

Proof-of-Principle Demonstration of Passive Decoy-State Quantum Digital Signatures Over 200 km


Chun-Hui Zhang,^{1,2,3} Xing-Yu Zhou,^{1,2,3} Hua-Jian Ding,^{1,2,3} Chun-Mei Zhang,^{1,2,3,4,*}
Guang-Can Guo,^{1,2,3,4} and Qin Wang^{1,2,3,4,†}

¹*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

²*Broadband Wireless Communication and Senser Network Technology, Key Lab of Ministry of Education, NUPT, Nanjing 210003, China*

³*Telecommunication and Networks, National Engineering Research Center, NUPT, Nanjing 210003, China*

⁴*Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei, Anhui 230026, China*

 (Received 27 March 2018; revised manuscript received 22 June 2018; published 18 September 2018)

Quantum digital signatures (QDSs) offer the information-theoretic security verified by quantum mechanics to send a message that is robust against forging and repudiation. We report a proof-of-principle demonstration of a passive decoy-state QDS system that can avoid leaking the modulation information of decoy states. To realize this, four local detection events are generated from the idler light of a parametric down-conversion process, and are then used as decoy states to estimate channel parameters more accurately. As a result, we successfully sign a more-than-one-bit message within 7 s at 100 km. Besides, we achieve a transmission distance of 200 km, which represents a further step toward the practical application of QDSs.

DOI: [10.1103/PhysRevApplied.10.034033](https://doi.org/10.1103/PhysRevApplied.10.034033)

I. INTRODUCTION

Digital signatures [1] are one of the most important cryptographic protocols, and have been applied on many occasions, such as software distributions, financial transactions, and electronic contracts. Many commonly used classical digital signatures offer computational security (e.g., the Rivest-Shamir-Adleman protocol [2] relying on the difficulty of large-integer factorization); however, they are vulnerable to algorithmic breakthroughs and the emergence of quantum computers. On the other hand, certain classical digital signatures can offer postquantum security against an attack by a large quantum computer [3]. Unfortunately, their security cannot be proved to date and they are potentially susceptible to algorithmic breakthroughs.

In contrast, analogously to quantum key distribution (QKD) [4–8], quantum digital signatures (QDSs) aim to offer information-theoretic security against attackers restricted only by the laws of physics. The first QDS protocol was proposed by Gottesman and Chuang [9] in 2001, and needs nondestructive state comparison, long-time quantum memory, and a secure quantum channel. Thereafter, to make QDSs more practical, both theoretical and experimental studies were performed [10–22].

In recent experimental demonstrations of QDSs [23–25], the active decoy-state method, which modulates the weak coherent state (WCS) source into several different intensities with acousto-optic or electro-optic modulators, is widely used. However, this active decoy-state method may leak the signal and decoy information to Eve due to the operation of active intensity modulations [26,27]. To reduce the possibility of signal and decoy-information leakage, the passive decoy-state method has been proposed [28,29], adopting the parametric down-conversion (PDC) source. In addition, because of the spontaneous feature of the PDC process, the intrinsic phase randomization can be immune to some source attacks [30,31], improving the security of systems.

The critical experimental challenge to implement the passive decoy-state method is that there are only two kinds of detection events, trigger or nontrigger, which gives a poor estimation for the contributions of single-photon components. Besides, as a local detection, the idler photons do not suffer from the modulation loss and channel loss, leading to a high dark-count rate and low maximum counting rate [32].

To eliminate these flaws, we perform a proof-of-principle demonstration of passive decoy-state QDSs based on the PDC source, where the idler photons are split into four kinds of local detection events with a beam splitter to estimate channel parameters more accurately. In so

*cmz@njupt.edu.cn

†qinw@njupt.edu.cn

doing, we have a fair signature rate at 100 km with this system. Particularly, we achieve a transmission distance of 200 km, which demonstrates the feasibility of passive decoy-state QDSs for practical applications.

II. MATERIALS AND METHODS

A. Passive decoy-state QDS protocol

Our passive decoy-state QDS protocol consists of a distribution stage and a messaging stage. The distribution stage uses the key-generating protocol (KGP) in pairs individually by Bob and Alice and Charlie and Alice to generate correlated bit strings, where Bob and Charlie send quantum states to Alice separately, and Alice measures the quantum states received. The messaging stage involves sending and signing classical messages, where Alice is the sender and Bob and Charlie are two recipients. The KGP, in essence, is similar to QKD but without error correction and privacy amplification, and the use of derivatives of QKD for QDSs was proposed by Wallden *et al.* [13]. Next we introduce our passive QDS protocol step by step.

Distribution stage:

(1) Bob (Charlie) uses the PDC process to generate N photon pairs, which are separated as the signal mode and the idler mode. In contrast to conventional passive schemes, here the idler mode is further split into two branches by a beam splitter and each branch is individually sent into a local single-photon detector (D_1 and D_2). As a result, four kinds of detection events are recorded as X_i ($i = 1, 2, 3, 4$); namely, no clicking, clicking only at D_1 , clicking only at D_2 , and clicking at both D_1 and D_2 .

