a credit card with the bank through an authenticated classic channel and gets a unique identifier (ID) C_{ID}. The bank generates the cardholder token C and encrypts it using the d-bit secure key string $K_{Y_C}^{\mathrm{P}}$, and then sends it to the client over an authenticated classical channel. Whenever a client initiates a payment request, the bank uses the h-bit secure key string $K_{Y_P}^{\mathrm{P}}$ to encrypt a generated one-time payment token P, and then sends the encrypted token to the client.

b. Client signature. The client signs the file W_{P} consisting of the cardholder token C, the payment token P, the TTP-TP's ID T_{ID}, and the payment amount M with the $3g$-bit secure key K_Y^{P} to get the signature S_C^{P}. Then, they sends their ID and signature $\{C_{\mathrm{ID}}, S_C^{\mathrm{P}}\}$ to the TTP-TP. Next, the TTP-TP combines their own ID, the payment amount, and the information sent by the client $\{T_{\mathrm{ID}}, M, C_{\mathrm{ID}}, S_C^{\mathrm{P}}\}$ to the bank.

c. The bank verifies the signature. Based on the information provided by TTP-TP, the bank locates cardholder token C and payment token P based on the client's C_{ID}, and verifies the signature with $\{T_{\mathrm{ID}}, M\}$. If the signature is verified correctly, the bank confirms the payment; otherwise it refuses the payment.

(iv) Transport protocol.

Once the TTP-TP receives the required payment, they will notify the merchant to ship the goods. The LC signs a transport protocol with the merchant and sends the signature and contract to the merchant. The merchant verifies the contract and sends the signature of the LC and the contract to TTP-TP. The TTP-TP publishes the XOR key after it receives the relevant information. The merchant then verifies the signature. Subsequently, the TTP-TP performs the same signature

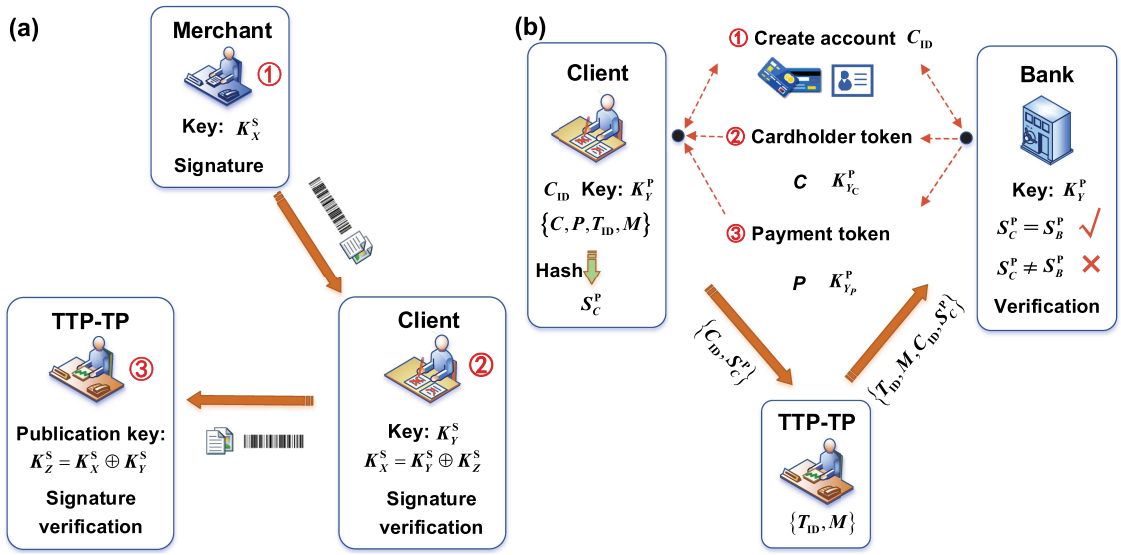

Fig. 2. Schematic diagrams of the subscription and payment protocols. (a) Subscription protocol. Firstly, the merchant drafts and signs the contract, and then sends the signature and the contract to the client. The client approves the contract and sends the merchant's signature and contract to the TTP-TP. The TTP-TP publishes the key $K_Z^S = K_X^S \oplus K_Y^S$. The client then verifies the signature. Once the validation of the signature is confirmed, the TTP-TP then performs another validation to ensure the legitimacy of the signature and the integrity of the contract. If the TTP-TP's signature validation passes, the sign of the subscription protocol is complete. (b) Payment protocol I. The client creates an account at the bank and receives an identifier (ID) C_{ID}. The bank generates a cardholder token C based on each client's ID. By using the d-bit secure key $K_{Y_C}^P$, the bank encrypts the cardholder token C and sends it to the client. The bank generates a one-time payment token P and encrypts it using the h-bit secure key $K_{Y_P}^P$, and then sends the encrypted token to the client. The client then signs the file W_P consisting of the cardholder token C, the payment token P, the TTP-TP's ID T_{ID}, and the payment amount M, and sends $\{C_{ID}, S_C^P\}$ to the TTP-TP. The TTP-TP combines the received information with their own private T_{ID} and the payment amount M, and forwards them to the bank. The bank verifies the signature and completes the payment.

verification operation and makes a decision based on signature consistency.

(v) Reception protocol.

After the client receives the goods, the client signs a reception protocol with the LC to provide the official proof of reception and confirms that the delivery arrives without missing items or damaged goods, or later than the target date. The signing procedure of the reception protocol is similar to that of the subscription contract, requiring the signature of the client, verified by the LC and TTP-TP.

(vi) Payment protocol II.

If the above signature is validated, the TTP-TP takes the appropriate commission and pays the remaining balance to the merchant. The details of the payment are similar to payment protocol I.

3. SECURITY ANALYSIS

The three protocols signed in the quantum e-commerce scheme constitute a basis for clarifying the responsibilities of all parties during each transaction stage. This means that any falsification of goods, false denials of dispatch, and reception by the merchants, LC, and clients can be discovered. During the contract signing process, any party involved may be malicious. The remaining honest participants can collaborate with the TTP-TP to defeat the potential attack that the malicious party may initiate. Additionally, during the payment process, we must be alert to the possible fraudulent behavior by payees, while not ignoring the potential eavesdroppers who may attempt to intercept the payment information. In this section, we take the subscription protocol as an example (the security of the three contract signing protocols is equivalent), analyze the repudiation and forgery attacks that a malicious eavesdropper might implement, and analyze the robustness of the protocol when all participants are honest. We also consider potential threats that could be implemented by the payees or eavesdroppers during the payment, including modification of the payment amount, double spending, and modification of the receiving account, and consider the robustness of the payment protocol. Furthermore, we investigate the contract signing rate, the payment rate, and the transaction rate of quantum e-commerce.

