Experimental quantum digital signature over 102 km

Hua-Lei Yin,[1,2] Yao Fu,[1,2] Hui Liu,[1,2] Qi-Jie Tang,[1,2] Jian Wang,[1,2] Li-Xing You,[3] Wei-Jun Zhang,[3] Si-Jing Chen,[3] Zhen Wang,[3] Qiang Zhang,[1,2,*] Teng-Yun Chen,[1,2,†] Zeng-Bing Chen,[1,2,‡] and Jian-Wei Pan[1,2,§]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*The CAS Center for Excellence in QIQP and the Synergetic Innovation Center for QIQP, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

(Received 31 July 2016; published 30 March 2017)

Quantum digital signature (QDS) is an approach to guarantee the nonrepudiation, unforgeability, and transferability of a signature with information-theoretical security. Previous experimental realizations of QDS relied on an unrealistic assumption of secure channels and the longest distance is several kilometers. Here, we have experimentally demonstrated a recently proposed QDS protocol without assuming any secure channel. Exploiting the decoy state modulation, we have successfully signed a one-bit message through an up to 102-km optical fiber. Furthermore, we continuously run the system to sign the longer message "USTC" with 32 bits at the distance of 51 km. Our results pave the way towards the practical application of QDS.

DOI: 10.1103/PhysRevA.95.032334

I. INTRODUCTION

Digital signature [1] is a basic primitive for plenty of cryptographic protocols, which has many applications in software distribution, financial transactions, contract management software, and so on. Classical digital signature mainly exploits the Rivest-Shamir-Adleman protocol [2], the security of which is based on the mathematical complexity of the integer factorization problem. This, however, may become vulnerable with a quantum computer [3]. By exploiting the laws of quantum mechanics, quantum key distribution (QKD) can offer two legitimate users to share a random key with information-theoretical security [4–6]. Similarly, one can expect to exploit the laws of quantum mechanics to sign a message with information-theoretical security, which is called quantum digital signature (QDS).

The first QDS protocol was proposed by Gottesman and Chuang in 2001 [7], where several technical challenges need to be fixed for a practical implementation, including nondestructive state comparison, long-time quantum memory, and a secure quantum channel. Thereafter, QDS has attracted a great deal of interest in the literature. Various QDS protocols have been proposed [8–12] and some pioneering experimental efforts have been made in this direction [13–16]. To name a few, Clarke *et al.* [13] utilize coherent states and linear optics to avoid the nondestructive operation and provide the first experimental attempt. Collins *et al.* [14] present a realization without the need of quantum memory, which, however, still needs the assumption of a secure quantum channel. A secure quantum channel means that the quantum channel should not be tampered with. Note that the basic model of quantum communication such as QKD [4,5] and quantum secret sharing [17] is that the quantum channel can be eavesdropped upon and tampered with. Therefore, the secure quantum channel is an unrealistic assumption and limits the application of QDS. Meanwhile, the symmetric Mach-Zehnder interferometer configuration of an optical multiport (two interwoven Mach-Zehnder interferometers) [18] in the experiment by Collins *et al.* [14] requires phase stability between distant parties, which is experimentally challenging for a long-distance implementation.

Very recently, new QDS protocols [19,20] have been proposed to remove the assumption of a secure quantum channel. A kilometer-range demonstration for the protocol in Ref. [11] is provided [15], which assumes QKD to remove the symmetric Mach-Zehnder interferometer configuration. In this paper, we provide a complete QDS experiment without quantum or classical secure channel assumption over a 102-km optical fiber. We do believe that with these experimental advances, QDS with information-theoretical security will come to practical applications soon.

Before describing the experiment in detail, we first introduce the QDS protocol [19] used in this paper. In a digital signature protocol, Alice, the sender, will send a message with a digital signature to two recipients, Bob and Charlie. Like previous protocols [9–16], in our decoy state quantum digital signature experiment, the security against forgery attack is decoupled from the security against repudiation attack, and the roles of Bob and Charlie are arbitrary. There is no need to fix the authenticator before the messaging stage: either Bob or Charlie can be the authenticator. Without loss of generality, in our experiment, we take Bob as the authenticator in the messaging stage. He then forwards the information that he received from Alice, to Charlie. In a successful digital signature protocol, Alice could not deny the signature, which is called nonrepudiation. On the other hand, Bob could not forge the message, which is called unforgeability. If Bob accepts the message, Charlie will also accept the message, which is called transferability. Our protocol is divided into three stages—distribution stage, estimation stage, and messaging stage.