(2) Bob (Charlie) randomly prepares the signal mode into a sequence of BB84 states [4] for each future possible message m ($m = 0$ or 1), and sends them to Alice. Alice randomly chooses the X basis or the Z basis to measure received photon pulses.

(3) Bob (Charlie) and Alice publicly announce their bases for each pulse. At the same time, Bob (Charlie) announces the detection event X_i each pulse belongs to. They keep the results of the same bases. Alice and Bob (Charlie) can extract sifted keys, denoted as B_m^A and K_m^B (C_m^A and K_m^C), of length n . B_m^A (C_m^A) is held by Bob (Charlie) and K_m^B (K_m^C) is held by Alice.

(4) To estimate the error rate, Bob (Charlie) and Alice randomly sacrifice a small number, k , of bits, denoted as V_m^B (V_m^C), leaving keys of length L of themselves, \tilde{B}_m^A and \tilde{K}_m^B (\tilde{C}_m^A and \tilde{K}_m^C).

(5) Bob (Charlie) randomly chooses half of his sifted key bits in his \tilde{B}_m^A (\tilde{C}_m^A) to keep, denoted as $\tilde{B}_{m,\text{keep}}^A$ ($\tilde{C}_{m,\text{keep}}^A$), and forwards the other half as well as the corresponding positions to Charlie (Bob) with the Bob-Charlie secret classical channel, denoted as $\tilde{B}_{m,\text{forward}}^A$ ($\tilde{C}_{m,\text{forward}}^A$). We denote Bob's (Charlie's) symmetrized keys as S_m^B (S_m^C),

which contains half of B_m^A and half of C_m^A . In other words, $S_m^B = (\tilde{B}_{m,\text{keep}}^A, \tilde{C}_{m,\text{forward}}^A)$ and $S_m^C = (\tilde{C}_{m,\text{keep}}^A, \tilde{B}_{m,\text{forward}}^A)$.

Messaging stage:

(1) Alice sends (m, Sig_m) to a recipient (such as Bob), where $\text{Sig}_m = (\tilde{K}_m^B, \tilde{K}_m^C)$.

(2) Bob checks (m, Sig_m) with his S_m^B and records the number of mismatches. If there are fewer than $s_a L/2$ mismatches with both halves of his keys, where s_a is an authentication threshold associated with the security level of the protocol, Bob accepts the message and goes to the next step; otherwise, he rejects the message and aborts this round.

(3) Bob forwards (m, Sig_m) to Charlie.

(4) Charlie also checks the forwarded message in the same way but with another threshold s_v ($s_v > s_a$). Charlie accepts the forwarded message if the number of mismatches in both halves of his keys is below $s_v L/2$.

In the KGP, whenever event X_i happens, the signal mode encoded with message m will be projected into the photon-number space $\rho_l = \sum_n a_n^l |n\rangle\langle n|$ ($l = x, y, z, w$), where l corresponds to event X_i ($i = 1, 2, 3, 4$). These events can be used for decoy states to estimate channel parameters more accurately. Because of the finite-size key effect, we consider the statistical fluctuation method in Ref. [33]. Besides, we use all four events in the Z basis to generate sifted keys. As in Ref. [15], we can find the min-entropy in the presence of Eve as

$$H_{\min}^\epsilon(Z|E) \gtrsim \underline{s}_1 [1 - H_2(\bar{e}_1)], \quad (1)$$

where \underline{s}_1 and \bar{e}_1 represent the lower bound of single-photon counts and the upper bound of the single-photon error rate, respectively, and $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary Shannon entropy function. Equation (1) holds with probability $1 - \epsilon$, and ϵ measures the failure probability of estimated parameters. The detailed derivation of those quantities and the key-bit formulae are presented in Appendix A. Using Eq. (1), we evaluate the minimum rate P_e at which Eve can introduce errors in the KGP given by

$$H_2(P_e) = \frac{2\underline{s}_1}{L} [1 - H_2(\bar{e}_1)]. \quad (2)$$

For the security analysis of our passive decoy-state QDS protocol, the robustness, forging, and repudiation probabilities should be considered [15]. The robustness probability, measuring the probability of aborting an honest run, is given by

$$P_{\text{robust}} \leq 2\epsilon_{\text{PE}}, \quad (3)$$

where ϵ_{PE} is the failure probability of estimating the error rates of Alice and Bob and Alice and Charlie with the Serfling inequality [34]. The repudiation probability,

characterizing Alice's signature accepted by Bob but rejected by Charlie, is given by

$$P_{\text{reputation}} \leq 2 \exp \left[- \left(\frac{s_v - s_a}{2} \right)^2 L \right], \quad (4)$$

where

$$s_a = \bar{E} + \frac{P_e - \bar{E}}{3}, \quad s_v = \bar{E} + \frac{2(P_e - \bar{E})}{3}. \quad (5)$$