A. Repudiation

In the case of a subscription protocol, if the merchant attempts to repudiate the transaction through a repudiation attack, even if the signature fails to pass the rigorous validation of the TTP-TP, we consider the merchant to have successfully executed a repudiation strategy for that transaction as long as it is acknowledged by the client. Both the client and TTP-TP are treated as trustworthy against possible repudiation attacks by the merchant. The client relies on the information disclosed by the TTP-TP, K_Z^S, in conjunction with their own key, K_Y^S, to derive the $3n$-bit key $K_X^S = K_Y^S \oplus K_Z^S$ and then verify the signature. The TTP-TP uses the $3n$-bit key string, K_X^S, which is distributed directly with the merchant, to verify the signature. The TTP-TP and client use exactly the same key bits to verify the signature and therefore make consistent decisions. The repudiation attack only succeeds if the client sends the

contract and signature to the TTP-TP in error. The bounds for successful repudiation are $\xi^{S}_{rep} = \xi_C$. We assume the failure probability of information transmission over the classical channel is $\xi_C = 10^{-11}$.

For the payment protocols, it makes no sense to deny the payment operation. The only meaningful attack the payers can perform is to change the payment amount M. Once the bank verifies the consistency of the signatures, it will make the payment based on the amount provided by the payee, rendering this attack ineffective.

B. Forgery

For a forgery attack of the subscription protocol, the client attempts to forge a contract and signature and cheats the TTP-TP to accept it. The TTP-TP will not release any information about the key K^{S}_{Z} until they receive the contract document and the merchant's signature sent by the client. The client cannot obtain the key bits K^{S}_{X} used for the merchant's signature until the contract and signature are sent. Moreover, the client will not get any information from the signature of the previous round because the LFSR-based Toeplitz matrix and the encryption key are refreshed in each round. The only thing the client can do is to guess the merchant's key or the irreducible polynomial $p(x)$ that forms the LFSR-based Toeplitz matrix. (Our protocol has no private amplification step. Any attacker may get partial information about the key.) Next, we quantify the leakage and give bounds on the maximum probability that the client guesses the n-bit key [30]. We consider the collective attack in the asymptotic case, where the client performs independent interactions on the merchant's quantum state to obtain a system $\rho^{x}_{\mathbb{C}}$, and performs the positive operator-valued measure (POVM) $\{E^{x}_{\mathbb{C}}\}_{x}$ on it. The probability that the client guesses the right n-bit key $\mathbb{Q}$ can be given by [54]

$$P_{\text{guess}}(\mathbb{Q}|\mathbb{C}) = \max_{\{E^{x}_{\mathbb{C}}\}_{x}} \Sigma_x P_x \text{tr}(E^{x}_{\mathbb{C}}\rho^{x}_{\mathbb{C}}) = 2^{-H_{\min}(\mathbb{Q}|\mathbb{C})_{\rho}}, \quad (1)$$

where $\mathbb{C}$ is the client's attack system; $H_{\min}(\mathbb{Q}|\mathbb{C})_{\rho}$ is the minimum entropy. The n-bit key string $\mathbb{Q}$ is generated in the pre-distribution phase; then $H_{\min}(\mathbb{Q}|\mathbb{C})_{\rho}$ can be evaluated, and the above equation can be rewritten as

$$P_{\text{guess}}(\mathbb{Q}|\mathbb{C}) = 2^{-\mathfrak{R}_n}. \quad (2)$$

This means that the maximum probability that the client guesses the n-bit key string correctly is $2^{-\mathfrak{R}_n}$, where $\mathfrak{R}_n$ is the unknown information in the n-bit key string $\mathbb{Q}$. According to the key rate calculation formula in the asymptotic case, it is given by [55,56]

$$\mathfrak{R}_n = nk^{\infty}, \quad (3)$$

$$K^{\infty} = \min_{\rho_{AB}\in S} D(\mathcal{G}(\rho_{AB})\|\mathcal{Z}[\mathcal{G}(\rho_{AB})]) - p_{\text{pass}}\delta_{\text{EC}}, \quad (4)$$

where $D(\rho\|\sigma) = \text{Tr}(\rho\log_2\rho) - \text{Tr}(\rho\log_2\sigma)$ is the quantum relative entropy; $\mathcal{G}$ represents a map that is positive and trace non-increasing for post-processing processes. ρ_{AB} denotes the joint state of the transmitter and the receiver after the quantum state of the transmitter has been transmitted through an insecure quantum channel. The set S contains all density operators that are compatible with the experimental observations. $\mathcal{Z}$ denotes a pinching quantum channel for achieving key mapping results. p_{pass} is the probability of sifting a raw key. δ_{EC} is the leakage information during error correction. Based on the probability that the client guesses the n-bit key string $\mathbb{Q}$ correctly, we can quantify the upper bound of the probability that the client guesses the irreducible polynomial and forges a message for the TTP-TP as [30]

$$\xi_{\text{for}} = m \cdot 2^{1-\mathfrak{R}_n}. \quad (5)$$

Equation (5) gives the optimal attack strategy for the client (see Appendix B for the details).

There are two type of forgery attacks against the payment protocols.

Forgery attack type I: the payee fabricates a fictitious payment amount and forges the payer's signature, with the intention of collecting payments that exceed the agreed amount between the parties. Further, the malicious eavesdroppers may attempt to forge payee account IDs and payer signatures to obtain illicit funds. These attack strategies are similar to the client forgery attack against the subscription protocol. In the subscription protocol, the client can obtain the contract and signature information provided by the merchant. In contrast, the payee and malicious eavesdroppers can only acquire the signature of the payer and partial information related to the file W_{P} in the payment protocol. The attack capabilities of the payee and malicious eavesdroppers are relatively limited, and the security bound of the subscription protocol remains applicable. Thus, the security bounds for such an attack are given by

$$\xi_p = m' \cdot 2^{1-g}, \quad (6)$$

where m' is the length of the file W_{P}.

