Efficient Quantum Digital Signatures without Symmetrization Step

Yu-Shuo Lu, Xiao-Yu Cao, Chen-Xun Weng, Jie Gu, Yuan-Mei Xie, Min-Gang Zhou, Hua-Lei Yin and Zeng-Bing Chen

National Laboratory of Solid State Microstructures,
School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China.

Quantum digital signatures (QDS) exploit quantum laws to guarantee non-repudiation, unforgeability and transferability of messages with information-theoretic security. Current QDS protocols face two major restrictions, including the requirement of the symmetrization step with additional secure classical channels and quadratic scaling of the signature rate with the probability of detection events. Here, we present an efficient QDS protocol to overcome these issues by utilizing the classical post-processing operation called post-matching method. Our protocol does not need the symmetrization step, and the signature rate scales linearly with the probability of detection events. Simulation results show that the signature rate is three orders of magnitude higher than the original protocol in a 100-km-long fiber. This protocol is compatible with existing quantum communication infrastructure, therefore we anticipate that it will play a significant role in providing digital signatures with unconditional security.

I. INTRODUCTION

Cryptography is essential for uncounted amount of applications that rely on non-repudiation, integrity and confidentiality of data. The two pillars of modern cryptography are encryption and digital signatures [1], where encryption guarantees confidentiality and digital signatures provide integrity and non-repudiation. Traditionally, public-key cryptography algorithms, such as the Rivest-Shamir-Adleman algorithm [2], are designed to simultaneously provide encryption and digital signature service. However, relying on the computational difficulty of certain mathematical problems, public-key cryptosystems are usually vulnerable to quantum computing attacks [3]. Quantum key distribution (QKD) allows two remote users to share a secret key string with information-theoretic security [4, 5]. By combining one-time pad encryption [6] and QKD, one can implement information communication with perfect confidentiality [7]. In addition, the direct transmission of private information is made possible in principle by quantum encryption [8].

Digital signatures are widely applied in e-mails, electronic commerce and software distribution to ensure data integrity and non-repudiation [9]. Similar to QKD used for encryption service, quantum digital signatures (QDS) are expected to provide information-theoretic security to sign documents. The first QDS protocol was proposed in 2001 [10], but it is unfeasible because of challenging experimental requirements. In the next decade or so, great efforts have been made in developing QDS protocols and an important achievement was the removal of the requirement of quantum memory [11, 12]. Nevertheless, the security analysis of the early QDS protocols are based on secure quantum channels, i.e., there is no eavesdropping, which is a conflicting assumption. In 2016, two independent QDS protocols were proposed and proved to be secure against the general attacks without the assumption of secure quantum channels [16, 17]. Importantly, their experimental devices and techniques have already been widely employed in QKD. These two protocols are important steps towards practical QDS [9]. The one in [16] is based on non-orthogonal encoding. The other [17] utilizes orthogonal encoding, which results in the need of an additional symmetrization step in the protocol. In addition, great achievements have been made in the experimental and theoretical research of information-theoretically secure QDS [13–20], including the field test of measurement-device-independent (MDI) QDS [21].

For the orthogonal encoding based protocol [17] (see also [18–27]), the need of the symmetrization step, which requires an additional secure classical channel, is the main issue. Currently, secure classical channels can only be realized by combining QKD and one-time pad encryption. The symmetrization step will consume 6L bits of secret key generated by QKD if one uses L bits as the signature [21]. Specially, in the worst case where the signer is located in the middle of two receivers, the low secret key rate of QKD between the two receivers severely limits the real-time signature rate of QDS. Besides, considering a quantum network with J users, there will be a need of J(J − 1)/2 secure classical channels [22], which is an unrealistically high amount in a real quantum network. For the non-orthogonal encoding based protocol [16], it does not require the symmetrization step. However, the signer has to send the same quantum states to two receivers. Only coincidence detection events, i.e., the two receivers both have click, are valid events. Let η be the probability that one receiver has click, if the signer sends N quantum states to the two receivers, there will be only ηN valid events. Therefore, the signature rate quadratically scales with the probability of detection events.

Here, inspired by the original protocol in [16], we
propose an efficient quantum digital signature protocol without symmetrization step. A novel classical post-processing operation called post-matching method is exploited in our protocol. With the help of the post-matching method, the requirement of coincidence detection is removed. Given that the signer sends $N$ quantum states to receivers, there will be $\eta N$ valid events. Therefore the signature rate decays linearly with the probability of detection events. Simulation results show that the signature rate of our scheme is 2 or even 3 orders of magnitude higher than that of Ref. [10] in large attenuation case, and is comparable to orthogonal encoding based protocol.

