Research Article | Vol. 29, No. 17 / 16 Aug 2021 / Optics Express 27661
Optics EXPRESS

Secure and practical multiparty quantum digital signatures

CHEN-XUN WENG,[1,2] YU-SHUO LU,[1,2] RUI-QI GAO,[1] YUAN-MEI XIE,[1] JIE GU,[1] CHEN-LONG LI,[1] BING-HONG LI,[1] HUA-LEI YIN,[1,3] AND ZENG-BING CHEN[1,4]

[1]*National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*
[2]*These authors contributed equally to this work*
[3]*hlyin@nju.edu.cn*
[4]*zbchen@nju.edu.cn*

Abstract: Quantum digital signatures (QDSs) promise information-theoretic security against repudiation and forgery of messages. Compared with currently existing three-party QDS protocols, multiparty protocols have unique advantages in the practical case of more than two receivers when sending a mass message. However, complex security analysis, numerous quantum channels and low data utilization efficiency make it intractable to expand three-party to multiparty scenario. Here, based on six-state non-orthogonal encoding protocol, we propose an effective multiparty QDS framework to overcome these difficulties. The number of quantum channels in our protocol only linearly depends on the number of users. The post-matching method is introduced to enhance data utilization efficiency and make it linearly scale with the probability of detection events even for five-party scenario. Our work compensates for the absence of practical multiparty protocols, which paves the way for future QDS networks.

1. Introduction

Digital signature can verify the authenticity of digital messages and has been widely applied in e-mail, e-commerce and software distribution [1]. As e-commerce becomes more and more significant in modern society, the need of unconditionally secure digital signatures against hacking attacks has arisen. Classical digital signatures offer security based on the computational complexity of mathematical problems [2–5]. However, the task of rapidly solving these mathematical problems becomes feasible when a quantum computer is available [6–10]. Fortunately, quantum digital signatures (QDSs) can offer information-theoretic security relying on quantum mechanics against adversaries who are supposed to have unbounded ability allowed by physics.

The first QDS protocol was proposed in 2001 [11], but there are some challenging requirements, such as secure quantum channels and long-term quantum memory. After that, the requirement of quantum memory was removed by converting the quantum signatures to classic information through quantum measurements, which makes QDS closer to real implementation [12–16]. Whereas, the security analyses of early protocols still rely on secure quantum channels where there is no eavesdropping. To further improve practicality, two independent QDS protocols without secure quantum channels were proposed and proved to be secure, which are based on non-orthogonal encoding [17] and orthogonal encoding [18], respectively. After these two protocols, numerous excellent achievements of QDS have been made theoretically and experimentally [19–35]. Protocols based on orthogonal encoding [18,19,33] need additional symmetrization step which results in extra channels. Recently, drawing on the experience of the four-state Scarani-Acin-Ribordy-Gisin 2004 quantum key distribution (SARG04 QKD) protocol

#433656 https://doi.org/10.1364/OE.433656
Journal © 2021 Received 9 Jun 2021; revised 15 Jul 2021; accepted 28 Jul 2021; published 11 Aug 2021

Optics EXPRESS

[36–41], a post-matching QDS protocol has been proposed based on non-orthogonal encoding [42]. It does not require additional symmetrization step and also achieves better performance than the original protocol [17].

Current QDS protocols mostly focus on three-party communication since the protocol involving more than two recipients will raise three major concerns. The first one is the increased number of quantum communication channels [43]. When extending orthogonal encoding protocol to multiparty scenarios, each pair of participants requires a quantum communication channel to symmetrize their secret keys. The M-party orthogonal encoding protocol requires $M(M-1)/2$ quantum channels. As M increases, it becomes more complex and less practical to implement. The second one is the poor data utilization efficiency leading to low signature rate if we expand the original non-orthogonal encoding protocol to multiparty scenarios. This is because the original non-orthogonal encoding protocol only consider coincidence detection events as valid events. For M-party protocol, it requires all detectors of $M-1$ recipients click. Let η be the probability that one recipient detector clicks. When the signer sends N quantum states to recipients, there are only $N\eta^{M-1}$ valid events, which is far from enough to perform multiparty protocols. Besides, complex security analysis is also a difficulty to be overcome because there exists a situation where some participants collude with each other to deceive others [44]. Although the security analysis of multi-party quantum digital signature schemes based on orthogonal encoding has made progress [45,46], it does not give an exact example and concrete simulation results.

In this paper, we propose a six-state three-party QDS protocol to enhance performance of signature rate and stability with the help of its higher bit error rate threshold compared with [42]. Furthermore, considering that three-photon or even four-photon components of six-state protocol can be used for the secure key, we extend this six-state protocol to four-party and five-party scenarios and overcome difficulties above, as shown in Fig. 1. According to our multiparty QDS framework, we simulate the performance of our three-party, four-party and five-party QDS and give a comparison among them. It is the first practical multiparty QDS framework and we provide security analysis.

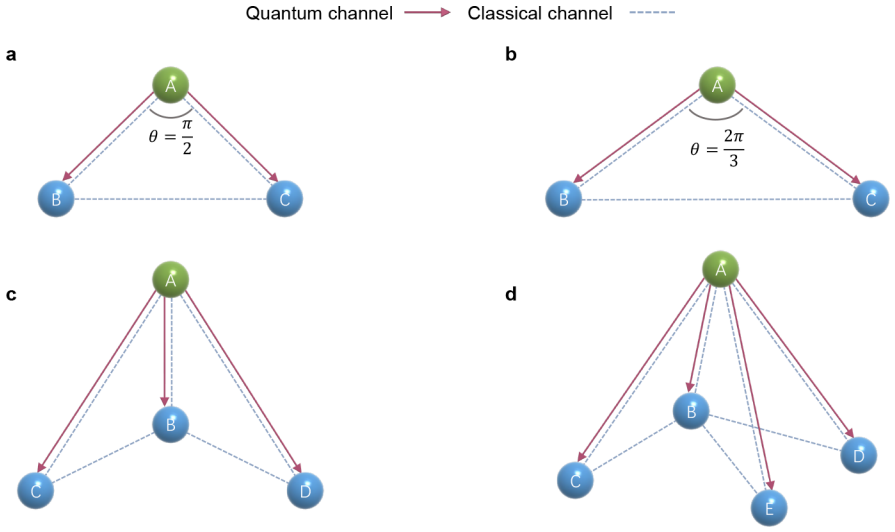

Fig. 1. Schematic diagrams of three-party, four-party and five-party protocol. The red line represents insecure quantum channel and the blue dash line is authenticated classical channel. θ is the angle between Alice-Bob and Alice-Charlie. **a.** Three-party protocol with $\theta = \frac{\pi}{2}$. **b.** Three-party protocol with $\theta = \frac{2\pi}{3}$. **c.** Four-party protocol. **d.** Five-party protocol.