Here \bar{E} is the upper bound of the observed error rate by use of the Serfling inequality. The forging probability, accounting for a signature not signed by Alice but accepted by both Bob and Charlie, is given by

$$P_{\text{forge}} \leq a + \epsilon_F + 6\epsilon_{\text{PE}}, \quad (6)$$

where a and ϵ_F are associated with the probability that Bob finds a signature with an error rate smaller than s_v , defined by

$$\epsilon_F := \frac{1}{a} \left(2^{-\left\{ \frac{2s_1}{L} [1 - H_2(\bar{e}_1)] - H_2(s_v) \right\}} + \epsilon \right), \quad (7)$$

and $6\epsilon_{\text{PE}}$ is the failure possibility of estimated channel parameters. Finally, we call the system secure to the level ϵ against aborting, repudiation and forging, and there is no reason to favor one probability over any of the others, hence we assume [22]

$$\epsilon \geq P_{\text{robust}} = P_{\text{reputation}} = P_{\text{forge}}. \quad (8)$$

B. Experimental setup

Figure 1 displays the experimental setup of our passive decoy-state QDS protocol. Bob (Charlie) generates 898-nm-wavelength coherent-state pulses with a repetition

rate of 76 MHz and a pulse duration of 2 ps with a mode-locked Ti:sapphire laser. After the second-harmonic generation (SHG) of a β -BaB₂O₄ crystal, the pulses are frequency doubled into 449 nm light. Then they pump a periodically poled LiNbO₃ (PPLN) crystal, generating nondegenerate parametric down-conversion photon pairs, centered at 633 and 1545 nm, respectively. The generated photon pairs are separated by a dichroic mirror. Pulses of 633 nm are split into two paths by a beam splitter, and are then coupled into fibers and sent individually into a silicon avalanche photodiode (SAPD). The SAPDs have a detection efficiency of 65% at 633 nm. Pulses of 1545 nm are filtered by a tunable band-pass filter with full width at half maximum of 3 nm, and are then sent into a low-loss asymmetric Mach-Zehnder interferometer (AMZI), where a phase modulator, driven by a control board, encodes the four BB84 states, $\{0, \pi/2, \pi, 3\pi/2\}$. To avoid most of the device loss of the normal Mach-Zehnder interferometer, in our low-loss AMZI, all connections use polarization-maintaining fibers and a fiber polarization beam splitter is used to replace the normal fiber beam splitter in either the input or the output. Then the encoded pulses are transmitted to Alice through a quantum channel.

At Alice's side, the received pulses are decoded by her AMZI and sent to a commercial superconducting-nanowire single-photon detector (SNSPD; TCOPRS-CCR-SW-85, SCONTEL). It provides a detection efficiency of 80% when operating at 2.15 K. To stabilize the system, one polarization controller is placed before each AMZI or SNSPD to adjust the polarization of the incident photons. At each side, a time-to-digital converter is used to collect signals from the detectors, and the time window for recording signals is set to 3 ns. The synchronization of whole system is realized by the clock of the Ti:sapphire laser.

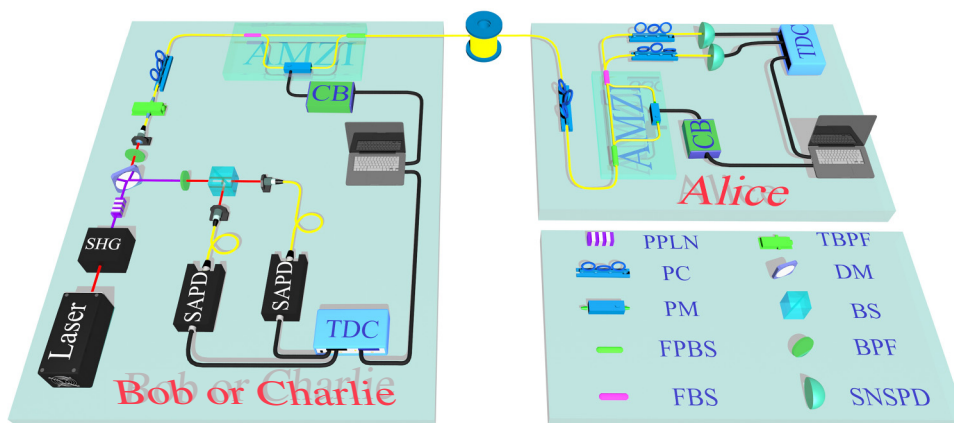


FIG. 1. Setup of the KGP. AMZI, asymmetric Mach-Zehnder interferometer; BPF, band-pass filter; BS, beam splitter; CB, control board; DM, dichroic mirror; FBS, fiber beam splitter; FPBS, fiber polarization beam splitter; PC, polarization controller; PPLN, periodically poled LiNbO₃ crystal; PM, phase modulator; SAPD, silicon avalanche photodiode; SHG, second-harmonic generation; SNSPD, superconducting-nanowire single-photon detector; TBPF, 3 nm fiber filter with tunable central wavelength; TDC, time-to-digital converter.