II. PROTOCOL DESCRIPTION

There are three participants in our protocol, namely the signer Alice and the receiver Bob and Charlie. As determined by Alice, either Bob or Charlie can be the authenticator of the signature, and the other becomes the verifier. There are noisy insecure quantum channels connecting Alice-Bob and Alice-Charlie, and authenticated classical channels between the three participants. There are three stages in our protocol: key generation, estimation and messaging. In our protocol, the three stages can be performed separately, which means they can generate raw keys and store them for a long time, and continue the processing operation called post-matching method, the requirement of coincidence detection and messaging. In our protocol, the three stages can be performed separately, which means they can generate raw keys and store them for a long time, and continue the estimation and messaging stage whenever Alice wants to sign the message. This makes our protocol more practical.

Our protocol exploits non-orthogonal encoding to generate logical bits [34]. There are four quantum states: $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$, where $|H\rangle$ and $|V\rangle$ are the eigenstates of the Pauli Z operator and $|+\rangle$ and $|-\rangle$ ($|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$) are the eigenstates of the Pauli X operator. These four quantum states can be arranged into four sets: $\{ |H\rangle, |+\rangle \}$, $\{ |V\rangle, |+\rangle \}$, $\{ |V\rangle, |-\rangle \}$, $\{ |H\rangle, |-\rangle \}$, where the first state in each set is encoded with bit value 0 and the second is encoded with 1. Alice randomly sends quantum states to receivers and assigns each quantum state to a set. The receivers randomly choose $Z$ or $X$ basis to perform polarization measurement on each quantum state. If the measurement outcome is orthogonal to one of the states in the set, the receiver obtains a conclusive result with bit value 0 or 1, otherwise the receiver obtains an inconclusive result, denoted by $\perp$. Note that the set assigned by Alice should contain the quantum state she sent. For example, if Alice sends $|H\rangle$, she should assign it to set $\{ |H\rangle, |+\rangle \}$ or $\{ |-\rangle, |H\rangle \}$. When she assigns it to the set $\{ |H\rangle, |+\rangle \}$ and Bob’s measurement outcome is $|-\rangle$ ($|V\rangle$), Bob obtains a conclusive result with bit value 0 (1).

The decoy-state method [31] [32] with three intensities is exploited to deal with photon-number-splitting attack for coherent state source. Data from the decoy state and vacuum state will be used for parameter estimation, and only data from the signal state will be used as test bits and secret keys. The setup for our QDS protocol is presented in Fig. 1. In the following part of the paper, we use superscripts $c$, $u$, $t$, $s$, overline (underline), to denote conclusive results, untest bits, test bits, expected value and the upper bound (lower bound) of expected value, respectively. We also use subscripts $P$ ($P \in \{ A, B, C \}$), 11 and 12 to denote Alice (Bob, Charlie), single-photon pair components and intensity respectively. Detailed descriptions of our protocol are given below.

1. Key generation. (1) Alice randomly selects a quantum state $\{ |H\rangle, |V\rangle, |+\rangle, |-\rangle \}$ with the same possibility and an intensity $\{ \mu, \nu, 0 \}$ (signal, decoy and vacuum state) with possibilities $p_{\mu}$, $p_{\nu}$ and $p_{0}$ respectively. For each possible message $m$ ($m = 0$ or 1), Alice prepares two different quantum state sequences with length $N$, namely $A_{B,m}$, and $A_{C,m}$. Alice sends $A_{B,m}$ to Bob and $A_{C,m}$ to Charlie through insecure quantum channels.

(2) For each quantum state, Bob and Charlie randomly choose $X$ or $Z$ basis to perform polarization measurement. Bob announces all the click events in $A_{B,m}$ through authenticated classical channel. Alice and Bob discard all the data that has no click. They keep the left data of length $n$, denote as $S_{AB,m}$ (kept by Alice) and $S_{B,m}$ (kept by Bob). Alice and Charlie perform the same step. As a result, Alice has four data strings $S_{AB,0}^{A}$, $S_{AB,1}^{A}$, $S_{AC,0}^{A}$ and $S_{AC,1}^{A}$. Bob (Charlie) has two strings $S_{B,0}^{B}$ ($S_{C,0}^{C}$) and $S_{B,1}^{B}$ ($S_{C,1}^{C}$). Since Alice randomly and independently chooses quantum states, the quantum states that Bob and Charlie receive are uncorrelated.