Optics EXPRESS

2. Protocol description

Let us start by the common notation. The 'signer' Alice assigns any one of recipients as 'authenticator' and other recipients become 'verifiers' automatically. For simplicity, we always let Bob become the authenticator and other recipients become verifiers automatically. Note that in this article we consider the symmetric situation where the fiber lengths between Alice and any one of recipients we mentioned in the following are equal. We will introduce detailed security analysis in Methods. In Table 1, we give a concise description of the framework.

Table 1. Brief description of M-party

Key generation	Alice prepares $M-1$ different quantum state sequences and sends them to $M-1$ recipients respectively. All recipients measure quantum states they received in the X, Y or Z basis at random and announce all click events. All participants discard no-click data and keep click data to form their own strings. After that, they perform post-matching process and encode their processed data strings by our rule.
Estimation	Alice informs any verifier to randomly select a certain proportion of strings as test bits. The verifier announces the location of test bits and asks Alice to publicly announce the data information of test bits. The recipients estimate the mismatching rate of conclusive results between their own string and Alice's string.
Messaging	To sign one-bit message, Alice sends her own untested data string to Bob. Whether Bob accepts it depends on Bob's mismatching rate of conclusive results. If Bob accepts, Bob forwards it to all verifiers respectively. Whether verifiers accept it depends on their own mismatching rate. All participants negotiate whether aborting the protocol according to the majority voting principle.

Three-party protocol. We take three-participant scenario as an example and describe all processes in detail. Alice chooses Bob as authenticator and Charlie becomes verifier. In our protocol, there are insecure quantum channels connecting Alice with Bob and Alice with Charlie. Moreover, there are authenticated classical channels between any two of three participants. There are six quantum states: $|+x\rangle$, $|-x\rangle$, $|+y\rangle$, $|-y\rangle$, $|+z\rangle$, $|-z\rangle$. $|\pm x\rangle$ are the eigenstates of Pauli X operator. $|\pm y\rangle$ are the eigenstates of Pauli Y operator. $|\pm z\rangle$ are the eigenstates of Pauli Z operator. These six states can be arranged into the 12 sets: $\{|\omega_1 x\rangle, |\omega_2 y\rangle\}$, $\{|\omega_3 y\rangle, |\omega_4 z\rangle\}$ and $\{|\omega_5 z\rangle, |\omega_6 x\rangle\}$, where $\omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6 \in \{+,-\}$. The first state in each set is encoded with bit value 0 and the second is encoded with bit value 1.

There are three steps in our QDS protocol: key generation, estimation and messaging.

In the key generation step, Alice uses phase-randomized weak coherent-state source to prepare the six states. For each possible message $m = 0$ and $m = 1$, Alice prepares two different unrelated sequences of quantum states $A_{B,m}$ and $A_{C,m}$ with length N respectively. Each state is randomly selected from the six states with the same probability by Alice. We denote the light intensity as λ ($\lambda \in \{\mu, \nu, 0\}$). Each quantum state is prepared with the intensity μ, ν or 0 and the corresponding possibility p_μ, p_ν, p_0 respectively. Alice sends sequences $A_{B,0}$, $A_{B,1}$ to Bob and $A_{C,0}$, $A_{C,1}$ to Charlie through insecure quantum channels. Bob and Charlie receive the sequences and then measure each quantum state in the X, Y or Z basis at random. Bob (Charlie) announces all the click events in $A_{B,m}$ ($A_{C,m}$) through authenticated classical channel, denoted as $S_{B,m}$ ($S_{C,m}$). Afterwards, Alice discards no-click data and keeps click data of length n to form strings $S_{AB,m}$ and $S_{AC,m}$. Alice publicly announces intensity information of all pulses and all three participants divide their remaining data strings into μ-string, ν-string and 0-string according to the intensity information. For instance, Bob divides $S_{B,m}$ into $S^{\mu}_{B,m}$, $S^{\nu}_{B,m}$ and $S^{0}_{B,m}$ according to the public intensity information.

The three participants perform post-matching method [42]. Alice takes the order of quantum states in $S^{\lambda}_{AB,m}$ as a reference and changes the order of $S^{\lambda}_{AC,m}$ to make it same as the order of

Optics EXPRESS

$S^{\lambda}_{AB,m}$. Alice requests Charlie to change the order of $S^{\lambda}_{C,m}$ into the same order. For instance, if $S_{AB,m} = \{s^1_{AB,m}, s^2_{AB,m}, s^3_{AB,m}, s^4_{AB,m}, s^5_{AB,m}, s^6_{AB,m}\} = \{|+x\rangle, |-x\rangle, |+y\rangle, |-y\rangle, |+z\rangle, |-z\rangle\}$, $S_{AC,m} = \{s^1_{AC,m}, s^2_{AC,m}, s^3_{AC,m}, s^4_{AC,m}, s^5_{AC,m}, s^6_{AC,m}\} = \{|+y\rangle, |+z\rangle, |-x\rangle, |-y\rangle, |-z\rangle, |+x\rangle\}$, Alice changes initial $S_{AC,m}$ into $S'_{AC,m}$, where $S'_{AC,m} = \{s^6_{AC,m}, s^3_{AC,m}, s^1_{AC,m}, s^4_{AC,m}, s^2_{AC,m}, s^5_{AC,m}\}$. She also informs Charlie to change the order of elements in $S_{C,m}$ into $S'_{C,m}$, where $S'_{C,m} = \{s^6_{C,m}, s^3_{C,m}, s^1_{C,m}, s^4_{C,m}, s^2_{C,m}, s^5_{C,m}\}$. Note that $S_{C,m}$ is the measurement result of $S_{AC,m}$, so $S'_{C,m}$ is the measurement result of $S'_{AC,m}$. As a result, although Alice sends two different quantum-state sequences, after post-matching process, two identical sequences $S_{AB,m}$ and $S'_{AC,m}$ are obtained by Bob and Charlie respectively. We illustrate our rule to generate logic bits as follows. For each quantum state sent, Alice randomly chooses one of 12 sets so that the state she sent is one of the two states in the set. Then she assigns the quantum state to this set. When the measurement outcome is orthogonal to any quantum state of the assigned set, the receiver gets a conclusive result encoded with logic bit 0 (the first state) or logic bit 1 (the second state). Otherwise, the receiver gets an inconclusive result denoted as '$\perp$'. They do not announce whether the results are conclusive or inconclusive. Following the rule, all of three participants encode their data strings with $K^{\lambda}_{A,m}$, $K^{\lambda}_{B,m}$ and $K^{\lambda}_{C,m}$ respectively. The function of binary logic is to quantify the mismatching rate of conclusive results between Alice's binary encoded data string and each recipient's binary encoded data string in the estimation step, which is used in the later security analysis.