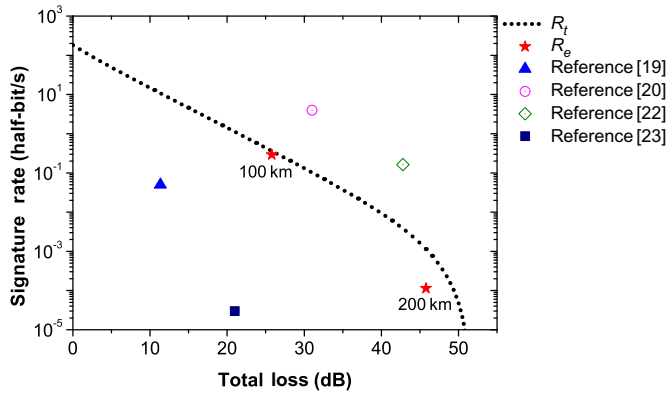


FIG. 2. The signature rates in this work and other reports. The horizontal axis represents the total channel loss, and the vertical axis indicates the signature rate. R_t refers to the theoretical predictions obtained with the same device parameters as in our experiment, while R_e refers to the experimental results.

In our experiment, the inherent system loss mainly caused by the filter, AMZIs, and polarization controllers is 5.8 dB. For each message m , we typically operate the system for 96 min, including the effective transmission of 80 min, and 16 min for scanning and compensating phases. This scan and transmission mode [35,36] can keep our system running stably for a long time. In our experiment, the pump light before the PPLN is kept at 3 mW so that the mean photon number of PDC light μ_0 is 0.54. After coupling into the fiber and passing through the first AMZI, the mean photon number of the signal pulses sent out is $\mu = \mu_0 \eta_s = 0.135$. Other parameters used in our experiment are given in Appendix B.

III. RESULTS AND DISCUSSION

With the desired security level, we calculate the signature rate or the time it would take to distribute a signature state sequence for signing one half-bit with the current system. The half-bit is the signature used for either a binary 0 or a binary 1, and both are required for us to be able to sign a single bit. In our experiment, we set $\epsilon_{PE} = 10^{-5}$, $a = 10^{-5}$, and $\epsilon = 10^{-10}$ [15], and the security level ϵ in this paper is 10^{-4} . We separately run the passive decoy-state

KGP system between Bob and Alice or between Charlie and Alice with two different losses of quantum channels (25.8 and 45.8 dB), equivalent to standard single-mode optical fibers of 100 and 200 km excluding the system loss of 5.8 dB, respectively. In each run, the total number of pulses sent from Bob (Charlie) is $N_t = 3.648 \times 10^{11}$. The wavelength of the signal light generated in our PDC process is 1545 nm, and for simplicity, here in our simulation we use the commonly used loss coefficient of 0.2 dB/km at telecommunication wavelength. The detailed experiment results are given in Appendix B.

After applying the statistical fluctuation method proposed in Ref. [33], we present the signature rates of our experimental data and corresponding theoretical predictions in Fig. 2. The dotted line denotes theoretical signature rates with the actual setup parameters, and the two asterisks represent experimental signature rates at different distances. We can see from Fig. 2 that our experimental data match very well with the theoretical predictions. In our experiment, at transmission distances of 100 and 200 km, the signature rates are obtained as 0.29 and 1.15×10^{-4} half-bits per second, respectively.

Furthermore, we compare data from our present work and from several previous reports [18–20,22,23] as listed in Table I. We also add these data to Fig. 2 to provide an easily understood visual comparison. Table I displays typical experimental parameters and the corresponding time cost to sign a half-bit message. Donaldson *et al.* [19], for a 850-nm-wavelength system, obtained an estimated time cost to securely sign a half-bit of around 20 s at 500 m, and the maximum transmission distance was to 2 km. Collins *et al.* [20] realized a QDS experiment through a 90-km fiber by using a differential-phase-shift (DPS) system with 1-GHz repetition rate. At this distance, it signed two bits per second (i.e., the estimated time to securely sign a half-bit was 0.25 s). Soon after, they improved their experimental system and achieved signing of a half-bit at 134 km in 5.67 s [22]. We can see from Fig. 2 that the signature rates in Refs. [20,22] are higher than ours for the same channel loss, which is mainly attributed to the high repetition rate of the laser and the highly efficient DPS protocols used. However, the security of the DPS protocol against coherent attacks has not been proven. It thus suffers an underlying

TABLE I. Comparison of signing a half-bit between different studies on QDSs. Here the security (ϵ) of all protocols holds at the level of 10^{-4} .