In the distribution stage, for each future possible message $m = 0,1$, Alice exploits weak coherent states to randomly

*qiangzh@ustc.edu.cn
†tychen@ustc.edu.cn
‡zbchen@ustc.edu.cn
§pan@ustc.edu.cn

prepare two identical qubit states from the BB84 states [21], $|H\rangle, |V\rangle, |+\rangle$, and $|-\rangle$, where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization states, $|+\rangle = (1/\sqrt{2})(|H\rangle + |V\rangle)$ and $|-\rangle = (1/\sqrt{2})(|H\rangle - |V\rangle)$. In order to avoid photon-number splitting attack, Alice exploits the decoy state method by randomly varying the intensity of the pulses. She chooses three intensities μ, ν, and zero, therein, μ as signal and ν as decoy state. Then, Alice randomly sends one qubit state with intensity of α to Bob and the other with intensity of β to Charlie, where $(\alpha, \beta) \in (\mu, \nu, 0)$. Note that the polarization states sent to Bob and Charlie are identical, while the intensities do not need to be the same.

Bob and Charlie independently and randomly exploit the Z or X basis to measure the received quantum state. Alice, Bob, and Charlie record the corresponding data when both Bob's and Charlie's detectors have a click. The nonorthogonal state encoding scheme [22] is used to identify the conclusive outcomes and inconclusive outcomes. For each quantum state, Bob (Charlie) compares his measurement outcomes with two nonorthogonal states announced by Alice. Therein, the quantum state sent by Alice is one of the states she announced. If his measurement outcome is orthogonal to one of Alice's announced states, he concludes a conclusive result that the other state has been sent. Otherwise, he concludes that it is an inconclusive outcome, which is only known by himself.

In the estimation stage, Alice announces the nine intensity sets and also the bit information of six intensity sets, $\mu 0$, 0μ, $\nu\nu$, $\nu 0$, 0ν, and 00. Charlie (Bob) estimates the yield Y_{11}^C (Y_{11}^B) and the quantum bit error rate e_{11}^C (e_{11}^B) for single-photon pairs of his conclusive results [19], where a single-photon pair represents that one photon is sent to Bob and one photon is sent to Charlie. The other three intensity sets $\mu\mu$, $\mu\nu$, and $\nu\mu$ constitute an overall data string. Bob or Charlie randomly chooses some data from the overall data string as the sampling data string and informs everyone. This random sampling is only used for defeating Alice's repudiation attack, so it is same whether Bob or Charlie implements the random sampling. They compare the bit value for the sampling string and estimate the quantum bit error rate of conclusive results, E_s^B and E_s^C, which are utilized to restrict repudiation from Alice. The remaining data strings of Alice, Bob, and Charlie are kept for the digital signature, denoted as S_{Am}, S_{Bm}, and S_{Cm}, respectively.

In the messaging stage, to sign a one-bit message m, Alice sends the message and the corresponding data string (m, S_{Am}) to the authenticator Bob. Bob will accept the message when the mismatching rate of his conclusive outcome is less than authentication security threshold T_a. If Bob accepts the message, he forwards (m, S_{Am}) to the verifier, Charlie. Charlie will accept the message when the mismatching rate of his conclusive outcome is less than (verification) security threshold T_v. We remark that both Bob and Charlie can be the authenticator before the messaging stage in our decoy state quantum digital signature, which is the same as with previous protocols [13–16].

Exploiting the entanglement distillation technique [19,23,24], the minimum entropy of Bob about Charlie's conclusive results with the single-photon pairs can be bounded by $1 - H(e_{p11}^C|e_{11}^C)$, where e_{p11}^C is the phase error rate and $H(e_{p11}^C|e_{11}^C)$ is the conditional Shannon entropy (see Appendix A for details). Given the bound of the minimum entropy of Bob, one can acquire the lower bound of mismatching rate S_{11} between Bob's declaration and Charlie's conclusive results with single-photon pairs, which can be given by [19,20]

$$1 - H\left(e_{p11}^C \middle| e_{11}^C\right) - H(S_{11}) = 0, \tag{1}$$

where $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy function. Exploiting the mismatching rate S_{11}, one can restrict the forgery attack of Bob.

From the view of Alice, the status of all data (conclusive results and inconclusive results) owned by Bob (Charlie) could be regarded as the same, since Bob (Charlie) does not announce the position of a conclusive result. By random sampling, the upper bound of the difference between the data owned by Bob and Charlie can be bounded. With this restriction, Alice has to send almost the same quantum states to Bob and Charlie and thus the potential repudiating attack is avoided. Taking into account the finite-size effect [25–28], the authentication (verification) security threshold T_a (T_v) can be determined. With T_a and T_v, one can calculate the probabilities of successful repudiation attack, forgery attack, and robustness. Detailed analysis can be found in Appendix A.