Here is the example of binary encoding process. The recipients randomly choose X, Y or Z basis to measure each quantum state Alice sent. Alice should publicly announce which of the 12 sets she picked for each state she sent. The set Alice picked should include the state she sent. The recipients will get a conclusive result if any one of the two states in the set is the eigenstate of the basis the recipient chose to measure. For example, Alice sends the state $|+x\rangle$. She will assign it to any one of $\{|+x\rangle, |+y\rangle\}$, $\{|+x\rangle, |-y\rangle\}$, $\{|+z\rangle, |+x\rangle\}$ and $\{|-z\rangle, |+x\rangle\}$. When she assigns it to $\{|+x\rangle, |+y\rangle\}$ and Bob's measurement outcome is $|-y\rangle$ ($|-x\rangle$), Bob will get a conclusive result with logic bit value 0 (1).

In the estimation step, we use superscript c to denote conclusive results, u to denote untested bits, t to denote test bits. The three participants estimate the bit error rate of single-photon pair components with decoy-state method in their μ strings. Alice announces the information of intensity $\lambda = \nu$ and $\lambda = 0$ publicly. Alice informs Charlie to randomly select a certain proportion, denoted as t, of μ strings as test bits. Charlie announces the location of test bits and asks Alice to publicly announce the data information of test bits. Denote the mismatching rate of conclusive results between $K^t_{A,m}$ and $K^t_{B,m}$ (between $K^t_{A,m}$ and $K^t_{C,m}$) as E^{ct}_B (E^{ct}_C). Moreover, Bob and Charlie calculate the proportion of conclusive results in $K_{B,m}$ and $K_{C,m}$ respectively, denoted as P^c_B and P^c_C. If either of them deviates greatly from the ideal value $\frac{1}{6}$, they also abort the protocol. Afterwards, all of them throw away the test bits and conserve the untested bits of μ strings with remaining length $(1-t)n_\mu$.

In the messaging step, to sign one-bit message m, Alice sends $\left\{m, K^u_{A,m}\right\}$ to Bob. Bob checks the mismatching rate of conclusive results E^{cu}_B between $K^u_{A,m}$ and $K^u_{B,m}$. If $E^{cu}_B \leq T_a$ (T_a is the authentication security threshold), Bob accepts the message. Otherwise, he rejects the message and aborts the protocol. When Bob accepts the message from Alice, he forwards $\left\{m, K^u_{A,m}\right\}$ to verifier Charlie. After that, Charlie checks the mismatching rate of conclusive results E^{cu}_C between $K^u_{A,m}$ and $K^u_{C,m}$. If $E^{cu}_C \leq T_v$ (T_v is the verification security threshold), Charlie accepts the message. Otherwise, Charlie rejects the message and aborts the protocol.

We define the signature rate as $R := \frac{1}{2N}$, where $2N$ is the minimum number of pulses required to securely sign a one-bit message. We define that it is secure enough to sign a 1-bit message when the robustness ε_{rob}, the probability of successful forgery ε_{for}, the probability of successful

Optics EXPRESS

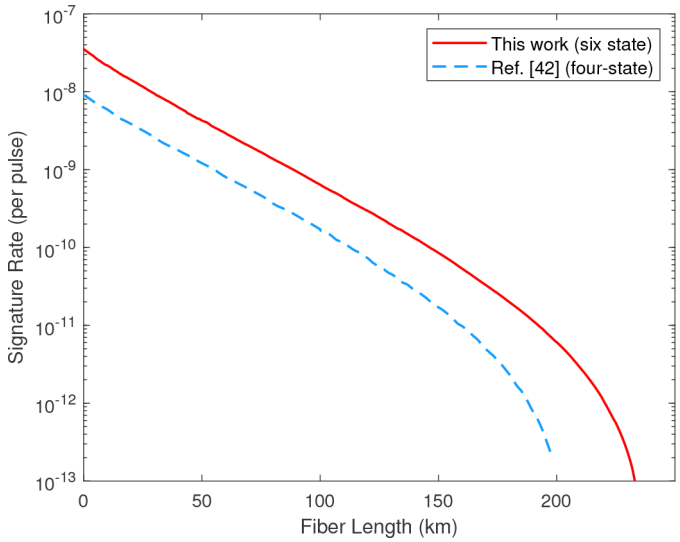

Fig. 2. Comparison of performance between our three-party protocol and four-state protocol [42]. The detection efficiency is 93%. The dark counting rate is 1×10^{-7}. The basis misalignment rate is 0.50%. The loss coefficient of fiber is 0.16 dB/km. As the fiber length increases, the superiority of our protocol becomes more apparent. The signature rate of our protocol is at least 400% higher than that of [42] in this case.

repudiation ε_{rep}, the failure probability of the Chernoff bound ϵ_1 and the failure probability of random sampling without replacement ϵ_2 do not exceed their thresholds respectively.

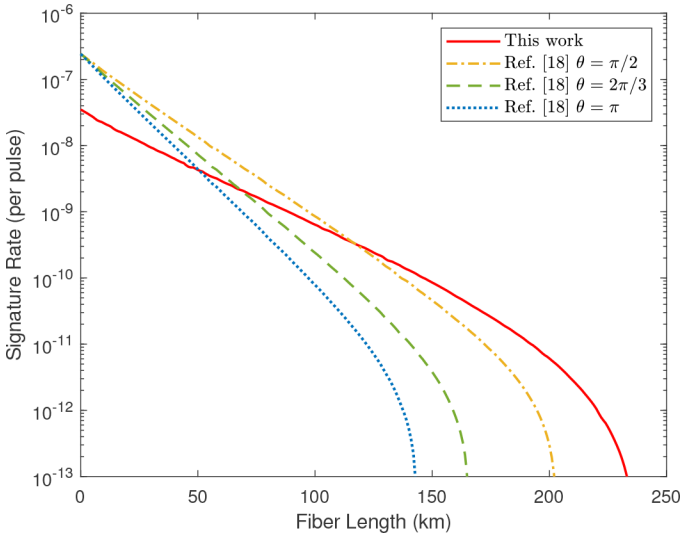

Fig. 3. Comparison of performance between our three-party protocol and orthogonal encoding protocol [18]. We simulate two protocols under the same experimental parameters. The signature rate of our protocol is lower at short distance. However, it decays more slowly than orthogonal encoding protocol and shows better performance especially at long distance. In this case, our protocol has a longer transmission distance.