Parameter	Reference [19]	Reference [20]	Reference [22]	Reference [23]	Present work
Light source	WCS	WCS	WCS	WCS	PDC
KGP	BB84	DPS	DPS	SARG04	Passive BB84
Maximal transmission distance (km)	2 (11.36 dB)	90 (31 dB)	134 (42.8 dB)	102 (21 dB)	200 (45.8 dB)
Laser repetition rate	100 MHz	1 GHz	1 GHz	75 MHz	76 MHz
Time	20 s at 0.5 km	0.25 s at 90 km	5.67 s at 134 km	33 420 s at 102 km	3.45 s at 100 km 8695.65 s at 200 km

threat from coherent attacks. Very recently, Yin *et al.* [23] reported an experimental QDS using the SARG04 protocol over 102 km. In their experimental system, it took 33 420 s to sign a half-bit at 102 km. Compared with those previous experimental demonstrations of QDSs, our system achieves a good balance between security and efficiency. First, it is secure to coherent attacks. Besides, it can sign one half-bit at 100 km within 3.45 s, and can reach a maximum signature distance of 200 km.

IV. CONCLUSIONS

We report a proof-of-principle demonstration of passive decoy-state QDSs. With the passive decoy-sate method, the probability of leaking signal and decoy information to an eavesdropper is avoided, which improves the security of the system. We successfully sign a more-than-one-bit message within 7 s at 100 km in our experimental system. Furthermore, we remark that the transmission distance of our system can reach up to 200 km. We attribute the superiority of our system to the use of the efficient passive decoy-state scheme compared with the scheme using only one local detector, and the low-loss experimental system. In addition, our work can also be extended to the recently proposed measurement-device-independent quantum digital signatures [17]. Hence, our work represents a significant further step along the progression of QDSs from the laboratory to practical application.

ACKNOWLEDGMENTS

We gratefully appreciate Dr. Shuang Wang for providing low-loss AMZIs, La-Bao Zhang for technical support, and Wei Chen and Zhen-Qiang Yin for enlightened discussions on the present work. We also acknowledge financial support from the National Key Research and Development Program of China through Grants No. 2018YFA0306400 and No. 2017YFA0304100, the National Natural Science Foundation of China through Grants No. 61475197, No. 61590932, No. 11774180, and No. 61705110, the Natural Science Foundation of the Jiangsu Higher Education Institutions through Grants No. 15KJA120002 and No. 17KJB140016, the Outstanding Youth Project of Jiangsu Province through Grant No. BK20150039, the Natural Science Foundation of Jiangsu Province through Grant No. BK20170902, the Priority Academic Program Development of Jiangsu Higher Education Institutions, and the

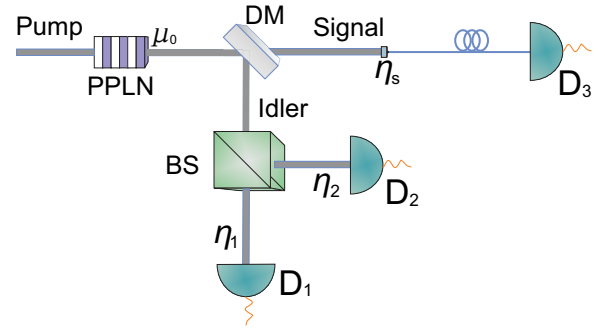


FIG. 3. Generation of the PDC source at Bob's (Charlie's) side. BS, beam splitter; DM, dichroic mirror; PPLN, periodically poled LiNbO₃ crystal.

Postgraduate Research and Practice Innovation Program of Jiangsu Province.

APPENDIX A: MODEL OF THE KGP

In this section, we mathematically model the KGP with statistical fluctuations. We start by analyzing the PDC source illustrated in Fig. 3. As described in the main text, the parametric down-converted photon pairs generated from a PPLN crystal are separated by a dichroic mirror. Then the idler mode is further split into two paths and sent to two local detectors (D₁, D₂). We can record four kinds of click events as X_i ($i = 1, 2, 3, 4$): (1) no clicking; (2) clicking only at D₁; (3) clicking only at D₂; (4) clicking at both D₁ and D₂. Below we formulate the photon-number distribution of signal state l ($l = x, y, z, w$), a_n^l , which is conditioned on recording event X_i . To give a clear analysis, we assume that the detectors at Bob's (Charlie's) side have a detection efficiency of 100%, but include the imperfect detection efficiency into the coupling loss.

For a pair of m -photon states from the PDC process, after conditional detection event X_i in the idler mode, the corresponding probability of finding n photons in the signal state l , which is coupled into the fiber, is given by

$$a_n^l = \sum_{m=n}^{\infty} \frac{\mu_0^m e^{-\mu_0}}{m!} C_m^n \eta_s^n (1 - \eta_s)^{m-n} P_{X_i|m}, \quad (\text{A1})$$

where $l = x, y, z, w$; μ_0 is the original mean photon number from the PDC process; C_m^n is the binomial coefficient, defined as $C_m^n = m! / (n!(m-n)!)$; η_s corresponds to the coupling efficiency of the signal mode; and $P_{X_i|m}$ is

TABLE II. Probability of event X_i occurring.

Case	$P_{X_1 s_1s_2}$	$P_{X_2 s_1s_2}$	$P_{X_3 s_1s_2}$	$P_{X_4 s_1s_2}$
$s_1 = 0, s_2 = 0$	$(1 - d_1)(1 - d_2)$	$d_1(1 - d_2)$	$d_2(1 - d_1)$	d_1d_2
$s_1 \neq 0, s_2 = 0$	0	$1 - d_2$	0	d_2
$s_1 = 0, s_2 \neq 0$	0	0	$1 - d_1$	d_1
$s_1 \neq 0, s_2 \neq 0$	0	0	0	1

TABLE III. Conditional probability $P_{X_i|m}$ that an m -photon state is projected into event X_i .