Forgery attack type II: the malicious party may attempt to implement double spending using the signature. Notice that this is virtually impossible because the payer's cardholder token and the payment token are not publicly available, and the payment token and signature bit are refreshed every round. In this case, getting all guesses exactly right is an almost impossible event, rendering this attack negligible.

C. Robustness

Given that all participants are trustworthy, the subscription protocols may still face the possibility of unexpected failure under certain conditions, that is, the error correction process in the pre-distribution of keys, and the use of classical authentication channels to send and disclose information. Although the failure probability of these two cases is very small, it still needs to be taken into account. During the pre-distribution of keys, the TTP-TP and the merchant (or the client) perform the error correction to obtain a final identical key, with a failure probability not exceeding ξ_{EC}. Furthermore, the failure probability that they send key K^{S}_{Z}, or contracts and signatures over a classical authentication channel does not exceed ξ_C. If any of the above aspects fails, it will result in the failure of the contract signing. Therefore, the bound of terminating the protocol when all participants are honest is $\xi^{S}_{\text{rob}} = 2\xi_{\text{EC}} + 3\xi_C$. In experiment, we assume the failure probability of the error correction $\xi_{\text{EC}} = 10^{-11}$.

The robustness of the payment protocol is similar to that of the subscription protocol. The payment protocol includes one QKD link and four classical channel links. Thus, the bound of the robustness is $\xi^{P}_{\text{rob}} = \xi_{\text{EC}} + 4\xi_C$.

There is no more than one malicious party in each round of the subscription protocol, i.e., at most one of the two attacks can occur. We can write the maximum probability that the transaction will fail and the security bound is given by

$$\xi_{\text{tot}} = 3m \cdot 2^{1-\mathfrak{R}_n} + 2m' \cdot 2^{1-g}. \tag{7}$$

D. Rate

For a single protocol, the optical switch will switch between two participants (merchant & client, or merchant & LC, or LC & client). The signing rates for the subscription protocol, the transport protocol, and the reception protocol are given by

$$R_{s_y} = \frac{Ru}{2(3n_y)}, \tag{8}$$

$$u = (1 - a)(1 - \text{FER}), \tag{9}$$

where R is the repetition rate of the system, $3n_y, y \in \{1,2,3\}$ is the consumed key bits for signing the subscription protocol, the transport protocol, and the reception protocol, respectively, a is the ratio of the raw data consumed by the parameter estimation, and FER is the frame error rate during the error correction process. In the experiment, we have set the security bound $\xi_{\text{for}} = 2 \times 10^{-10}$ for each protocol. According to Eq. (5), we can determine the amount of unknown key $\mathfrak{R}_n$ consumed during the signing process. From Eqs. (3) and (4), the n_y-bit key consumption for each signing can be determined. The factor 2 arises from the switching of the optical switch between two participants.

The QDP rate is given by

$$R_{p_j} = \frac{Ruk^{\infty}}{3g_j + h}, \tag{10}$$

where $R_{p_j}, j \in \{\text{I}, \text{II}\}$ are the payment rates for payment protocol I and payment protocol II, respectively. In Eq. (10), we do not take into account the d-bit key consumed by the encrypted cardholder C, as it is used only once. The QDP utilizes secure keys to encrypt one-time payment tokens P and sign the file W_{P}; thus in each QDP process, we only need to consider the consumption of secure keys.

Considering the time multiplexing due to the optical switches and the serial operation of the subscription protocol, the payment protocol II, the transport protocol, and the reception protocol, the transaction rate of the quantum e-commerce is given by

$$R_{\text{e}} = \frac{1}{\frac{1}{R_{p_{\text{II}}}} + \frac{1}{R_{s_1}} + \frac{1}{R_{s_2}} + \frac{1}{R_{s_3}}}, \tag{11}$$

where $1/R_{p_{\text{II}}}$, $1/R_{s_1}$, $1/R_{s_2}$, and $1/R_{s_3}$ are the time consumption for a single run of the corresponding protocols. Because the payment protocol I is running in parallel with other protocols, it is not included in Eq. (11), as shown in Fig. 3(a).

4. EXPERIMENT AND RESULTS

A. Experimental Setup

The experimental setup of the quantum e-commerce is shown in Fig. 3(b). In the experiment, we employ time-division multiplexing (TDM) and frequency-division multiplexing (FDM) techniques to construct an efficient point-to-multipoint CV-QKD system, and achieve effective isolation of the pilot tone from the quantum signals. A continuous-wave single-frequency laser at wavelength of 1550.12 nm (NKT Koheras BASIK X15) is injected into an IQ modulator (iXblue MXIQER-LN-30) to generate quantum signal with QPSK modulation and the pilot tone. The DC bias voltage of the IQ modulator is controlled by a commercial automatic locking module. The pilot tone and the quantum signal (repetition rate 625 MHz) are configured with 800 MHz frequency intervals [Fig. 4(a)]. This arrangement allows simple and accurate frequency and phase recovery