Optics EXPRESS

As shown in Fig. 2, we simulate the four-state protocol of [42] to compare it with our six-state protocol. The performance of our protocol is better than that of [42]. For example, when the fiber length is 150 km, the original four-state protocol requires about 2.93×10^{10} pulses to sign a one-bit message. However, under the same conditions our six-state protocol only needs about 5.85×10^{9} pulses. When the fiber length is 150 km, the signature rate of our protocol is approximately 500% higher than four-state . Moreover, we also simulate the performance of orthogonal encoding based protocol with symmetrization step in [18] to compare with our protocol as shown in Fig. 3. We denote the angle between Alice-Bob and Alice-Charlie as θ. Denote the distance between Alice and Bob (Charlie) as D_{AB} (D_{AC}) and the distance between Bob and Charlie as D_{BC}. For a symmetric case, $D_{AB} = D_{AC}$ and $D_{BC} = 2D_{AB} \sin\theta/2$. D_{BC} increases as θ gets larger. When θ is close to π , the transmission distance of QKD (D_{BC}) increases much faster than D_{AB}. Detailed information can be found in Ref. [42]. Define the effective signature rate as $R_{eff} := \max\{\frac{1}{2N}, \frac{R_{QKD}}{6L}\}$, where L is the length of generated key and R_{QKD} is the secret key rate of QKD. R_{QKD} is simulated by the key rate formula of [47]. We simulate three cases of $\theta = \pi$, $\theta = \frac{2\pi}{3}$ and $\theta = \frac{\pi}{2}$. Our protocol has a longer transmission distance and greater performance of signature rate especially at long distance in these cases where the signature rate of our protocol decays more slowly. We also simulate our protocol's performance under different dark counting rates and different basis misalignment rates as shown in Fig. 4 and Fig. 5 respectively. From two figures, we can see that our protocol shows obviously high error rate tolerance and stability against noise.

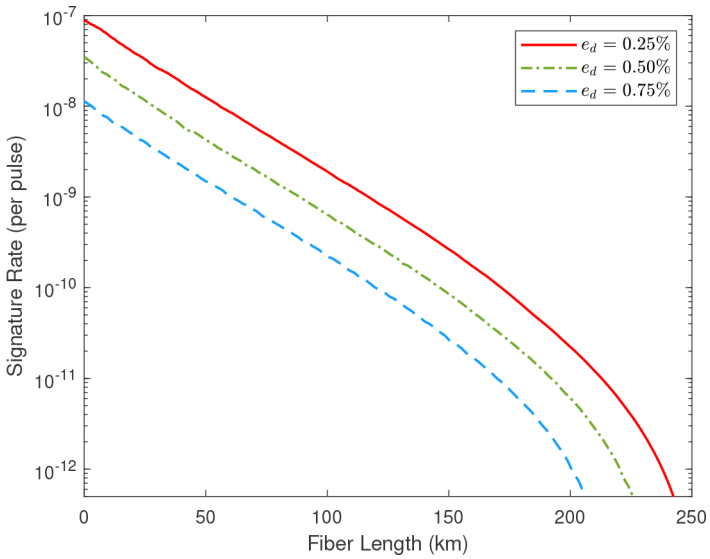

Fig. 4. Optimal signature rate of three-party protocol with the same dark counting rate $p_d = 1 \times 10^{-7}$ under different basis misalignment rate.

Four-party QDS protocol. In our four-party protocol, there are 'signer' Alice, 'authenticator' Bob, 'verifier' Charlie and 'verifier' David. Their positions are shown in Fig. 1(c). The operation among Alice, Bob and Charlie are the same as three-party protocol, which we will not describe in detail here. We focus on the difference due to the new participant 'verifier' David instead.

For each possible message $m = 0$ and $m = 1$, following the rule of generating logic bits, David encodes his data strings with $K^{\lambda}_{D,m}$ in the key generation step.

In the estimation step, the four participants estimate the bit error rate of triple-photon components with decoy-state method in their μ strings. Alice announces all information of intensity $\lambda = \nu$ and $\lambda = 0$. Then Alice informs any one of verifiers to randomly select a proportion

Optics EXPRESS

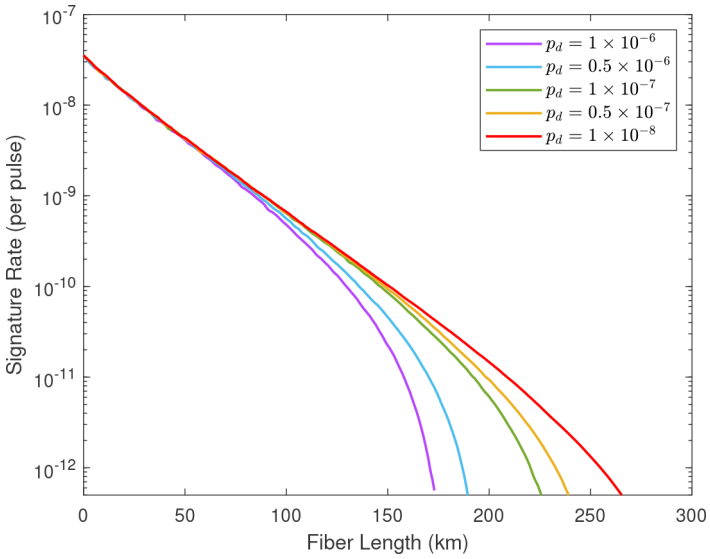

Fig. 5. Optimal signature rate of three-party protocol with the same basis misalignment rate $e_d = 0.5\%$ under different dark counting rates.

of μ strings as test bits. All verifiers announce the location of their test bits respectively and request Alice to announce the data information of test bits publicly. Denote the mismatching rate of conclusive results between $K^t_{A,m}$ and $K^t_{B,m}$ as E^{ct}_B, the mismatching rate of conclusive results between $K^t_{A,m}$ and $K^t_{C,m}$ as E^{ct}_C and the mismatching rate of conclusive results between $K^t_{A,m}$ and $K^t_{D,m}$ as E^{ct}_D. Moreover, Bob, Charlie and David calculate the proportion of conclusive results in $K_{B,m}$, $K_{C,m}$ and $K_{D,m}$ respectively, denoted as P^c_B, P^c_C and P^c_D.