Case	$P_{X_i m}$
$s_1 = 0, s_2 = 0$	$(1 - d_1)(1 - d_2)[1 - \eta_{10} - (1 - t)\eta_{20}]^m$
$s_1 \neq 0, s_2 = 0$	$(1 - d_2)[1 - (1 - t)\eta_{20}]^m - (1 - d_1)(1 - d_2)[1 - \eta_{10} - (1 - t)\eta_{20}]^m$
$s_1 = 0, s_2 \neq 0$	$(1 - d_1)[1 - t\eta_{10}]^m - (1 - d_1)(1 - d_2)[1 - \eta_{10} - (1 - t)\eta_{20}]^m$
$s_1 \neq 0, s_2 \neq 0$	$1 - (1 - d_1)[1 - t\eta_{10}]^m - (1 - d_2)[1 - (1 - t)\eta_{20}]^m + (1 - d_1)(1 - d_2)[1 - \eta_{10} - (1 - t)\eta_{20}]^m$

the probability of event X_i given any m -photon state of the idler mode, expressed as

$$P_{X_i|m} = \sum_{s_1 s_2} P_{X_i|s_1 s_2} P_{s_1 s_2|m}. \quad (\text{A2})$$

Here $P_{s_1 s_2|m}$ denotes the projecting probability of the m -photon state passing through the beam splitter and being projected into state $|s_1 s_2\rangle$, and $P_{X_i|s_1 s_2}$ denotes the probability of event X_i given a projection state $|s_1 s_2\rangle$. For $P_{X_i|s_1 s_2}$, if a vacuum projection state arrives, the local detector will click with a probability of d_j (the dark-count rate) and not click with a probability of $(1 - d_j)$, $j = 1, 2$. For a non-vacuum projection state, the local detector will definitely click. We then list all $P_{X_i|s_1 s_2}$ as shown in Table II. For $P_{s_1 s_2|m}$, as deduced in Ref. [29], we find

$$\begin{aligned} P_{s_1 s_2|m} &= \sum_{k=0}^m \sum_{s_2=0}^{m-k} \sum_{s_1=0}^k C_m^k t^k (1-t)^{m-k} C_k^{s_1} \eta_{10}^{s_1} (1-\eta_{10})^{k-s_1} \\ &\quad \times C_{m-k}^{s_2} \eta_{20}^{s_2} (1-\eta_{20})^{m-k-s_2} \\ &= \sum_{k=0}^m \sum_{s_2=0}^{m-k} \sum_{s_1=0}^k \frac{m! t^k (1-t)^{m-k} \eta_{10}^{s_1} \eta_{20}^{s_2} (1-\eta_{10})^{k-s_1}}{s_1! s_2! (k-s_1)! (m-k-s_2)!}, \end{aligned} \quad (\text{A3})$$

where t represents the transmission efficiency of the beam splitter, and η_{10} and η_{20} denote the overall efficiency of each branch in the idler mode, which includes the detection efficiency but excludes the transmission efficiency of the beam splitter (t). Combining the data in Table II and Eq. (A3), we obtain the conditional probability $P_{s_1 s_2|m}$ in Eq. (A2), which is given in Table III. With Eq. (A1), we calculate the corresponding simplified photon-number

distributions of the l ($l = x, y, z, w$) state as

$$\begin{aligned} a_n^x &= (1 - d_1)(1 - d_2) e^{-\mu_0(\eta_{10} + \eta_{20})} P_n[\mu_0 \eta_s (1 - \eta_1 - \eta_2)], \\ a_n^y &= (1 - d_2) e^{-\mu_0 \eta_2} P_n[\mu_0 \eta_s (1 - \eta_2)] - a_n^x, \\ a_n^z &= (1 - d_1) e^{-\mu_0 \eta_1} P_n[\mu_0 \eta_s (1 - \eta_1)] - a_n^x, \\ a_n^w &= P_n[\mu_0 \eta_s] - a_n^x - a_n^y - a_n^z, \end{aligned} \quad (\text{A4})$$

where $P_n(\xi) = (\xi^n/n!)e^{-\xi}$; $\eta_1 = t\eta_{10}$ and $\eta_2 = (1-t)\eta_{20}$ can be regarded as the overall efficiency from the crystal to the detectors.