II. EXPERIMENTAL SETUP

In the implementation, the quantum stage setup is shown in Fig. 1. Alice prepares four polarization-encoded BB84 states with four electrically modulated distributed feedback laser diodes. The emissions of the laser diodes are centered at 1550 nm with a pulse duration of 0.4 ns and repetition frequency of 75 MHz. The difference of the central wavelength from these lasers is well controlled to be less than 0.02 nm via temperature control. In order to decrease side channel attacks, we need to carefully adjust the four lasers and make the spectrum, waveform, and time modes as indistinguishable as possible. The spectrum and waveform modes are adjusted to be generally almost overlapped. The time mode is controlled to be less than 20 ps. We combine the four laser diodes with two polarization beam splitters (PBSs) and one 45-deg rotation beam splitter into a single fiber. An electrical variable optical attenuator is used to attenuate the average photon number per pulse to the experimental level. The dense wavelength division multiplexer with 100-GHz bandwidth is used to filter any spurious emission. After the filtration, the quantum states are sent out to Bob through a fiber spool.

We exploit the decoy state method [29–31] by varying the injection electrical current for the laser diodes. We set the intensities of signal states $\mu = 0.22$, decoy states $\nu = 0.066$, and vacuum states zero and their corresponding probability distributions are $P_\mu = 60\%$, $P_\nu = 35\%$, and $P_0 = 5\%$, respectively. All random signals for choosing polarization states or intensities are derived from random numbers generated beforehand. Meanwhile, the phases for the directly modulated laser diode are random, which is immune to the unambiguous state discrimination attack [32].

In Bob's side, the detector system contains four superconducting nanowire single-photon detectors (SNSPDs) that provide the detection efficiency of 52% at the dark count rate of 10 counts per second. A polarization measurement module