To sign one-bit message m, Alice sends $\left\{m, K^u_{A,m}\right\}$ to Bob. Bob checks the mismatching rate of conclusive results E^{cu}_B between $K^u_{A,m}$ and $K^u_{B,m}$. If $E^{cu}_B \leq T_a$, Bob accepts the message. Otherwise, he rejects the message and aborts the protocol. When Bob accepts the message from Alice, he forwards $\left\{m, K^u_{A,m}\right\}$ to Charlie and David respectively. After that, Charlie checks the mismatching rate of conclusive results E^{cu}_C between $K^u_{A,m}$ and $K^u_{C,m}$. If $E^{cu}_C \leq T_{Cv}$ (T_{Cv} is the verification security threshold of Charlie), Charlie accepts the message. Otherwise, Charlie rejects the message. David checks the mismatching rate of conclusive results E^{cu}_D between $K^u_{A,m}$ and $K^u_{D,m}$. If $E^{cu}_D \leq T_{Dv}$ (T_{Dv} is the verification security threshold of David), David accepts the message. Otherwise, David rejects the message. Either of Charlie and David rejects the message means that the protocol will be aborted. All participants negotiate whether aborting the protocol or not according to the majority voting principle.

Five-party QDS protocol. When it comes to our five-party protocol, there are five participants 'signer' Alice, 'authenticator' Bob, 'verifier ' Charlie, 'verifier' David and 'verifier' Emery. Their positions are shown in Fig. 1(d). The processes among Alice, Bob, Charlie and David are the same as the four-party protocol. We only focus on the operation involving Emery here.

In the key generation step, Emery encodes his data strings with $K^{\lambda}_{E,m}$ following the process as we described above.

In the estimation step, the five participants estimate the bit error rate of four-photon component with decoy-state method in their μ strings. Alice announces the information of intensity $\lambda = \nu$ and $\lambda = 0$. Alice informs any one verifier to randomly select a certain proportion of μ strings as test bits. The participants estimate their mismatch rate of conclusive results. Denote the mismatching rate of conclusive results between $K^t_{A,m}$ and $K^t_{E,m}$ as E^{ct}_E. Moreover, Emery calculates

Optics EXPRESS

the proportion of conclusive results in $K_{E,m}$, denoted as P_E^c. If any one of Bob, Charlie, David and Emery deviates greatly from the ideal value $\frac{1}{6}$, they abort the protocol. Afterwards, all of them throw away the test bits and keep the untested bits of μ strings with remaining length $(1-t)n_\mu$.

In the messaging step, Alice sends $\left\{m, K_{A,m}^u\right\}$ to Bob in order to sign one-bit message m. Bob checks E_B^{cu}. If $E_B^{cu} \leq T_a$, Bob accepts the message. Otherwise, he rejects the message and aborts the protocol. When Bob accepts the message from Alice, he forwards $\left\{m, K_{A,m}^u\right\}$ to Charlie, David and Emery respectively. Emery checks the mismatching rate of conclusive results E_E^{cu} between $K_{A,m}^u$ and $K_{E,m}^u$. If $E_E^{cu} \leq T_{Ev}$ (T_{Ev} is the verification security threshold of Emery), Emery accepts the message. Otherwise, Emery rejects. All participants negotiate whether aborting the protocol or not according to the majority voting principle.

3. Security analysis

Our security analysis follows [17] and [42]. We build the framework for M-party (M=3, 4, 5) protocol about three security criteria: robustness, security against forgery and security against repudiation. Here, we apply majority voting principle to solve dispute. For four-party protocol, there are at most one dishonest participant. Any two of participants making the wrong decision leads to successful attack. For five-party protocol, we should consider the colluding attack where there are two dishonest participants. We can assume Emery is a fixed dishonest player and he will collude with the other dishonest participant (Alice or Bob). Emery always unconditionally supports his partner. In other words, Charlie and David must make the same correct decision. This situation is equivalent to the four-party scenario above where there exists only one dishonest participant among Alice, Bob, Charlie and David.

The upper bound and lower bound of expected value of parameter a can be given by a variant of Chernoff bound [48]: $\overline{a}^* = a + \beta + \sqrt{2\beta a + \beta^2}$ and $\underline{a}^* = a - \frac{\beta}{2} - \sqrt{2\beta a + \frac{\beta^2}{4}}$ where $\beta = \ln \frac{1}{\varepsilon_1}$ and ϵ_1 is the failure probability of the Chernoff bound. We use k to denote k-photon component, where $k = M - 1$.

(1) Robustness Robustness (ε_{rob}) represents the probability that the protocol is aborted when the antagonist is inactive. In messaging step, Bob does not accept the message if $E_B^{cu} > T_a$. We can quantify robustness by random sampling without replacement theorem [48] in finite sample case.

(2) Security against forgery Forgery attack means Bob wishes that more than half of verifiers would accept the forwarded message forged by Bob $\{m, K_{BF}\}$. In this case, Bob needs to obtain as much information as he can about quantum states that all verifiers receive, like an eavesdropper in SARG04 QKD protocol [21,36,38,41].

All positions of recipients are equal. Without loss of generality, we first consider the probability that Charlie is deceived by Bob. We exploit the decoy state method [49–52] to estimate the bit error rate e_b of k-photon component.

Considering the process where Alice sends pulses to all recipients, we have

$$s_{C1}^{c\mu^*} \geq \frac{p_\mu e^{-\mu}}{\nu(\mu-\nu)}\left(\mu^2 e^\nu \frac{\underline{n}_{C\nu}^{c^*}}{p_\nu} - \nu^2 e^\mu \frac{\overline{n}_{C\mu}^{c^*}}{p_\mu} + (\nu^2-\mu^2)\frac{\underline{n}_{C0}^{c^*}}{p_0}\right), \tag{1}$$

where $s_{C1}^{c\mu^*}$ is the number of conclusive single-photon events in Charlie's μ string.

$$s_{Q1}^{\mu^*} \geq \frac{p_\mu e^{-\mu}}{\nu(\mu-\nu)}\left(\mu^2 e^\nu \frac{\underline{n}_{Q\nu}^{*}}{p_\nu} - \nu^2 e^\mu \frac{\overline{n}_{Q\mu}^{*}}{p_\mu} + (\nu^2-\mu^2)\frac{\underline{n}_{Q0}^{*}}{p_0}\right), \tag{2}$$

$$s_{Q1}^{\mu^*} \leq \frac{p_\mu \mu e^{-\mu}}{\nu}\left(e^\nu \frac{\overline{n}_{Q\nu}^{*}}{p_\nu} - \frac{\underline{n}_{Q0}^{*}}{p_0}\right), \tag{3}$$