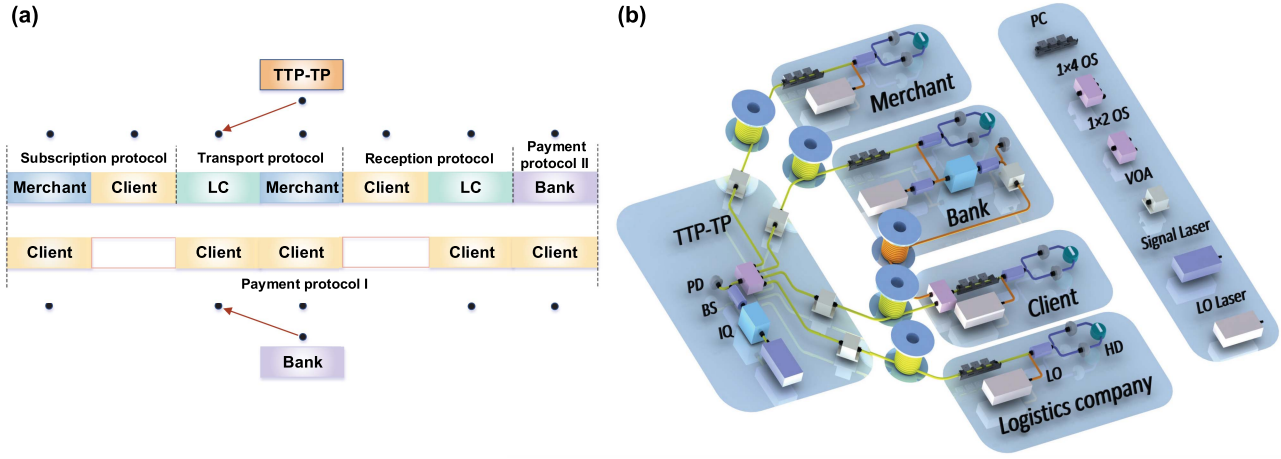

Fig. 3. Experimental quantum e-commerce. (a) Time allocation of the optical switches. We evenly divide the working time of the optical switches into seven intervals. The subscription protocol, the transport protocol, and the reception protocol are allocated two intervals each, while the payment protocol II occupies one interval. During the time slot when the TTP-TP is conducting key distribution with the client, the bank and the client will suspend their key distribution operations. Outside of this time slot, the bank and the client will recover their key distribution. (b) Experimental setup. The TTP-TP prepares quantum states and sends them to the merchant, the client, the LC, and the bank, respectively. Moreover, the bank sends the prepared quantum states to the client. After receiving the quantum signals, they measure both quadratures of the quantum states using heterodyne detection. By data post-processing, keys are shared between the parties. Then the quantum e-commerce is implemented following the procedures in Section 2. IQ, in-phase and quadrature modulator; BS, beam splitter; PD, photoelectric detector; HD, heterodyne detector; VOA, variable optical attenuator; OS, optical switch; PC, polarization controller.

for quantum signals. The radio frequency (RF) electrical signals loaded onto the IQ modulator are generated by converting the digital signals into analogue signals using an arbitrary waveform generator with a 12.5 Gsamples/s sampling rate (AWG, Tektronix, AWG70002A). A 1×4 programmable optical switch is placed after the IQ modulator to route the quantum signals to different quantum channels. A variable optical attenuator is added to the output port of transmitter to adjust the modulation variance of each quantum signal. The prepared quantum signals are sent to the merchant, the client, the LC, and the bank via four independent 80 km standard single-mode fibers, respectively.

At the receiver site, the participants use a manual polarization controller to recover the polarization state of the quantum signal to enable interference between the quantum signal and the local local oscillator (LLO) [57–63]. The participants independently prepared their LLO with a frequency interval of 2 GHz to the quantum signal, and the power of the LLO is 4 mW. This not only significantly reduces the interference of low-frequency noise on the quantum signal, but also circumvents the adverse effects of the negative first-order sidebands [64]. Subsequently, the signal interferes with the LLO at a 50:50 optical fiber coupler and the interfered optical signals are directly fed into a heterodyne detector with a bandwidth of 1.6 GHz (HD, Thorlabs, PDB480C-AC). The output signals from the heterodyne detector are sampled by a 6.25 Gsamples/s oscilloscope (MSO, Tektronix, MSO64B) and stored on the computer's hard disc for digital signal processing (DSP). In addition, the bank acts as a receiver as well as a transmitter. A 10/90 passive beam splitter is employed to split a small portion of the LO for the preparation of quantum states with QPSK modulation. The preparation process of the quantum state is similar to that of the TTP-TP. The prepared quantum signals are sent to the client via an 80 km standard single-mode fiber. In order to receive the quantum signals from the TTP-TP and the bank with a single HD, a 1×2 programmable optical switch is used to route the quantum signals.

B. Digital Signal Processing

Figure 4 shows the DSP procedures used to generate and extract the quantum signals [65]. The modulation signals are upsampled (12.5 Gsamples/s) and pulse shaped using a digital rising cosine (RC) filter with a roll-off factor of 0.2. Then, it is frequency up-shifted to 1.2 GHz and summed with the pilot tone (400 MHz sinusoidal signal) to form the final digital signal. The spectrum of the digital signal is depicted in Fig. 4(a). The QPSK coherent states generated are given by

$$|\alpha\rangle = |x + ip\rangle \exp(i\omega t) = |[x\cos(\omega t) - p\sin(\omega t)] + i[x\sin(\omega t) + p\cos(\omega t)]\rangle, \tag{12}$$

where $x\cos(\omega t) - p\sin(\omega t)$ and $x\sin(\omega t) + p\cos(\omega t)$ are the real and imaginary parts of the complex amplitude of the coherent states, which are proportional to the generated I and Q digital signals, respectively.

The acquired signals from the HD are transformed into frequency domain by fast Fourier transform (FFT). The power spectra of the electronic noise, shot noise, quantum signals, and pilot tone at the receiver are shown in Fig. 4(b). Based on the estimated optical frequency offsets between the transmitter and receiver, the pilot tone and quantum signal are down-converted and low-pass filtered to remove the out-of-band noise. Subsequently, the pilot tone is used to recover the phase of the quantum signal. In order to estimate the frequency deviation and phase fluctuation accurately, the signal to noise ratio of the pilot tone in our experiments is set to around 32 dB.

C. Experimental Results

The experimental parameters of the quantum e-commerce over 80 km standard single-mode fibers are listed in Table 1. In order to optimize the performance of the protocol, the experimental modulation variance at the transmitter is optimized by the theoretical simulation. From Table 1, we see that the detection efficiency and excess noise are the key factors affecting the key rate at the same transmission loss. The signing rate is limited by the minimum key rate, by which we can determine a signing rate of 1.51×10^3 for signing a 33 kilobits file with 2×10^{-10} security bound.

The experimental excess noise of the quantum commerce between different participants at 80 km single-mode fiber is