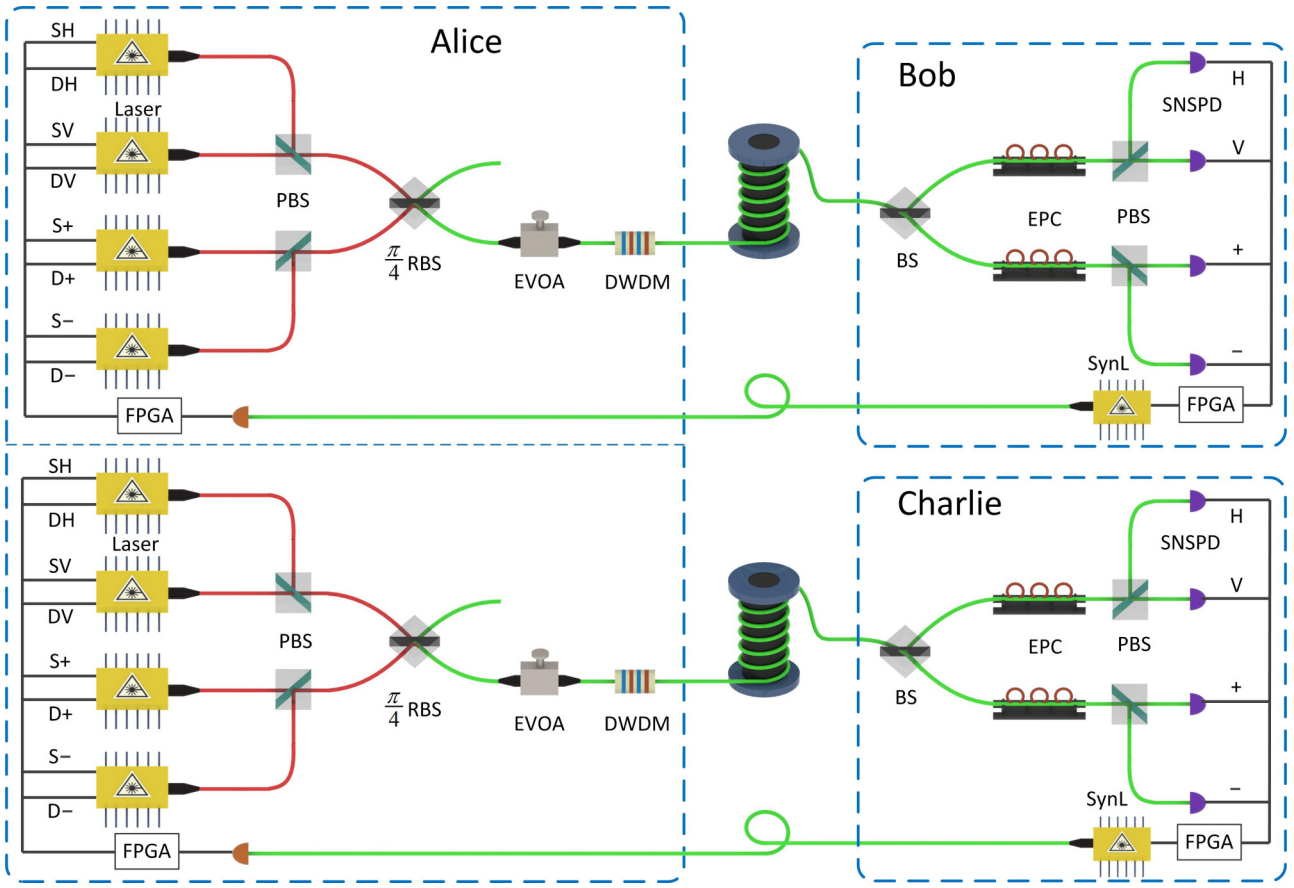

FIG. 1. Experimental setup for quantum digital signature. Alice randomly prepares two copies of BB84 states with decoy state method and sends to Bob and Charlie through two fiber spools, respectively. Bob and Charlie detect the photon with their SNSPDs (superconducting nanowire single-photon detector). PBS, polarization beam splitter; $\frac{\pi}{4}$RBS, $\pi/4$ rotation beam splitter; EVOA, electrical variable optical attenuator; DWDM, dense wavelength division multiplexer; BS, beam splitter; EPC, electric polarization controller; FPGA, filed programmable gate array; SynL, synchronization laser.

is connected to the detector system via single-mode fibers and consists of one beam splitter, two electric polarization controllers (EPCs), and two PBSs. By exploiting the polarization feedback algorithm [33], the EPC is controlled to compensate the polarization fluctuation in the fiber spool. The optical pulses go through the polarization measurement module to be detected by the SNSPD. One additional manual polarization controller of each detector channel is exploited to resolve the polarization sensitivity of the SNSPDs. The insertion loss of the polarization measurement module is around 1.2 dB.

Bob exploits a crystal oscillator circuit to generate 500-kHz electric signals as the synchronization signals of the system. Bob sends synchronization laser pulses (SLPs) at 1570 nm modulated by the 500-kHz electric signals to Alice through an additional fiber. A photoelectric detector and phase-locked loop utilized by Alice detect the SLP and regenerate a system clock frequency of 75 MHz by frequency multiplication as the clock for her four laser diodes. The measurements of Bob and Charlie are independent from each other. It is not necessary for all participants to share one common reference clock. Therefore, Alice exploits another similar setup to send quantum states to Charlie. Therein, the polarization states sent to Bob and Charlie are identical, while the intensities are random.

III. RESULTS

In our experiment, we perform a symmetrical case that the fiber lengths from Alice to Bob and Alice to Charlie are almost the same. The lengths of the fiber spools are 25, 51, 76, and 102 km, respectively. For each distance, we send two groups of quantum states to sign one future bit message in the signature stage, where the first group is used to sign future message bit $m = 0$ and the second group is for bit $m = 1$. The parameter estimation and the message signature are implemented in a local area network connecting the three users.

The bit error rates E_s^B and E_s^C of Bob's and Charlie's conclusive results in the sampling data string are listed in Table I. Exploiting the decoy state method [19], the yield and quantum bit error rate of single-photon pairs can be acquired. The lower bound of the mismatching rate S_{11} can be calculated using Eq. (A1), and S_{11} is shown in Table I. Given that the security bound is $\varepsilon_{\text{sec}} < 10^{-5}$ and the robustness bound is $\varepsilon_{\text{rob}} < 10^{-6}$, the authentication and verification security thresholds T_a and T_v can be chosen with proper values, which are also shown in Table I. More details of experimental results can be found in Appendix B.

Except for proof-of-principle demonstration of a one-bit QDS like all previous experimental demonstrations, we also

TABLE I. The error rates and secure thresholds at different distances in our experiment. Therein, ε_{rep} (ε_{for}) represents the probability of successful repudiation (forgery) attack. N represents the total pulse pairs sent by Alice to sign a half bit.