Optics EXPRESS

where $Q \in \Omega$ and

$$\Omega = \begin{cases} \{B\} & \text{if M=3,} \\ \{B, D\} & \text{if M=4,} \\ \{B, D, E\} & \text{if M=5,} \end{cases} \tag{4}$$

and $s_{Q1}^{\mu^*}$ is the number of single-photon events in Q's μ strings. Therefore, we have

$$s_{Ck}^{c\mu^*} \geq \underline{s}_{C1}^{c\mu^*} \times \prod_{Q\in\Omega} \frac{s_{Q1}^{\mu^*}}{\overline{n}_{Q\mu}^*}, \tag{5}$$

where $s_{Ck}^{c\mu^*}$ is the number of events that all recipients receive a single-photon in μ string and Charlie has a conclusive result simultaneously. For example, when it comes to four-party, $s_{C3}^{c\mu^*} \geq \underline{s}_{C1}^{c\mu^*} \times \frac{s_{B1}^{\mu^*}}{\overline{n}_{B\mu}^*} \times \frac{s_{D1}^{\mu^*}}{\overline{n}_{D\mu}^*}$.

We also have

$$t_{C1}^{c\mu^*} \leq \frac{p_\mu \mu e^{-\mu}}{\nu}(e^{\nu}\frac{\overline{m}_{C\nu}^{c^*}}{p_\nu} - \frac{\underline{n}_{C0}^{c^*}}{2p_0}), \tag{6}$$

and

where $t_{C1}^{c\mu^*}$ is the number of single-photon error events of Charlie's conclusive results in μ string with respect to Alice. We can get

$$t_{Ck}^{c\mu^*} \leq \overline{t}_{C1}^{c\mu^*} \times \prod_{Q\in\Omega} \frac{\overline{s}_{Q1}^{\mu^*}}{\underline{n}_{Q\mu}^*} \tag{7}$$

where $t_{Ck}^{c\mu^*}$ is the number of events that all recipients receive a single-photon in μ string, Charlie has a conclusive result and his classic bit mismatches with Alice's.

Therefore, the bit error rate e_b can be given by $e_b = t_{Ck}^{c\mu^*}/s_{Ck}^{c\mu^*}$.

The relationship between phase error rate e_p and bit error rate e_b [17] in six-state SARG04 protocol is

$$e_p = \begin{cases} \frac{4-\sqrt{2}}{4} + \frac{3}{2\sqrt{2}}e_b & \text{if M=3,} \\ \frac{1}{4} + \frac{3}{4}e_b & \text{if M=4,} \\ \min\{xe_b + f(x)\}, \forall x & \text{if M=5,} \end{cases} \tag{8}$$

where $f(x) = \frac{6-4x+\sqrt{6-12\sqrt{2}x+16x^2}}{12}$.

E_{BFk}^* can be given by $H(E_{BFk}^*) = 1 - I_B = 1 - H(e_p|e_b)$, where $H(e_p|e_b)$ is the conditional Shannon entropy function, I_B is mutual information provided by [17] and E_{BFk}^* is the expected value of minimum mismatching rate of conclusive results of the k-photon component between correct $K_{A,m}^u$ and forged $K_{BF,m}^u$.

We employ Chernoff Bound [53] and the probability of successful forgery (ε_{for}) can be given by

$$\varepsilon_{for} = \exp\left[-\frac{(E_{BFk}^* - T_{vk})^2}{2E_{BFk}^*} n_k^{cu}\right], \tag{9}$$

where $T_{vk} = T_v n^{cu}/n_k^{cu}$ is the error rate threshold of k-photon component, $n^{cu} = (1-t)n_\mu^c$ is the number of conclusive results in $K_{C,m}^u$ and $n_k^{cu} = (1-t)s_{Ck}^{c\mu}$ is the number of k-photon component

Optics EXPRESS

in $K^u_{C,m}$. Note that ϵ_{for} is determined by the probability of deceiving the most vulnerable recipient. Therefore,

$$T_v = \begin{cases} T_{Cv} & \text{if M=3,} \\ \min\{T_{Cv}, T_{Dv}\} & \text{if M=4,} \\ \min\{T_{Cv}, T_{Dv}, T_{Ev}\} & \text{if M=5.} \end{cases} \tag{10}$$

(3) Security against repudiation Alice repudiates successfully when Bob accepts the message and more than half of the verifiers refuse to accept it. The probability of repudiation ε_{rep} can be given by

$$\varepsilon_{rep} = \exp\left[-\frac{\left(A - P^c_B T_a\right)^2}{2A} n^u\right]. \tag{11}$$

A is the solution of the following equation:

$$\frac{\left[P^c_C T_v - P^c_C\left(\frac{\overline{\Delta}^{cu}}{n^{cu}} + \frac{A}{P^c_B}\right)\right]^2}{3P^c_C\left(\frac{\overline{\Delta}^{cu}}{n^{cu}} + \frac{A}{P^c_B}\right)} = \frac{(A - P^c_B T_a)^2}{2A}, \tag{12}$$

with $P^c_B T_a < A < P^c_B\left(T_v - \frac{\overline{\Delta}^{cu}}{n^{cu}}\right)$. $\overline{\Delta}^{cu}$ can be given by

$$\overline{\Delta}^{cu} = \begin{cases} \overline{\Delta}^{cu}_{BC} & \text{if M=3,} \\ \max\{\overline{\Delta}^{cu}_{BC}, \overline{\Delta}^{cu}_{BD}\} & \text{if M=4,} \\ \max\{\overline{\Delta}^{cu}_{BC}, \overline{\Delta}^{cu}_{BD}, \overline{\Delta}^{cu}_{BE}\} & \text{if M=5,} \end{cases} \tag{13}$$

where $\overline{\Delta}^{cu}_{BC}$ is the relative Hamming distance between E^{cu}_B and E^{cu}_C, $\overline{\Delta}^{cu}_{BD}$ is the relative Hamming distance between E^{cu}_B and E^{cu}_D, $\overline{\Delta}^{cu}_{BE}$ is the relative Hamming distance between E^{cu}_B and E^{cu}_E.