(3) Alice announces the intensity information of all pulses. According to the intensity information, the three participants divide each of their data strings into three strings, namely $\mu$ string, $\nu$ string and 0 string. For example, Bob divides $S_{B,m}$ into $S_{B,m}^{0}$, $S_{B,m}^{\nu}$ and $S_{B,m}^{\mu}$.

(4) For the data strings corresponding to each intensity $\lambda$ ($\lambda \in \{ \mu, \nu, 0 \}$), Alice takes $S_{AB,m}^{A}$ as the reference and changes the order of elements in $S_{AC,m}^{A}$. Denote the changing result as $S_{AC,m}^{A}$. Alice should make $S_{AB,m}^{A}$ and $S_{AC,m}^{A}$ identical. Without loss of generality, she requests Charlie to change the order of elements in $S_{C,m}^{A}$ into the same order. We call this the post-matching method. After post-matching, the data obtained by Bob and Charlie

![FIG. 1. Schematic diagram of a setup for our QDS protocol.](image-url)
changing the order of data. For example, if \( S_A^{c,m} \) elements in \( S_A^{c,m} \) and \( \overline{S}_A^{c,m} \), after post-matching, it is equivalent to Alice simultaneously sending the same quantum states to Bob and Charlie. To publicly announce the value of these bits. We denote \( E_{\overline{C}}^{cu} \) and \( E_{\overline{C}}^{ct} \), respectively. If \( E_{\overline{B}}^{cu} \) or \( E_{\overline{C}}^{cu} \) shows a big deviation from the ideal value \( \frac{1}{2} \), they will also abort the protocol. The three participants discard the test bits and keep the remaining untest bits in \( \mu \) strings with length \( n^u \). We denote these untest bit strings as \( K_{A,m}^u, K_{B,m}^u \) and \( K_{C,m}^u \). They will be used as secret keys to sign the message in the messaging stage.

(2) Bob and Charlie announce \( \{E_B^{ct}, P_B^c\} \) and \( \{E_C^{ct}, P_C^c\} \). The three participants publicly negotiate to determine the values of authentication security threshold \( T_a \) and verification security threshold \( T_v \).

3. Messaging. (1) To sign a one-bit message \( m \), Alice sends the message and the corresponding secret key \( \{m, K_{A,m}^u\} \) to the authenticator Bob. Bob calculates the mismatch rate of conclusive results between \( K_{A,m}^u \) and \( K_{B,m}^u \), which is denoted as \( E_{B}^{cu} \). If \( E_{B}^{cu} < T_a \), Bob accepts the message and forwards \( \{m, K_{A,m}^u\} \) to Charlie, otherwise he rejects the message and announces to abort the protocol.

(2) After receiving \( \{m, K_{A,m}^u\} \) forwarded by Bob, Charlie calculates the mismatch rate of conclusive results \( E_{C}^{cu} \) between \( K_{A,m}^u \) and \( K_{C,m}^u \). Charlie accepts the message if \( E_{C}^{cu} < T_v \). When both Bob and Charlie accept the message, Alice successfully signs the message.

III. SECURITY ANALYSIS

In our protocol, Alice randomly chooses unrelated quantum states to send to Bob and Charlie. After post-matching, it is equivalent to Alice simultaneously sending the same quantum states to Bob and Charlie. To perform post-matching, Alice exposes information of order, but does not leak information of quantum states. In this case, eavesdroppers cannot obtain more information of quantum states compared with the case where Alice actually sends two copies of quantum states. Thus the security analysis of our protocol can directly follow the lines in Ref. \[16\]. In the three-participant scenario, transferability and nonrepudiation are equivalent. Accordingly, there are three security criteria: robustness, security against forging and security against repudiation. For simplicity, we just briefly present our results. For more detail, refer to Ref. \[16\].

1. Robustness. The robustness means the probability of an honest abort \( \epsilon_{rob} \). In messaging stage, Bob rejects the message sent by Alice when \( E_{B}^{cu} > T_a \). In the case of finite sample size, the robustness can be quantified by exploiting random sampling without replacement theorem \[33\].

2. Security against forging. In a forgery attack, Bob sends the message he wishes to forge and its corresponding secret key \( \{m, K_{B,F,m}^u\} \) to Charlie. The forgery attack is successful if Charlie accepts Bob’s forged message. An honest Bob knows only about \( \frac{1}{4} \) of conclusive results in \( K_{A,m}^u \). If Bob is an adversary, his optimal strategy is to acquire information of quantum states Charlie receives as much as possible, which is equivalent to the
eavesdropping attack of Eve in four-state Scarani-Acin-Ribordy-Gisin 2004 (SARG04) QKD with two-photon source [30, 31, 32].