With the above formulae and the model presented in Ref. [7], we can derive the lower bound of the counts (\underline{s}_1) and the upper bound of the quantum-bit error rate (QBER) (\bar{e}_1) for single-photon pulses as

$$\begin{aligned} s_1 \geq \underline{s}_1 &= (a_1^x + a_1^y + a_1^z + a_1^w) \\ &\quad \times \frac{a_2^z \bar{\Delta}[n_x] - a_2^x \bar{\Delta}[n_z] - (a_2^z a_0^x - a_2^x a_0^z) \bar{s}_0}{(a_1^x a_2^z - a_1^z a_2^x)}, \end{aligned} \quad (\text{A5})$$

$$e_1 \leq \bar{e}_1 = (a_1^x + a_1^y + a_1^z + a_1^w) \frac{\bar{\Delta}[n_y^e] - e_0 a_0^y \underline{s}_0}{a_1^y \underline{s}_1}, \quad (\text{A6})$$

where

$$\bar{s}_0 = \min \left\{ \frac{\bar{\Delta}[n_x^e]}{a_0^x e_0}, \frac{\bar{\Delta}[n_y^e]}{a_0^y e_0}, \frac{\bar{\Delta}[n_z^e]}{a_0^z e_0}, \frac{\bar{\Delta}[n_w^e]}{a_0^w e_0} \right\}, \quad (\text{A7})$$

$$\underline{s}_0 = \max \left\{ \frac{a_1^y \bar{\Delta}[n_x] - a_1^x \bar{\Delta}[n_y]}{a_0^x a_1^y - a_0^y a_1^x}, \frac{a_1^z \bar{\Delta}[n_x] - a_1^x \bar{\Delta}[n_z]}{a_0^x a_1^z - a_0^z a_1^x}, 0 \right\}. \quad (\text{A8})$$

Here e_0 ($= 0.5$) and s_0 denote the quantum-bit error rate and conditional counts of vacuum pulses at Alice's side,

TABLE IV. Two sets of parameters used in the experiment.

Channel	η_1	η_2	η_s	η_{Alice}	d_1 (counts/pulse)	d_2 (counts/pulse)	e_d
Bob-Alice	9.17%	10.21%	25.03%	80%	1.63×10^{-7}	2.08×10^{-7}	1.81%
Charlie-Alice	9.25%	10.40%	24.88%	80%	6.63×10^{-7}	4.90×10^{-7}	1.54%

TABLE V. Measured counts and QBERs of different events in the Z basis on quantum links of Bob-Alice and Charlie-Alice.

Attenuation	Event	Bob-Alice		Charlie-Alice	
		Counts (n_l^Z)	QBER (%)	Counts (n_l^Z)	QBER (%)
25.8 dB (at 100 km)	X_1	18 658 916	3.28	16 856 368	1.74
	X_2	3 357 757	3.08	3 060 586	1.53
	X_3	3 615 194	3.07	3 262 813	1.53
	X_4	358 987	3.06	316 053	1.46
45.8 dB (at 200 km)	X_1	167 803	5.23	155 001	5.25
	X_2	28 307	3.01	26 773	2.65
	X_3	31 577	3.08	28 826	2.74
	X_4	3017	2.95	2756	3.05

respectively, and n_l and n_l^e ($l = x, y, z, w$) represent the overall counts and the quantum-bit errors for the l event. According to n_l and n_l^e , the QBER is $E_l = n_l^e/n_l$. Note that we use the method proposed in Ref. [33] to take statistical fluctuation into consideration. The upper and lower bounds of the measured values are given by

$$\underline{\Delta}[\chi] = \frac{\chi}{1 + \underline{\delta}}, \quad \bar{\Delta}[\chi] = \frac{\chi}{1 - \bar{\delta}}, \quad (\text{A9})$$

which hold with probability $1 - \zeta$ ($\zeta = 10^{-7}$ in our experiment), and $\underline{\delta}$ and $\bar{\delta}$ are obtained by our solving the following equation: set

$$\left[\frac{e^{\underline{\delta}}}{(1 + \underline{\delta})^{1 + \underline{\delta}}} \right]^{\chi/(1 + \underline{\delta})} = \frac{1}{2}\zeta, \quad \left[\frac{e^{-\bar{\delta}}}{(1 - \bar{\delta})^{1 - \bar{\delta}}} \right]^{\chi/(1 - \bar{\delta})} = \frac{1}{2}\zeta. \quad (\text{A10})$$

Subsequently, we can use Eqs. (A5) and (A6) to work out min-entropy in the presence of Eve as

$$H_{\min}^e(Z|E) \gtrsim \varepsilon_1[1 - H_2(\bar{e}_1)]. \quad (\text{A11})$$

APPENDIX B: EXPERIMENTAL RESULTS

To characterize the photon-number distribution of the PDC source, we build a Hanbury Brown–Twiss setup on the signal mode with or without heralding by the idler mode, and calculate the value of the normalized second-order correlation function $g^2(\tau)$ of the signal photons. We obtain $g^2(0) = 1.002 \pm 0.004$ without heralding by the idler mode, which confirms the Poisson distribution of the photon-pair number; we obtain $g^2(0) = 0.244 \pm 0.002$ with heralding and find a sub-Poissonian distribution.