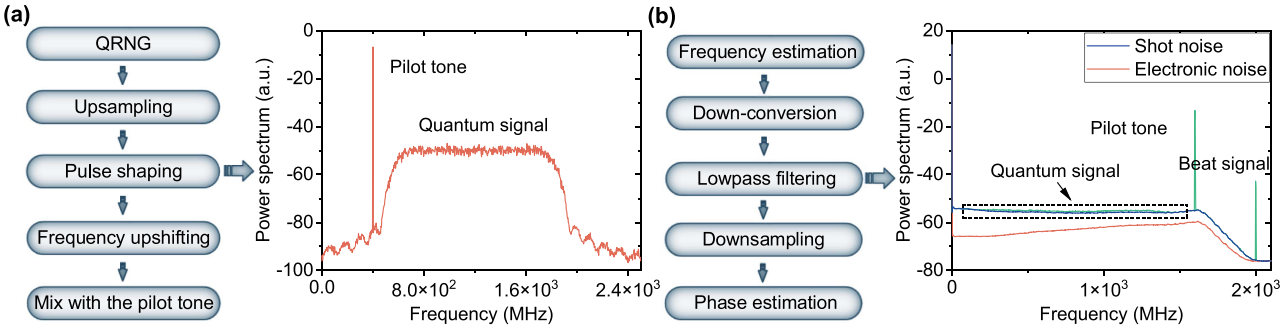

Fig. 4. Digital signal processing in the quantum e-commerce. (a) Generation of the quantum signal and the pilot tone at the transmitter. The TTP-TP and the bank generate modulation signals with quantum true random numbers, which are boosted to a sampling rate of 12.5 Gsamples/s by upsampling. Then, the upsampling signals are pulse shaped and frequency up-shifted to 1.2 GHz. Finally, the pilot tone (400 MHz sinusoidal signal) is added in. (b) Extraction of the quantum signal at the receiver. The fast Fourier transform (FFT) transforms the acquired signal into frequency domain to retrieve the frequency of the pilot tone. The quantum signal and the pilot tone are downconverted to the baseband and low-pass filtered to eliminate the out-of-band noises. The phase of the quantum signal is recovered using that of the pilot tone.

Table 1. Experimental Parameters of the Quantum e-Commerce at 80 km Single-Mode Fiber[a]

Participants	V_M (SNU)	v_{el} (SNU)	η (%)	ε (SNU)	$\Re$ or K_p (bits per second)	Protocol	R_{s_y} or R_{p_j} (times per second)
TTP-TP & merchant	1.00	0.22	0.52	0.0056	4.13×10^5	Subscription protocol	1.43×10^3
TTP-TP & LC	1.01	0.22	0.61	0.0050	5.38×10^5	Transport protocol	1.43×10^3
TTP-TP & client	1.00	0.24	0.49	0.0039	4.38×10^5	Reception protocol	1.51×10^3
TTP-TP & bank	1.01	0.26	0.50	0.0064	4.14×10^5	Payment protocol I	1.96×10^3
Bank & client	1.04	0.24	0.49	0.0110	3.00×10^5	Payment protocol II	2.70×10^3

[a]V_M, modulation variance of the quantum signal; v_{el}, electronic noise for heterodyne detection; η, detection efficiency; ε, excess noise; $\Re$, unknown bits per second distributed between the TTP-TP & merchant, TTP-TP & LC, and TTP-TP & client; K_p, secret key rate of TTP-TP & bank and bank & client; R_{s_y}, the signing rate for signing a 33 kilobits file with security bound 2×10^{-10}; R_{p_j}, payment rate with security bound 2×10^{-10}.

shown in Fig. 5. Thirty data blocks, corresponding to an operation time of 8 h, are shown. For each experimental point, a data size of 5.12×10^8 is used to estimate the excess noise. The average excess noises for the TTP-TP & merchant, TTP-TP & LC, TTP-TP & client, TTP-TP & bank, and bank & client are 0.0056, 0.0050, 0.0039, 0.0064, and 0.011 SNUs, respectively. The results indicate that the excess noise of the system is suppressed to a low level and can keep stable. The main source of excess noise contribution to the system is the phase noise between the LLO and the quantum signal.

Figure 6 shows the results of contract signing rate, payment rate, and transaction rate as a function of distance in quantum e-commerce. The signing rates of the subscription protocol, transport protocol, and reception protocol are depicted in Fig. 6(a). The blue solid line is the theoretical simulation using the experimental parameters. The red circle, purple triangle, and green pentagram are the experiment results. In Fig. 6(b),

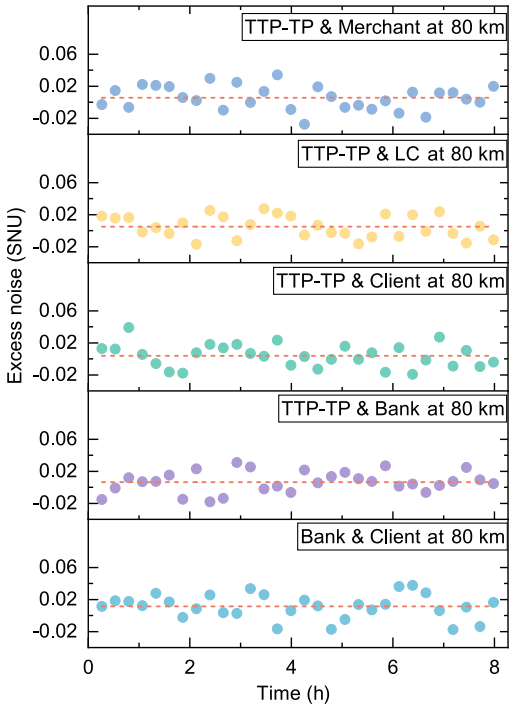

Fig. 5. Excess noise of the CV-QKD between different participants at 80 km single-mode fiber. The solid circles denote experimental points; the dashed line indicates the average value of the excess noise.

the payment rates for the payment protocols I and II are shown. The payment rates take into account the secure key consumption of the payment tokens and signing. By using Eq. (11) and the experimental parameters, the transaction rate of the complete quantum e-commerce is determined to 411 times per second, as depicted in Fig. 6(c). It consists of the signing of three files and two digital payments. Most of the time, the key distribution between the bank and client can operate in parallel with the key distribution between the TTP-TP & merchant, LC, and bank; therefore no additional time overhead is required.

The transaction rate between the quantum e-commerce and the size of the signature file is depicted in Fig. 7. The shadow areas indicate the transaction rates for different sizes of files at higher security levels of $\xi_{tot} < 10^{-9}$. For the same level of security, the larger the signature file, the lower the transaction rate for the quantum e-commerce. Moreover, when the size of signature files increases to 10^7 bits, the transaction rate starts to present a linear reduction with the size of the signature files.

5. DISCUSSION AND CONCLUSION

In our complete quantum e-commerce scheme, we assume that the third-party trading platform (TP-TP) is trusted. On the one hand, the e-commerce trading platforms are tightly regulated by the government. On the other hand, just as in classical e-commerce, the clients will judge the credibility of a trading platform by checking the credit qualification (certification) and users' comments. Both merchants and clients tend to choose the TP-TP with good reputations for transactions. Therefore, the credibility of TP-TP is a reasonable assumption and crucial for the practical application of quantum e-commerce. Additionally, the TTP-TP can be treated as untrusted TP-TP. In the decentralized scheme [39], the untrusted TP-TP does not obtain the client's key before the client receives the merchant's contract and signature. Therefore, our scheme needs to change the structure of the key distribution; more precisely, the signer distributes keys to the untrusted TP-TP and the signature verifier. Then, after rigorous analysis of the potential attacks that the TTP-TP may carry out, which are equivalent to the forgery attacks that the signature verifiers implement, our scheme can be easily adapted to be decentralized in principle.