We assume only single-photon pairs that Alice sends to Bob and Charlie are secure. In this case, Bob and Charlie both receive a single-photon. Using Chernoff bound [33], the probability of a successful forgery attack \(\varepsilon_{\text{for}}\) can be given by

\[
\varepsilon_{\text{for}} = \exp \left[ -\frac{(E_{BF1}^* - T_{\text{cl}})^2}{2E_{BF1}^*} \right],
\]

where \(E_{BF1}^*\) is the expected value of minimum mismatch rate of conclusive results of the single-photon pair components between \(K_{B,m}^\alpha\) and \(K_{B,F,m}^\beta\), \(T_{\text{cl}} = T_v n_e / n_{C11}^\mu\) is the error rate threshold of single-photon pair, \(n_{C11}^\mu = (1 - \varepsilon_1) n_{\mu}^\mu\) is the number of conclusive results in \(K_{B,m}^\mu\), \(n_{C11}^\mu = (1 - \varepsilon_1) s_{C11}^{\mu\ast}\) is the number of single-photon pair components in \(K_{B,m}^\mu\) and \(s_{C11}^{\mu\ast}\) is the number of events in which Bob and Charlie both receive a single-photon in \(\mu\) string and Charlie has a conclusive result.

To obtain the value of \(E_{BF1}^*\), one should exploit de-coy state method to estimate \(s_{C11}^{\mu\ast}\) and \(s_{C111}^{\mu\ast}\), where \(s_{C11}^{\mu\ast}\) is the number of events that Bob and Charlie both receive a single-photon in \(\mu\) string, Charlie has a conclusive result, and his classical bit is mismatching with Alice’s. We use \(n_{\mu\lambda}\) to denote the number of detection events of the participant \(P\) of intensity \(\lambda\) and \(m_{\mu\alpha}\) to denote the number of mismatching bits. The expected value of parameter \(x\) can be acquired by the variant of Chernoff bound [33]:

\[
\overline{x} = x + \beta + \sqrt{2\beta \chi + \beta^2} \quad \text{and} \quad \overline{x}^\ast = x - \beta - \sqrt{2\beta \chi + \beta^2}
\]

with \(\beta = \ln \frac{1}{\epsilon_1}\), where \(\epsilon_1\) is the failure probability of the Chernoff bound.

Separately consider the process that Alice sends pulses to Bob and to Charlie, we have

\[
s_{C11}^{\mu\ast} \geq \frac{p_{\mu} e^{-\mu}}{\nu (\mu - \nu)} \left[ \nu^2 e^{\mu} \frac{n_{C11}^{\mu\ast}}{p_{\mu}} - \nu^2 e^{\mu} \frac{n_{C11}^{\mu\ast}}{p_{\mu}} + (\nu^2 - \mu^2) \frac{n_{C11}^{\mu\ast}}{p_{\mu}} \right],
\]

and

\[
s_{B1}^{\mu\ast} \geq \frac{p_{\mu} e^{-\mu}}{\nu (\mu - \nu)} \left[ \nu^2 e^{\mu} \frac{n_{B1}^{\mu\ast}}{p_{\mu}} - \nu^2 e^{\mu} \frac{n_{B1}^{\mu\ast}}{p_{\mu}} + (\nu^2 - \mu^2) \frac{n_{B1}^{\mu\ast}}{p_{\mu}} \right],
\]

where \(s_{B1}^{\mu\ast}\) is the number of single-photon events in Bob’s \(\mu\) string and \(s_{C11}^{\mu\ast}\) is the number of conclusive single-photon events in Charlie’s \(\mu\) string. \(s_{C111}^{\mu\ast}\) can be given by

\[
s_{C111}^{\mu\ast} \geq s_{C11}^{\mu\ast} \times \frac{s_{B1}^{\mu\ast}}{n_{B1}^{\mu\ast}},
\]