	25 km 4.9 dB attenuation		51 km 9.8 dB attenuation		76 km 14.8 dB attenuation		102 km 19.8 dB attenuation	
T_v	2.0%		2.0%		1.9%		2.2%	
T_a	0.6%		0.6%		0.55%		0.7%	
Message	$m=0$	$m=1$	$m=0$	$m=1$	$m=0$	$m=1$	$m=0$	$m=1$
E_s^B	0.35%	0.39%	0.37%	0.37%	0.36%	0.29%	0.51%	0.45%
E_s^C	0.26%	0.29%	0.25%	0.22%	0.30%	0.26%	0.42%	0.40%
S_{11}	4.33%	4.21%	4.27%	4.35%	4.28%	4.10%	4.46%	4.42%
Time	20 s	20 s	180 s	180 s	1620 s	1620 s	33420 s	33420 s
N	1.5×10^{9}	1.5×10^{9}	1.35×10^{10}	1.35×10^{10}	1.215×10^{11}	1.215×10^{11}	2.5065×10^{12}	2.5065×10^{12}
ε_{rep}	7.1×10^{-10}	1.4×10^{-6}	1.6×10^{-10}	3.4×10^{-11}	5.3×10^{-8}	4.9×10^{-12}	4.9×10^{-8}	5.7×10^{-13}
ε_{for}	7.4×10^{-15}	5.6×10^{-9}	4.1×10^{-13}	4.1×10^{-12}	2.5×10^{-8}	3.7×10^{-9}	1.4×10^{-19}	7.0×10^{-10}
ε_{rob}	8.2×10^{-12}	3.9×10^{-8}	1.6×10^{-9}	4.6×10^{-10}	1.2×10^{-7}	1.2×10^{-14}	2.2×10^{-9}	2.0×10^{-18}

implement QDS for a longer message. We continuously collect 64 groups and each group has 180 s at the distance of 51 km. The bit error rates of Bob's and Charlie's conclusive results E_s^B and E_s^C in the sampling data string for each group are shown in Fig. 2. We set the security bound to be $\varepsilon_{\text{sec}} < 10^{-5}$ and the robustness bound to be $\varepsilon_{\text{rob}} < 10^{-6}$ for each group. For simplicity, the authentication and verification security thresholds T_a and T_v can be fixed to be 2.0 and 0.6%, respectively. Note that the secure thresholds can be different for each group. We can sign a 32-bit message since two groups need to be used to sign a one-bit message. Before Alice signs the long message, she will publicly announce the length of the message bits. Here, we have successfully signed a 32-bit message "USTC" by taking more than 3 h. The process of signing the message can be found in Fig. 3.

IV. CONCLUSION

We have experimentally demonstrated a QDS protocol without the assumption of any secure channel. Exploiting the decoy state modulation and the BB84 state encoding, we have successfully signed a one-bit message through an up to 102-km optical fiber. Furthermore, we continuously run the system to sign the longer message "USTC" with 32 bits at the distance of 51 km. We remark that it takes 360 s to sign a one-bit message at the distance of 51 km, which currently seems to be not so practical. However, if we implement the full parameter optimization and joint constrained statistical fluctuation [34], combined with the six-state encoding [19], the signature rate will increase obviously with more than two orders of magnitude. In order to increase the practicability of QDS in real-world applications, one may let signal pulses and synchronization pulses multiplex a single fiber. We leave the important work for real-world applications in the future. We

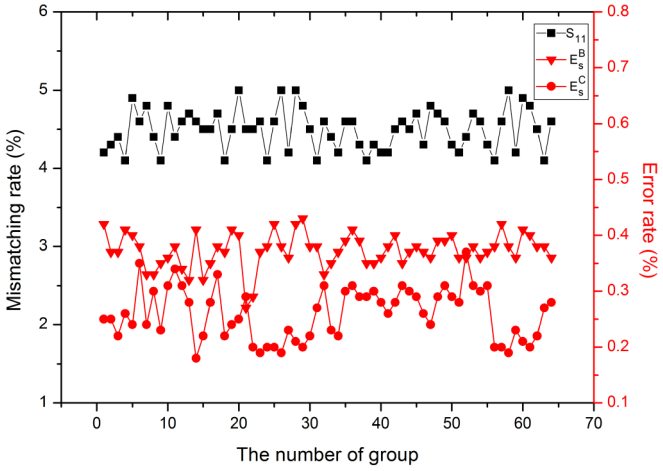

FIG. 2. The error rates and the mismatching rates for each group. The experimental error rates E_s^B (E_s^C) of Bob's (Charlie's) conclusive results in the sampling data string are almost 0.3–0.4% (0.2–0.3%). The mismatching rates S_{11} calculated by Eq. (A1) are almost 4.2–5.0%.