During the execution of the subscription, transport, and reception protocols, we use the shared keys by TTP-TP and the participants after the error correction and the privacy amplification step is not implemented. Given that the key length used

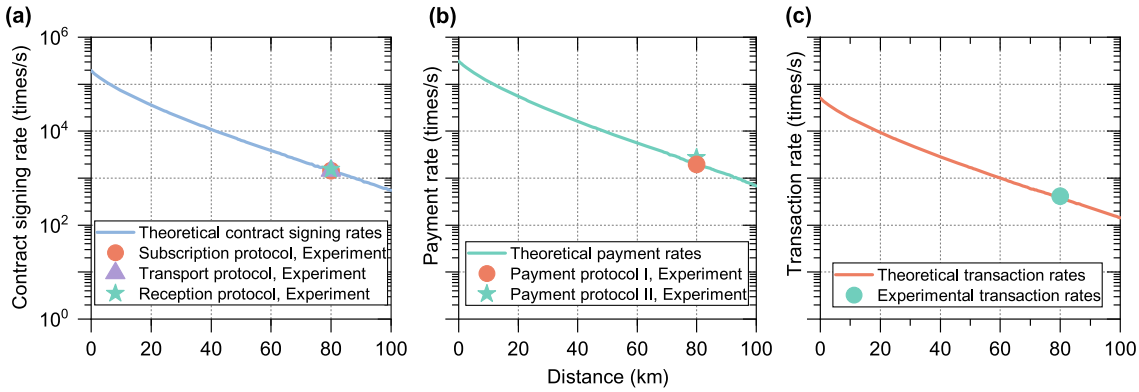

Fig. 6. Contract signing rates, payment rates, and transaction rates versus the distance in quantum e-commerce. (a) Signing rates for the subscription protocol, the transport protocol, and the reception protocol. (b) Payment rates for the payment protocol I and payment protocol II. (c) Transaction rates for the complete quantum e-commerce. The solid line denotes the result of the theoretical simulation. Circles, triangles, and pentagrams denote the experimental results.

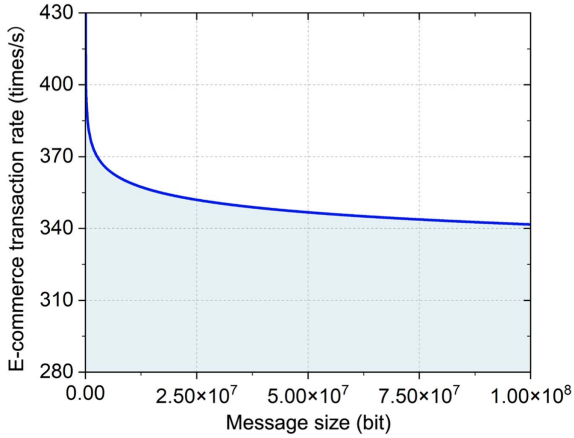

Fig. 7. Transaction rate versus the signature file size in quantum e-commerce. The blue line indicates the transaction rates of a complete quantum e-commerce with 10^{-9} security level at 80 km single-mode fiber. The shadow area denotes a higher security level of $\xi_{\text{tot}} < 10^{-9}$. For a file of 100 megabits size, we can still achieve a secure transaction rate of 341 per second.

in the signing process is relatively short, the finite size effect has a significant impact on the security. In our present work, we primarily focus on the design and proof-of-principle experimental verification of the QDP and quantum e-commerce schemes; the finite size effect will be investigated in our future research.

We propose and experimentally demonstrate a complete quantum e-commerce scheme based on an efficient and practical QDP method with i.t.-security. The quantum e-commerce scheme consists of subscription, payment, transport, and reception stages and involves five parties. It guarantees integrity, authentication, nonrepudiation, traceability, and impartiality during the transaction process. By choosing the Taobao seller service agreement as an example, our experimental system is capable of supporting 411 times transactions per second. The transactions rate can be improved by exploiting higher speed quantum communication systems in the future. For the future quantum Internet, various quantum enabled technologies and applications are essential. Our scheme advances the field of practical quantum e-commerce.

APPENDIX A: HASH FUNCTION

In the Galois field GF(2), an irreducible polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ of order n is randomly generated, where $a_r = 0$ or 1, $r \in \{0,1,\ldots,n-1\}$. The generated n-bit string $p_a = \{a_{n-1}, a_{n-2}, \ldots, a_1, a_0\}$ is used as the coefficients of the polynomial $p(x)$. The signer first generates $p_1(x)$ from the local n-bit random numbers and then checks the polynomial for irreducibility. If the polynomial is irreducible, it is used to generate the LFSR-based Toeplitz matrix H_{nm}. For a polynomial, $p(x)$ over GF(2) is irreducible; the sufficient and necessary condition for the polynomial is [38,66]

$$\begin{cases} x^{2^n} \equiv x \bmod p(x) \\ \gcd\left(x^{2^{\frac{n}{q}}} - x, p(x)\right) = 1 \end{cases}, \tag{A1}$$

where q is any prime factor of n; $\gcd(x^{2^{\frac{n}{q}}} - x, p(x))$ is the greatest common divisor of $x^{2^{\frac{n}{q}}} - x$ and $p(x)$. By utilizing the fast modular composition (FMC) algorithms and extended Euclidean algorithms [67], the computational complexity can be effectively simplified.

The signer uses the n-bit key string $K_{X_1}^{S}$ to generate an initial vector $s = (b_n, b_{n-1}, \ldots, b_2, b_1)^T$ that acts as the first column of the LFSR-based Toeplitz matrix. The LFSR-based Toeplitz matrix is then constructed as $H_{nm} = (s, s_1, \ldots, s_{m-1})$, where $s_1 = (b_{n+1}, b_n, \ldots, b_3, b_2)^T$. The latter column of the Toeplitz matrix is obtained by shifting all the elements of the previous column down by one, and the first element satisfies $b_{n+1} = p_a \cdot s$. The hash value of the contract is calculated by $\text{Hash}^S = H_{nm} \cdot W$.