Bring in Eqs. (2) (3), we have

\[
s_{C11}^{\mu\ast} \geq \frac{p_{\mu} e^{-\mu}}{\nu (\mu - \nu)} \left[ \nu^2 e^{\mu} \frac{n_{C11}^{\mu\ast}}{p_{\mu}} - \nu^2 e^{\mu} \frac{n_{C11}^{\mu\ast}}{p_{\mu}} + (\nu^2 - \mu^2) \frac{n_{C11}^{\mu\ast}}{p_{\mu}} \right],
\]

and

\[
s_{B1}^{\mu\ast} \geq \frac{p_{\mu} e^{-\mu}}{\nu (\mu - \nu)} \left[ \nu^2 e^{\mu} \frac{n_{B1}^{\mu\ast}}{p_{\mu}} - \nu^2 e^{\mu} \frac{n_{B1}^{\mu\ast}}{p_{\mu}} + (\nu^2 - \mu^2) \frac{n_{B1}^{\mu\ast}}{p_{\mu}} \right],
\]

where \(t_{C1}^{\mu\ast}\) is the number of single-photon errors of Charlie’s conclusive results in \(\mu\) string with respect to Alice. \(t_{C1}^{\mu\ast}\) can be given by:

\[
t_{C1}^{\mu\ast} \leq t_{C1}^{\mu\ast} \times \frac{n_{B1}^{\mu\ast}}{n_{B1}^{\mu\ast}}.
\]

Bring in Eqs. (6) (7), we have

\[
t_{C11}^{\mu\ast} \leq \frac{p_{\mu} e^{-\mu}}{\nu (\mu - \nu)} \left[ \nu^2 e^{\mu} \frac{n_{C11}^{\mu\ast}}{p_{\mu}} - \nu^2 e^{\mu} \frac{n_{C11}^{\mu\ast}}{p_{\mu}} + (\nu^2 - \mu^2) \frac{n_{C11}^{\mu\ast}}{p_{\mu}} \right],
\]

and

\[
t_{B1}^{\mu\ast} \leq \frac{p_{\mu} e^{-\mu}}{\nu (\mu - \nu)} \left[ \nu^2 e^{\mu} \frac{n_{B1}^{\mu\ast}}{p_{\mu}} - \nu^2 e^{\mu} \frac{n_{B1}^{\mu\ast}}{p_{\mu}} + (\nu^2 - \mu^2) \frac{n_{B1}^{\mu\ast}}{p_{\mu}} \right],
\]

where \(A = \frac{(P_C T_v - P_C^c) \left( \frac{\Delta_{BC}}{n_C} + A \right)}{2 A}\),

\[
3 P_C^c \left( \frac{\Delta_{BC}}{n_C} + A \right),
\]

with \(P_C T_v < A < P_C^c \left( T_v - \frac{\Delta_{BC}}{n_C} \right)\).

The overall secrecy is:

\[
\varepsilon_{\text{tot}} = 11 \varepsilon_1 + \varepsilon_2 + \varepsilon_{\text{for}} + \varepsilon_{\text{rob}} + \varepsilon_{\text{rep}},
\]

where \(\varepsilon_2\) is the failure probability of random sampling without replacement.
IV. PERFORMANCE

In order to show the performance of our protocol, we simulate a fiber-based QDS system. Define signature rate $R := \frac{1}{2N}$, where $2N$ is the minimum number of pulses required to securely sign a one-bit message. Fig. 3 shows the signature rate $R$ as a function of transmission distance. We consider the case where channels between Alice-Bob and Alice-Charlie are symmetric.

The security bounds are set to $\varepsilon_{for} \leq 10^{-10}$, $\varepsilon_{rob} \leq 10^{-10}$, $\varepsilon_{rep} \leq 10^{-10}$ and $\varepsilon_1 = \varepsilon_2 \leq (10^{-9} - 3 \times 10^{-10})/12$. We numerically optimize the minimum number of pulses required to securely sign a one-bit message with the free parameters $\{\mu, \nu, p_\mu, p_\nu, t\}$ by global search algorithm. For a fair comparison, we simulate the performance of the original protocol in Ref. [10] with the same experimental parameters. As shown in Fig. 3, the solid red line represents the signature rate of this work and the blue dashed line represents the original QDS protocol. Obviously, our protocol requires far less number of pulses to sign a one-bit message. Specifically, at 50 km and 100 km, our protocol requires $3.3 \times 10^8$ and $3.4 \times 10^9$ pulses to sign a one-bit message, but the protocol in Ref. [10] requires $3.8 \times 10^{10}$ and $3.7 \times 10^{12}$ pulses. The signature rate of our protocol is 2 or even 3 orders of magnitude higher than the original protocol at long distance.