We measure the experimental parameters of our system given in Table IV (i.e., the mean photon number μ_0 generated from the PPLN per pulse; the overall transmission efficiencies of the idler mode, η_i ($i = 1, 2$), and the coupling efficiencies of the signal mode, η_s ; the detection efficiency of the SNSPD, η_{Alice} ; the dark-count rate of the local detectors, d_i ($i = 1, 2$); and the misalignment of

our Mach-Zehnder interferometers e_d is system parameter which needs to be measured before we start to distribute quantum keys).

We run our system for 96 min. Table V shows the the measured counts and QBER of the state l ($l = x, y, z, w$) at different distances. With these experiment results, we can sign messages at a rate of 0.29 and 1.15×10^{-4} half-bits per second at 100 and 200 km, respectively.

- [1] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory* **22**, 644 (1976).
- [2] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21**, 120 (1978).
- [3] D. J. Bernstein and T. Lange, Post-quantum cryptography, *Nature* **549**, 188 (2017).
- [4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175
- [5] A. K. Ekert, Quantum Cryptography based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [6] X. B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [7] H. K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [8] H. K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [9] D. Gottesman and I. Chuang, Quantum digital signatures, arXiv:quant-ph/0105032.
- [10] J. M. Arrazola and N. Lütkenhaus, Quantum communication with coherent states and linear optics, *Phys. Rev. A* **90**, 042335 (2014).
- [11] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light, *Nat. Commun.* **3**, 1174 (2012).
- [12] V. Dunjko, P. Wallden, and E. Andersson, Quantum Digital Signatures without Quantum Memory, *Phys. Rev. Lett.* **112**, 040502 (2014).

- [13] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Quantum digital signatures with quantum-key-distribution components, *Phys. Rev. A* **91**, 042304 (2015).
- [14] T. Y. Wang, X. Q. Cai, Y. L. Ren, and R. L. Zhang, Security of quantum digital signatures for classical messages, *Sci. Rep.* **5**, 9231 (2015).
- [15] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, *Phys. Rev. A* **93**, 032325 (2016).
- [16] J. M. Arrazola, P. Wallden, and E. Andersson, Multiparty quantum signature schemes, *Quantum Inf. Comput.* **16**, 0435 (2016).
- [17] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, Measurement-device-independent quantum digital signatures, *Phys. Rev. A* **94**, 022328 (2016).
- [18] 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**, 040502 (2014).
- [19] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, Experimental demonstration of kilometer-range quantum digital signatures, *Phys. Rev. A* **93**, 012329 (2016).
- [20] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system, *Opt. Lett.* **41**, 4883 (2016).
- [21] 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**, 100503 (2016).
- [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**, 3235 (2017).
- [23] 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**, 032334 (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 measurement-device-independent quantum digital signatures over a metropolitan network, *Phys. Rev. A* **95**, 042338 (2017).
- [25] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, Experimental measurement-device-independent quantum digital signatures, *Nat. Commun.* **8**, 1098 (2017).
- [26] J. Z. Hu and X. B. Wang, Reexamination of the decoy-state quantum key distribution with an unstable source, *Phys. Rev. A* **82**, 012331 (2010).
- [27] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z. F. Han, G. C. Guo, and A. Karlsson, Experimental Decoy-State Quantum Key Distribution with a Sub-Poissonian Heralded Single-Photon Source, *Phys. Rev. Lett.* **100**, 090501 (2008).
- [28] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion, *Phys. Rev. Lett.* **99**, 180503 (2007).
- [29] Q. Wang, C. H. Zhang, and X. B. Wang, Scheme for realizing passive quantum key distribution with heralded single-photon sources, *Phys. Rev. A* **93**, 032312 (2016).
- [30] Y. L. Tang, H. L. Yin, X. Ma, C. H. F. Fung, Y. Liu, H. L. Yong, T. Y. Chen, C. Z. Peng, Z. B. Chen, and J. W. Pan, Source attack of decoy-state quantum key distribution using phase information, *Phys. Rev. A* **88**, 022308 (2013).
- [31] S. H. Sun, M. Gao, M. S. Jiang, C. Y. Li, and L. M. Liang, Partially random phase attack to the practical two-way quantum-key-distribution system, *Phys. Rev. A* **85**, 032304 (2012).
- [32] Q. C. Sun, W. L. Wang, Y. Liu, F. Zhou, J. S. Pelc, M. M. Fejer, C. Z. Peng, X. F. Chen, X. Ma, Q. Zhang, and J. W. Pan, Experimental passive decoy-state quantum key distribution, *Laser Phys. Lett.* **11**, 085202 (2014).
- [33] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Improved key-rate bounds for practical decoy-state quantum-key-distribution systems, *Phys. Rev. A* **95**, 012333 (2017).
- [34] R. J. Serfling, Probability inequalities for the sum in sampling without replacement, *Ann. Stat.* **2**, 39 (1974).
- [35] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Faraday Michelson system for quantum cryptography, *Opt. Lett.* **30**, 2632 (2005).
- [36] Z. F. Han, X. F. Mo, Y. Z. Gui, and G. C. Guo, Stability of phase-modulated quantum key distribution systems, *Appl. Phys. Lett.* **86**, 221103 (2005).