APPENDIX B: ATTACK OF GUESSING

The LFSR-based Toeplitz matrix H_{nm} is determined by an irreducible polynomial $p(x)$ and the initial vector s. It has been

proved that guessing the irreducible polynomial $p(x)$ is the optimal attack by the following proposition [30].

Proposition. For the LFSR-based Toeplitz hash function $h_{p,s}(W) = H_{nm} \cdot W$, if $p(x)|W(x) = W_{m-1}x^{m-1} + \cdots + W_1 x + W_0$, then $h_{p,s}(W) = 0$.

More precisely, the attacker, knowing $p(x)$, can generate a file themselves W' that satisfies $h(W') = 0$. At this point, the attacker can perform the following attack: the attacker uses an n'-bit string to decrypt the encrypted p_a and acquire an expected irreducible polynomial $p'(x)$. The attacker produces a W'-bit bit string satisfying the above $p'(x)|W'(x)$ relation. If $p'(x) = p(x)$, then $h(W') = 0$. The attacker modifies contract W to $W \oplus W'$ and the new contract and the old signature $\{W \oplus W', S^S\}$ will pass the TTP-TP verification.

Since the orders of $W'(x)$ and $p(x)$ are m and n, respectively, the maximum number of guesses for $p(x)$ does not exceed m/n. Note that here it is necessary to consider that the attacker knows that the polynomial $p(x)$ is irreducible. The probability that $p(x)$ is successfully guessed is

$$P_s = \frac{m}{n} P(p'(x) = p(x)|p'(x) \in \mathbb{Z}), \tag{B1}$$

where $P(p'(x) = p(x)|p'(x) \in \mathbb{Z})$ denotes the probability of making a single guess on an irreducible polynomial $p'(x) = p(x)$ under the $\mathbb{Z}$ set of all irreducible polynomials of order n in GF(2). The number of irreducible polynomials of order n does not exceed $2^{n-1}/n$. Thus the probability of finding the irreducible polynomial is $P(p'(x) \in \mathbb{Z}) \le (2^{n-1}/n)/2^n = 1/(2n)$. Finally, the probability of a successful attack is given by

$$P_s = \frac{m}{n} \cdot \frac{P(p'(x) = p(x))}{P(p'(x) \in \mathbb{Z})} \le \frac{m}{n} \cdot \frac{2^{-\mathfrak{R}_n}}{1/(2n)} = m \cdot 2^{1-\mathfrak{R}_n}. \tag{B2}$$

Funding. National Natural Science Foundation of China (62175138, 62205188); Shanxi 1331KSC; Innovation Program for Quantum Science and Technology (2021ZD0300703).

Disclosures. The authors declare no conflicts of interests.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1997).
2. E. Martín-López, A. Laing, T. Lawson, *et al.*, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," Nat. Photonics **6**, 773–776 (2012).
3. É. Gouzien and N. Sangouard, "Factoring 2048-bit RSA integers in 177 days with 13436 qubits and a multimode memory," Phys. Rev. Lett. **127**, 140503 (2021).
4. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory **22**, 644–654 (1976).
5. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**, 120–126 (1978).
6. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory **31**, 469–472 (1985).
7. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, *et al.*, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
8. E. Diamanti, H.-K. Lo, B. Qi, *et al.*, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 16025 (2016).
9. F. Xu, X. Ma, Q. Zhang, *et al.*, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
10. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
11. C. Portmann and R. Renner, "Security in quantum cryptography," Rev. Mod. Phys. **94**, 025008 (2022).
12. Y. Zhang, Y. Bian, Z. Li, *et al.*, "Continuous-variable quantum key distribution system: past, present, and future," Appl. Phys. Rev. **11**, 011318 (2024).
13. J. Yin, Y.-H. Li, S.-K. Liao, *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature **582**, 501–505 (2020).
14. Y. Liu, W.-J. Zhang, C. Jiang, *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," Phys. Rev. Lett. **130**, 210801 (2023).
15. S. Wang, Z.-Q. Yin, D.-Y. He, *et al.*, "Twin-field quantum key distribution over 830-km fibre," Nat. Photonics **16**, 154–161 (2022).
16. D. Gottesman and I. Chuang, "Quantum digital signatures," arXiv, arXiv:quant-ph/0105032 (2001).
17. H.-L. Yin, Y. Fu, and Z.-B. Chen, "Practical quantum digital signature," Phys. Rev. A **93**, 032316 (2016).
18. R. Amiri, P. Wallden, A. Kent, *et al.*, "Secure quantum signatures using insecure quantum channels," Phys. Rev. A **93**, 032325 (2016).
19. Y.-S. Lu, X.-Y. Cao, C.-X. Weng, *et al.*, "Efficient quantum digital signatures without symmetrization step," Opt. Express **29**, 10162–10171 (2021).
20. C.-X. Weng, Y.-S. Lu, R.-Q. Gao, *et al.*, "Secure and practical multiparty quantum digital signatures," Opt. Express **29**, 27661–27673 (2021).
21. J.-Q. Qin, C. Jiang, Y.-L. Yu, *et al.*, "Quantum digital signatures with random pairing," Phys. Rev. Appl. **17**, 044047 (2022).
22. P. J. Clarke, R. J. Collins, V. Dunjko, *et al.*, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," Nat. Commun. **3**, 1174 (2012).
23. V. Dunjko, P. Wallden, and E. Andersson, "Quantum digital signatures without quantum memory," Phys. Rev. Lett. **112**, 040502 (2014).
24. R. J. Collins, R. J. Donaldson, V. Dunjko, *et al.*, "Realization of quantum digital signatures without the requirement of quantum memory," Phys. Rev. Lett. **113**, 040502 (2014).
25. I. V. Puthoor, R. Amiri, P. Wallden, *et al.*, "Measurement-device-independent quantum digital signatures," Phys. Rev. A **94**, 022328 (2016).
26. T. Shang, Q. Lei, and J. Liu, "Quantum random oracle model for quantum digital signature," Phys. Rev. A **94**, 042314 (2016).
27. M. Thornton, H. Scott, C. Croal, *et al.*, "Continuous-variable quantum digital signatures over insecure channels," Phys. Rev. A **99**, 032341 (2019).
28. W. Zhao, R. Shi, J. Shi, *et al.*, "Multibit quantum digital signature with continuous variables using basis encoding over insecure channels," Phys. Rev. A **103**, 012410 (2021).
29. C.-H. Zhang, X. Zhou, C.-M. Zhang, *et al.*, "Twin-field quantum digital signatures," Opt. Lett. **46**, 3757–3760 (2021).
30. B.-H. Li, Y.-M. Xie, X.-Y. Cao, *et al.*, "One-time universal hashing quantum digital signatures without perfect keys," Phys. Rev. Appl. **20**, 044011 (2023).
31. R. J. Collins, R. Amiri, M. Fujiwara, *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**, 4883–4886 (2016).
32. C. Croal, C. Peuntinger, B. Heim, *et al.*, "Free-space quantum signatures using heterodyne measurements," Phys. Rev. Lett. **117**, 100503 (2016).