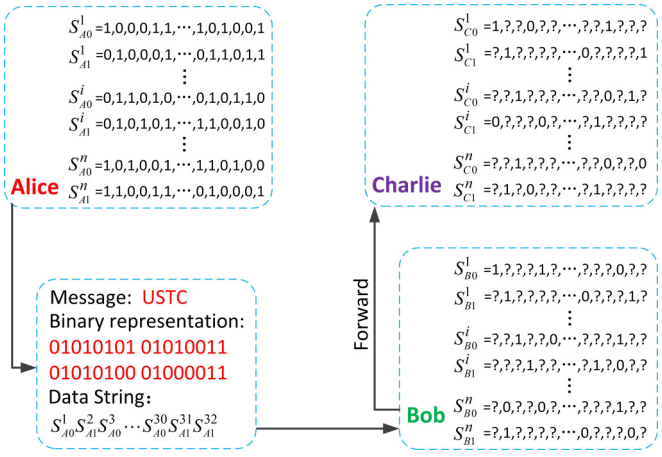

FIG. 3. Demonstration of signing the message string "USTC" in the messaging stage. Alice sends the ASCII code for the message "01010101010100110101010001000011" and the corresponding data string $S_{A0}^1 S_{A1}^2 \cdots S_{A1}^{31} S_{A1}^{32}$ to Bob through the authenticated classical channel. Bob compares the data strings $S_{A0}^1 S_{A1}^2 \cdots S_{A1}^{31} S_{A1}^{32}$ and $S_{B0}^1 S_{B1}^2 \cdots S_{B1}^{31} S_{B1}^{32}$, and accepts the message since the error rate of Bob's conclusive rates is less than T_a for each group. Bob forwards the message and the corresponding data string to Charlie through the authenticated classical channel. Charlie compares the data strings $S_{A0}^1 S_{A1}^2 \cdots S_{A1}^{31} S_{A1}^{32}$ and $S_{C0}^1 S_{C1}^2 \cdots S_{C1}^{31} S_{C1}^{32}$, and accepts the message since the error rate of Charlie's conclusive rates is less than T_v for each group.

TABLE II. List of the total pulses, the total counts, and the error counts in the case of 25 km in the laboratory. Numbers in brackets indicate powers of 10.

		$m=0$			$m=1$		
25 km		0	ν	μ	0	ν	μ
$N_{\alpha\beta}$	0	4.13[06]	2.62[07]	4.47[07]	4.13[06]	2.62[07]	4.47[07]
	ν	2.64[07]	1.85[08]	3.14[08]	2.64[07]	1.85[08]	3.14[08]
	μ	4.45[07]	3.14[08]	5.42[08]	4.45[07]	3.14[08]	5.42[08]
$M_{\alpha\beta}$	0	1	4	13	0	2	13
	ν	3	10743	59590	2	10206	56841
	μ	4	59339	340524	9	56775	323515
$M^B_{\alpha\beta}$	0	0	0	7	0	0	6
	ν	1	2715	14937	1	2545	14330
	μ	3	14778	85049	0	14320	81006
$M^C_{\alpha\beta}$	0	0	1	4	0	1	6
	ν	1	2768	14839	1	2614	14215
	μ	2	14990	84844	4	14108	80513
$E^B_{\alpha\beta}M^B_{\alpha\beta}$	0	0	0	5	0	0	4
	ν	0	13	61	0	10	83
	μ	0	52	283	0	48	335
$E^C_{\alpha\beta}M^C_{\alpha\beta}$	0	0	0	0	0	0	0
	ν	1	8	31	1	8	43
	μ	1	58	188	3	53	212

remark that the polarization drift compensation will become very difficult when the fiber is self-supporting overhead optical cables. The protocol used in our experiment is less efficient than that in Ref. [20] in the long-distance case. But the protocol used in our experiment requires less quantum channels and quantum communication systems.

ACKNOWLEDGMENTS

This work has been supported by the National Fundamental Research Program (under Grant No. 2013CB336800), the National Natural Science Foundation of China (under Grant No. 61125502), the Chinese Academy of Science, the

TABLE III. List of the total pulses, the total counts, and the error counts in the case of 51 km in the laboratory. Numbers in brackets indicate powers of 10.