We also simulate the performance of orthogonal encoding based protocol [17] with the cost of symmetrization taken into consideration. Assume Bob and Charlie utilize three-intensity decoy-state BB84 QKD protocol to perform symmetrization. Define the effective signature rate $R_{\text{eff}} := \min \{ \frac{1}{2NL}, \frac{R_{\text{QKD}}}{6L}\}$, where $L$ is the length of key generated by key generation protocol in [17] and $R_{\text{QKD}}$ is the secret key rate of QKD. Note that $\frac{6L}{R_{\text{QKD}}}$ is the number of pulses required for QKD to perform symmetrization [21]. $R_{\text{QKD}}$ is simulated by the key rate formula in [37], where we choose error-correction efficiency $f = 1.22$, data-post-processing block size $N = 10^{10}$, secrecy $\varepsilon_{\text{sec}} = 10^{-10}$ and the same experimental parameters as Fig. 3.

Denote the angle between Alice-Bob and Alice-Charlie as $\theta$, the distance between Alice and Bob (Charlie) as $D_{AB}$ ($D_{AC}$), and the distance between Bob and Charlie as $D_{BC}$. In symmetric case, $D_{AB} = D_{AC}$, and $D_{BC} = 2\sin(\frac{\theta}{2})D_{AB}$. At short distance where $R_{\text{QKD}}$ is very high, $R_{\text{eff}}$ is mainly determined by $\frac{1}{2NL}$. When $\theta$ is close to $\pi$, the transmission distance of QKD ($D_{BC}$) increases much faster than $D_{AB}$. In this case, $R_{\text{eff}}$ is determined by $R_{\text{QKD}}/6L$ at long distance. We simulate the case of $\theta = \pi$ and $\theta = \pi$. As shown in Fig. 4, the signature rate of [17] is higher than that of our protocol at short distance, but when distance between the two receivers is large, the signature rate will be severely limited by the low secret key rate of QKD in the symmetrization step. By contrast, our protocol decays much slower and has a significantly longer transmission distance.

In addition, the typical experimental parameters and corresponding signature rate of some recent QDS experiments are listed in Table. 1. This work shows a comparable performance with orthogonal encoding based protocol [21] even though the latter does not execute the symmetrization step. We remark that the symmetrization step is essential to the complete protocol, as demonstrated in experiments [21, 22].

V. CONCLUSION

In this paper, we have proposed a non-orthogonal encoding based efficient quantum digital signature protocol. A novel method called post-matching is applied, which can increase the signature rate from decaying with $\eta^2$ to $\eta$. Our protocol has a high signature rate and does not require the symmetrization operation thereby overcomes the major obstacles of existing QDS protocols. This pro-
TABLE I. Comparison of Parameters of Recent QDS Experiments

| Protocol         | Ref. [19] | Ref. [21] | Ref. [22] | Ref. [26] | Ref. [25] | This work |
|------------------|-----------|-----------|-----------|-----------|-----------|-----------|
| Repetition rate  | SARG04    | MDI       | MDI       | BB84      | BB84      | SARG04    |
| Transmission     | 75MHz     | 75MHz     | 1GHz      | 50MHz     | 1GHz      | 1GHz      |
| Security parameter | 102 km    | 55.6 km   | 50 km     | 280 km    | 125 km    | 125 km    |
| Signature        | 66840     | 149987    | 45        | 21407     | 22.7      | 14.9      |
| Symmetrization   | No need   | Yes       | Yes       | Non-exec  | Non-exec  | No need   |

Protocol can be directly implemented with current commercially available QKD devices. Therefore, it should be the preferred solution to the application of QDS. This work is a great step for the development of quantum network with QDS. Moreover, we believe the key idea of post-matching method has the potential to be applied in various cryptographic tasks that require to establish multiparty correlations, such as multiparty quantum communication [38].

**FUNDING**

National Natural Science Foundation of China (61801420); Key Research and Development Program of Guangdong Province (2020B0303040001); Fundamental Research Funds for the Central Universities.
[28] T.-Y. Wang, X.-Q. Cai, Y.-L. Ren, and R.-L. Zhang, Sci. Rep. 5, 9231 (2015).
[29] T.-Y. Wang, J.-F. Ma, and X.-Q. Cai, Quantum Information Processing 16, 19 (2017).
[30] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).
[31] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[32] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[33] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Sci. Rep. 10, 14312 (2020).
[34] K. Tamaki and H.-K. Lo, Phys. Rev. A 73, 010302 (2006).
[35] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, Sci. Rep. 6, 29482 (2016).
[36] H. Chernoff, Ann. Math. Stat. 23, 493 (1952).
[37] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A 89, 022307 (2014).
[38] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. 114, 090501 (2015).