33. G. L. Roberts, M. Lucamarini, Z. L. Yuan, *et al.*, "Experimental measurement-device-independent quantum digital signatures," Nat. Commun. **8**, 1098 (2017).
34. X.-B. An, H. Zhang, C.-M. Zhang, *et al.*, "Practical quantum digital signature with a gigahertz BB84 quantum key distribution system," Opt. Lett. **44**, 139–142 (2019).
35. H.-J. Ding, J.-J. Chen, L. Ji, *et al.*, "280-km experimental demonstration of a quantum digital signature with one decoy state," Opt. Lett. **45**, 1711–1714 (2020).
36. S. Richter, M. Thornton, I. Khan, *et al.*, "Agile and versatile quantum communication: signatures and secrets," Phys. Rev. X **11**, 011038 (2021).
37. Y. Pelet, I. V. Puthoor, N. Venkatachalam, *et al.*, "Unconditionally secure digital signatures implemented in an eight-user quantum network," New J. Phys. **24**, 093038 (2022).
38. H.-L. Yin, Y. Fu, C.-L. Li, *et al.*, "Experimental quantum secure network with digital signatures and encryption," Natl. Sci. Rev. **10**, nwac228 (2022).
39. X.-Y. Cao, B.-H. Li, Y. Wang, *et al.*, "Experimental quantum e-commerce," Sci. Adv. **10**, eadk3258 (2024).
40. S. Wiesner, "Conjugate coding," ACM SIGACT News **15**, 78–88 (1983).
41. F. Pastawski, N. Y. Yao, L. Jiang, *et al.*, "Unforgeable noise-tolerant quantum tokens," Proc. Natl. Acad. Sci. USA **109**, 16079–16082 (2012).
42. K. Bartkiewicz, A. Černoch, G. Chimczak, *et al.*, "Experimental quantum forgery of quantum optical money," npj Quantum Inf. **3**, 7 (2017).
43. M. Bozzio, A. Orieux, L. T. Vidarte, *et al.*, "Experimental investigation of practical unforgeable quantum money," npj Quantum Inf. **4**, 5 (2018).
44. J.-Y. Guan, J. M. Arrazola, R. Amiri, *et al.*, "Experimental preparation and verification of quantum money," Phys. Rev. A **97**, 032338 (2018).
45. M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," Phys. Rev. A **99**, 022336 (2019).
46. K. Jiráková, K. Bartkiewicz, A. Černoch, *et al.*, "Experimentally attacking quantum money schemes based on quantum retrieval games," Sci. Rep. **9**, 16318 (2019).
47. K. Horodecki and M. Stankiewicz, "Semi-device-independent quantum money," New J. Phys. **22**, 023007 (2020).
48. A. Kent, D. Lowndes, D. Pitalúa-García, *et al.*, "Practical quantum tokens without quantum memories and experimental tests," npj Quantum Inf. **8**, 28 (2022).
49. Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, *et al.*, "One-hour coherent optical storage in an atomic frequency comb memory," Nat. Commun. **12**, 2381 (2021).
50. P. Schiansky, J. Kalb, E. Sztatecsny, *et al.*, "Demonstration of quantum-digital payments," Nat. Commun. **14**, 3849 (2023).
51. https://aws.amazon.com/agreement/?nc1=hls.
52. https://terms.alicdn.com/legal-agreement/terms/suit_bu1_taobao/suit_bu1_taobao201908081502_44434.html.
53. H. Krawczyk, "LFSR-based hashing and authentication," in *Annual International Cryptology Conference* (1994), pp. 129–139.
54. R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Trans. Inf. Theory **55**, 4337–4347 (2009).
55. J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution," Phys. Rev. X **9**, 041064 (2019).
56. J. Lin and N. Lütkenhaus, "Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution," Phys. Rev. Appl. **14**, 064030 (2020).
57. B. Qi, P. Lougovski, R. Pooser, *et al.*, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**, 041009 (2015).
58. H. Wang, Y. Li, Y. Pi, *et al.*, "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," Commun. Phys. **5**, 162 (2022).
59. Y. Tian, Y. Zhang, S. Liu, *et al.*, "High-performance long-distance discrete-modulation continuous-variable quantum key distribution," Opt. Lett. **48**, 2953–2956 (2023).
60. L. Li, T. Wang, X. Li, *et al.*, "Continuous-variable quantum key distribution with on-chip light sources," Photon. Res. **11**, 504–516 (2023).
61. T. Wang, P. Huang, L. Li, *et al.*, "High key rate continuous-variable quantum key distribution using telecom optical components," New J. Phys. **26**, 023002 (2024).
62. Y. Bian, Y. Pan, X. Xu, *et al.*, "Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip," Appl. Phys. Lett. **124**, 174001 (2024).
63. A. A. E. Hajomer, I. Derkach, N. Jain, *et al.*, "Long-distance continuous-variable quantum key distribution over 100-km fiber with local oscillator," Sci. Adv. **10**, eadi9474 (2024).
64. N. Jain, I. Derkach, H.-M. Chin, *et al.*, "Modulation leakage vulnerability in continuous-variable quantum key distribution," Quantum Sci. Technol. **6**, 045001 (2021).
65. Z. Chen, X. Wang, S. Yu, *et al.*, "Continuous-mode quantum key distribution with digital signal processing," npj Quantum Inf. **9**, 28 (2023).
66. M. O. Rabin, "Probabilistic algorithms in finite fields," SIAM J. Comput. **9**, 273–280 (1980).
67. J. von zur Gathen and J. Gerhard, *Modern Computer Algebra* (Cambridge University, 2013).