		$m=0$			$m=1$		
51 km		0	ν	μ	0	ν	μ
$N_{\alpha\beta}$	0	3.72[07]	2.35[08]	4.02[08]	3.72[07]	2.35[08]	4.02[08]
	ν	2.37[08]	1.66[09]	2.82[09]	2.37[08]	1.66[09]	2.82[09]
	μ	4.01[08]	2.82[09]	4.87[09]	4.01[08]	2.82[09]	4.87[09]
$M_{\alpha\beta}$	0	0	2	4	0	0	5
	ν	0	10958	62904	1	11334	62323
	μ	2	61726	359788	2	61619	356586
$M^B_{\alpha\beta}$	0	0	0	2	0	0	2
	ν	0	2805	15806	0	2923	15695
	μ	2	15312	89669	0	15506	89527
$M^C_{\alpha\beta}$	0	0	0	0	0	0	0
	ν	0	2835	15877	1	2818	15491
	μ	0	15518	90300	0	15382	89748
$E^B_{\alpha\beta}M^B_{\alpha\beta}$	0	0	0	1	0	0	1
	ν	0	12	57	0	15	54
	μ	0	70	372	0	59	294
$E^C_{\alpha\beta}M^C_{\alpha\beta}$	0	0	0	0	0	0	0
	ν	0	9	44	0	8	30
	μ	0	40	204	0	31	192

10000-Plan of Shandong Province, and the Science Fund of Anhui Province for Outstanding Youth.

APPENDIX A: DECOY STATE SCHEME AND FINITE-SIZE EFFECT

In this section, we will review the probability of repudiation and forgery attack calculations for the QDS protocol. No one can unambiguously discriminate two copies of quantum states from the four polarization states $|H\rangle,|V\rangle,|+\rangle,|-\rangle$. For the two-photon components, the minimum entropy of Bob about Charlie's conclusive results acquired by the nonorthogonal state encoding scheme [22] can be quantified by the entanglement distillation technique [19,23,24]. The relationship between phase error rate e_p and bit error rate e_b is given by

$$e_p = \min_x\{xe_b + f(x)\},\forall x, \quad \frac{2-\sqrt{2}}{4}e_b \leqslant a \leqslant \frac{2+\sqrt{2}}{4}e_b, \tag{A1}$$

and

$$f(x) = \frac{3-2x+\sqrt{6-6\sqrt{2}x+4x^2}}{6}, \tag{A2}$$

where a is the probability that both bit flip and phase shift occur, which quantifies the mutual information between phase and bit errors. The conditional Shannon entropy function can be given by [19]

$$\begin{aligned} H(e_p|e_b) = &-(1+a-e_b-e_p)\log_2\frac{1+a-e_b-e_p}{1-e_b} \\ &-(e_p-a)\log_2\frac{e_p-a}{1-e_b}-(e_b-a)\log_2\frac{e_b-a}{e_b} \\ &-a\log_2\frac{a}{e_b}. \end{aligned} \tag{A3}$$

The intensity set $\alpha\beta$ represents that Alice sends weak coherent-state pulses to Bob with intensity α and weak coherent-state pulses to Charlie with intensity β. Alice prepares the phase randomized weak coherent-state pulse pairs in the Z basis or X basis with the intensity sets of $\mu\mu$, $\mu\nu$, $\nu\mu$, $\mu 0$, 0μ, $\nu\nu$, $\nu 0$, 0ν, and 00. In the photon-number space, the density matrix for a pulse pair of intensity $\alpha\beta$ can be given by

$$\rho_{\alpha\beta} = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} e^{-\alpha}\frac{\alpha^n}{n!}e^{-\beta}\frac{\beta^m}{m!}|n\rangle\langle n||m\rangle\langle m|. \tag{A4}$$

The effective detection event can be defined as that both Bob and Charlie have a detection click. We denote $N_{\alpha\beta}$ as the number of pulses sent by Alice with the intensity set $\alpha\beta$. $M_{\alpha\beta}$ is the number of effective detection events. $M^B_{\alpha\beta}$ ($M^C_{\alpha\beta}$) is the number of effective detection events given that Bob (Charlie) has the conclusive results. The gain $Q^C_{\alpha\beta}$ is the ratio of $M^C_{\alpha\beta}$ to $N_{\alpha\beta}$. $E^C_{\alpha\beta}$ is the quantum bit error rate in $M^C_{\alpha\beta}$ events.