Therefore, the total security can be given by

$$\varepsilon_{tot} = \begin{cases} 11\epsilon_1 + \epsilon_2 + \varepsilon_{rob} + \varepsilon_{for} + \varepsilon_{rep} & \text{if M=3,} \\ 17\epsilon_1 + \epsilon_2 + \varepsilon_{rob} + \varepsilon_{for} + \varepsilon_{rep} & \text{if M=4,} \\ 23\epsilon_1 + \epsilon_2 + \varepsilon_{rob} + \varepsilon_{for} + \varepsilon_{rep} & \text{if M=5,} \end{cases} \tag{14}$$

where ϵ_1 is the failure probability of the Chernoff bound and ϵ_2 is the failure probability of random sampling without replacement.

In our simulation, we set the security bounds as $\varepsilon_{tot} \leq 10^{-9}$, $\varepsilon_{for} \leq 10^{-10}$, $\varepsilon_{rob} \leq 10^{-10}$, $\varepsilon_{rep} \leq 10^{-10}$ and $\varepsilon_1 = \varepsilon_2$.

Note that as shown in Fig. 6, expanding the QDS framework to an increasing number of users implies that the signature rate R decreases more rapidly than just linearly as the number of parties increases. That is because, for M-party protocol, only the $M-1$ photon component can be considered to be secure when we consider security against forgery. That means the addition of a new user requires an extra single photon reducing the efficiency which makes signature rate get lower as we pointed in Eq. (5). Additionally, the relationships between phase error rate e_p and bit error rate e_b of $M-1$ photon component in six-state SARG04 protocol are different as shown in Eq. (8). That will also influence the signature rate of multiparty QDS.

Furthermore, the increase of system loss and the decrease of detection efficiencies will both lead to the decrease of valid detection events when sending the same number of pulses. That means the statistical fluctuation will increase resulting in the increase of the probability of successful repudiation and forgery. Moreover, the enhancement of security constraint also results in the statistical fluctuation increasing. Therefore, more pulses are required to keep the protocol safe, i.e., the signature rate will be lower.

Optics EXPRESS

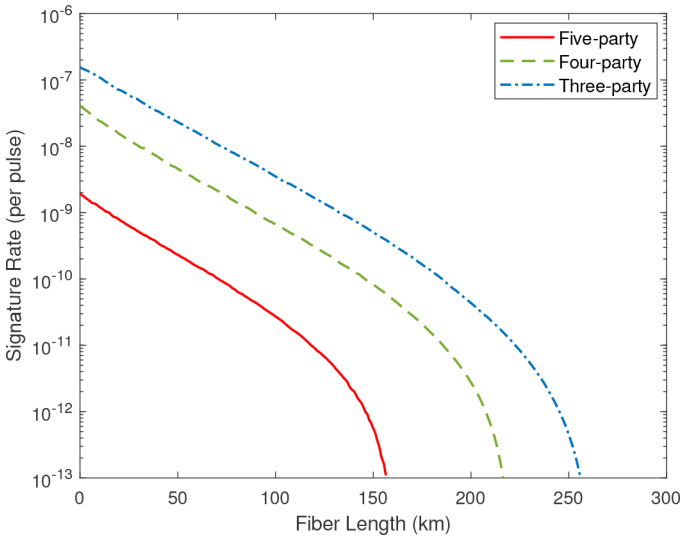

Fig. 6. The performance of three-party, four-party and five-party protocol under the same basis misalignment rate $e_d = 0.1\%$. With the help of post-matching method, extending three-party to four-party or even five-party scenario is feasible because our data utilization efficiency is highly improved.

4. Conclusion

In summary, we have presented a practical QDS framework that consists of multiple participants. In our three-party protocol, signature rate, secure transmission distance and error tolerance achieve better performance because of higher error rate threshold. Additionally, as shown in Fig. 6, our protocol can be extended to multiparty scenarios with great performance. In our simulation, when the basis misalignment rate $e_d = 0.1\%$ and dark counting rate $p_d = 1 \times 10^{-7}$, our three-party, four-party and five-party QDS protocols can reach the transmission distance of 265 km, 220 km and 156 km respectively. When the fiber length is 150 km, the signature rates of three-party, four-party and five-party are 5.1×10^{-10}, 8.3×10^{-11} and 5.6×10^{-13} respectively. As shown in Fig. 4, the signature rate does not decrease dramatically as e_d increases, showing the great fault tolerance. For example, when fiber length is 150 km, the signature rates are 2.7×10^{-10}, 8.5×10^{-11} and 2.7×10^{-11} under $e_d = 0.25\%$, 0.50% and 0.75% respectively.

The insurmountable barrier for original non-orthogonal encoding protocol to realize multiparty QDS protocol is low data utilization efficiency due to the requirement of coincidence detection. But our M-party protocol perfectly overcome this barrier because we can highly increase data utilization efficiency from $O(\eta^{M-1})$ to $O(\eta)$ with post-matching method, resulting in pronounced improvement of signature rate. Compared with orthogonal encoding protocol, our multiparty protocols are concise and maneuverable since our M-party protocol only needs $M - 1$ quantum channels as we shown in Fig. 1. The requirement of fewer quantum channels is a noticeable advantage of our QDS framework.

Also, in our work, we have presented security analysis of generalized multiparty QDS framework. These multiparty QDS protocols promise robustness, security against forgery and security against repudiation. We also solved the complex problem of colluding attack existing in the five-party scenario which never happens in three-party QDS by majority voting. This work provides specific ideas for practical multiparty QDS protocol. It will be interesting to apply ideas of our QDS framework to realize large-scale QDS networks in the near future.

Funding. National Natural Science Foundation of China (61801420); Key-Area Research and Development Program

Optics EXPRESS

of Guangdong Province (2020B0303040001); Fundamental Research Funds for the Central Universities (020414380182).

Disclosures. The authors declare no conflicts of interest.

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. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory **22**(6), 644–654 (1976).
2. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**(2), 120–126 (1978).
3. M. Rabin, "Digitalized signatures," *Foundations of Secure Computation* pp. 155–168 (1978).
4. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory **31**(4), 469–472 (1985).
5. D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," IJIS **1**(1), 36–63 (2001).
6. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, (IEEE, 1994), pp. 124–134.
7. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Rev. **41**(2), 303–332 (1999).
8. M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," Phys. Today **54**, 60 (2001).
9. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Yuezhen Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," Nature **574**(7779), 505–510 (2019).
10. H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "Quantum computational advantage using photons," Science **370**, 1460–1463 (2020).
11. D. Gottesman and I. Chuang, Quantum digital signatures, arXiv preprint quant-ph/0105032 (2001).
12. 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**(1), 1174 (2012).
13. V. Dunjko, P. Wallden, and E. Andersson, "Quantum digital signatures without quantum memory," Phys. Rev. Lett. **112**(4), 040502 (2014).
14. R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of quantum digital signatures without the requirement of quantum memory," Phys. Rev. Lett. **113**(4), 040502 (2014).
15. P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components," Phys. Rev. A **91**(4), 042304 (2015).
16. C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, "Free-space quantum signatures using heterodyne measurements," Phys. Rev. Lett. **117**(10), 100503 (2016).
17. H.-L. Yin, Y. Fu, and Z.-B. Chen, "Practical quantum digital signature," Phys. Rev. A **93**(3), 032316 (2016).
18. R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," Phys. Rev. A **93**(3), 032325 (2016).
19. I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, "Measurement-device-independent quantum digital signatures," Phys. Rev. A **94**(2), 022328 (2016).
20. T. Shang, Q. Lei, and J. Liu, "Quantum random oracle model for quantum digital signature," Phys. Rev. A **94**(4), 042314 (2016).
21. 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, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan, "Experimental quantum digital signature over 102 km," Phys. Rev. A **95**(3), 032334 (2017).
22. R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, M. Sasaki, E. Andersson, and G. S. Buller, "Experimental demonstration of quantum digital signatures over 43 db channel loss using differential phase shift quantum key distribution," Sci. Rep. **7**(1), 3235 (2017).
23. Y.-G. Yang, Z.-C. Liu, J. Li, X.-B. Chen, H.-J. Zuo, Y.-H. Zhou, and W.-M. Shi, "Theoretically extensible quantum digital signature with starlike cluster states," Quantum Inf. Process. **16**(1), 12 (2017).
24. H.-L. Yin, W.-L. Wang, Y.-L. Tang, Q. Zhao, H. Liu, X.-X. Sun, W.-J. Zhang, H. Li, I. V. Puthoor, L.-X. You, E. Andersson, Z. Wang, Y. Liu, X. Jiang, X. Ma, Q. Zhang, M. Curty, T.-Y. Chen, and J.-W. Pan, "Experimental

Optics EXPRESS

measurement-device-independent quantum digital signatures over a metropolitan network," Phys. Rev. A **95**(4), 042338 (2017).
25. G. Roberts, M. Lucamarini, Z. Yuan, J. Dynes, L. Comandar, A. Sharpe, A. Shields, M. Curty, I. Puthoor, and E. Andersson, "Experimental measurement-device-independent quantum digital signatures," Nat. Commun. **8**(1), 1098 (2017).
26. 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**(3), 034033 (2018).
27. M. Thornton, H. Scott, C. Croal, and N. Korolkova, "Continuous-variable quantum digital signatures over insecure channels," Phys. Rev. A **99**(3), 032341 (2019).
28. 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, X.-Y. Zhou, G.-C. Guo, and Z.-F. Han, "Practical quantum digital signature with a gigahertz bb84 quantum key distribution system," Opt. Lett. **44**(1), 139–142 (2019).
29. W. Qu, Y. Zhang, H. Liu, T. Dou, J. Wang, Z. Li, S. Yang, and H. Ma, "Multi-party ring quantum digital signatures," J. Opt. Soc. Am. B **36**(5), 1335–1341 (2019).
30. H. Zhang, X.-B. An, C.-H. Zhang, C.-M. Zhang, and Q. Wang, "High-efficiency quantum digital signature scheme for signing long messages," Quantum Inf. Process. **18**(1), 3 (2019).
31. 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**(7), 1711–1714 (2020).
32. C.-M. Zhang, Y. Zhu, J.-J. Chen, and Q. Wang, "Practical quantum digital signature with configurable decoy states," Quantum Inf. Process. **19**(5), 151 (2020).
33. C.-H. Zhang, Y.-T. Fan, C.-M. Zhang, G.-C. Guo, and Q. Wang, Twin-field quantum digital signatures, arXiv preprint arXiv:2003.11262 (2020).
34. W. Zhao, R. Shi, J. Shi, P. Huang, Y. Guo, and D. Huang, "Multibit quantum digital signature with continuous variables using basis encoding over insecure channels," Phys. Rev. A **103**(1), 012410 (2021).
35. S. Richter, M. Thornton, I. Khan, H. Scott, K. Jaksch, U. Vogl, B. Stiller, G. Leuchs, C. Marquardt, and N. Korolkova, "Agile and versatile quantum communication: Signatures and secrets," Phys. Rev. X **11**(1), 011038 (2021).
36. V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**(5), 057901 (2004).
37. C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum-key-distribution protocols," Phys. Rev. A **73**(1), 012337 (2006).
38. K. Tamaki and H.-K. Lo, "Unconditionally secure key distillation from multiphotons," Phys. Rev. A **73**(1), 010302 (2006).
39. Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, "An experimental comparison of BB84 and SARG04 quantum key distribution protocols," Laser Phys. Lett. **11**(9), 095201 (2014).
40. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
41. H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, "Security of quantum key distribution with multiphoton components," Sci. Rep. **6**(1), 29482 (2016).
42. Y.-S. Lu, X.-Y. Cao, C.-X. Weng, J. Gu, Y.-M. Xie, M.-G. Zhou, H.-L. Yin, and Z.-B. Chen, "Efficient quantum digital signatures without symmetrization step," Opt. Express **29**(7), 10162–10171 (2021).
43. K. Longmate, E. Ball, E. Dable-Heath, and R. Young, "Signing information in the quantum era," AVS Quantum Sci. **2**(4), 044101 (2020).
44. X.-Q. Cai, T.-Y. Wang, C.-Y. Wei, and F. Gao, "Cryptanalysis of multiparty quantum digital signatures," Quantum Inf. Process. **18**(8), 252 (2019).
45. J. M. Arrazola, P. Wallden, and E. Andersson, "Multiparty quantum signature schemes," QIC **16**, 435–464 (2016).
46. M. Şahin and İ. Yilmaz, "Multi-partied quantum digital signature scheme without assumptions on quantum channel security," J. Phys.: Conf. Ser. **766**, 012021 (2016).
47. C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," Phys. Rev. A **89**(2), 022307 (2014).
48. H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, "Tight security bounds for decoy-state quantum key distribution," Sci. Rep. **10**(1), 14312 (2020).
49. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**(23), 230503 (2005).
50. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
51. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
52. X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," Phys. Rev. A **72**(1), 012322 (2005).
53. H. Chernoff, "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations," Ann. Math. Statist. **23**(4), 493–507 (1952).