Denote Y^C_{11} (e^C_{11}) as the yield (bit error rate) of Alice sending single-photon pairs (one photon is sent to Bob and the other is sent to Charlie) and Charlie having conclusive results. Exploiting the decoy state method [19], the lower bound of yield Y^C_{11} and the upper bound of e^C_{11} with analytic form can be written as

$$\begin{aligned} Y^C_{11} \geqslant &\frac{1}{\mu^2\nu^2(\mu-\nu)}\times\{\mu^3[e^{2\nu}Q^C_{\nu\nu}-e^{\nu}(Q^C_{\nu 0}+Q^C_{0\nu})] \\ &-\nu^3[e^{2\mu}Q^C_{\mu\mu}-e^{\mu}(Q^C_{\mu 0}+Q^C_{0\mu})]+(\mu^3-\nu^3)Q^C_{00}\} \end{aligned} \tag{A5}$$

and

$$\begin{aligned} e^C_{11} \leqslant &\frac{1}{\nu^2 Y^C_{11}}[e^{2\nu}E^C_{\nu\nu}Q^C_{\nu\nu}+E^C_{00}Q^C_{00} \\ &-e^{\nu}(E^C_{\nu 0}Q^C_{\nu 0}+E^C_{0\nu}Q^C_{0\nu})]. \end{aligned} \tag{A6}$$

TABLE IV. List of the total pulses, the total counts, and the error counts in the case of 76 km in the laboratory. Numbers in brackets indicate powers of 10.

		$m=0$			$m=1$		
76 km		0	ν	μ	0	ν	μ
$N_{\alpha\beta}$	0	3.34[08]	2.12[09]	3.62[09]	3.34[08]	2.12[09]	3.62[09]
	ν	2.13[09]	1.50[10]	2.54[10]	2.13[09]	1.50[10]	2.54[10]
	μ	3.60[09]	2.54[10]	4.39[10]	3.60[09]	2.54[10]	4.39[10]
$M_{\alpha\beta}$	0	0	0	4	0	0	6
	ν	2	10912	62070	1	10794	61148
	μ	6	62252	363460	3	62362	360661
$M^B_{\alpha\beta}$	0	0	0	2	0	0	0
	ν	1	2681	15491	1	2722	15346
	μ	2	15781	91014	0	15670	90341
$M^C_{\alpha\beta}$	0	0	0	3	0	0	1
	ν	0	2741	15779	0	2785	15198
	μ	2	15716	91624	0	15543	90804
$E^B_{\alpha\beta}M^B_{\alpha\beta}$	0	0	0	1	0	0	0
	ν	0	14	50	0	12	44
	μ	0	52	297	0	45	261
$E^C_{\alpha\beta}M^C_{\alpha\beta}$	0	0	0	0	0	0	0
	ν	0	8	63	0	10	35
	μ	1	45	272	0	60	265

TABLE V. List of the total pulses, the total counts, and the error counts in the case of 102 km in the laboratory. Numbers in brackets indicate powers of 10.

		$m=0$			$m=1$		
102 km		0	ν	μ	0	ν	μ
$N_{\alpha\beta}$	0	6.90[09]	4.37[10]	7.47[10]	6.90[09]	4.37[10]	7.47[10]
	ν	4.41[10]	3.09[11]	5.24[11]	4.41[10]	3.09[11]	5.24[11]
	μ	7.44[10]	5.24[11]	9.05[11]	7.44[10]	5.24[11]	9.05[11]
$M_{\alpha\beta}$	0	0	1	13	0	3	8
	ν	1	21333	120069	1	22744	127079
	μ	11	120257	698071	6	127284	740794
$M^B_{\alpha\beta}$	0	0	0	8	0	0	2
	ν	0	5371	30050	1	5640	31713
	μ	2	29996	175595	3	32088	186024
$M^C_{\alpha\beta}$	0	0	0	2	0	1	1
	ν	0	5411	30174	1	5668	31701
	μ	5	30267	175246	3	32217	185762
$E^B_{\alpha\beta}M^B_{\alpha\beta}$	0	0	0	2	0	0	0
	ν	0	31	182	0	34	127
	μ	0	154	856	1	145	767
$E^C_{\alpha\beta}M^C_{\alpha\beta}$	0	0	0	0	0	0	0
	ν	0	20	113	0	21	162
	μ	2	147	799	0	140	820

We exploit the standard error analysis method [25] to calculate the finite-size effect of decoy state estimation. Thus, we have

$$Q^{CU}_{\alpha\beta} = Q^C_{\alpha\beta}\left(1+\frac{\gamma}{\sqrt{N_{\alpha\beta}Q^C_{\alpha\beta}}}\right), \tag{A7}$$

and

$$Q^{CL}_{\alpha\beta} = Q^C_{\alpha\beta}\left(1-\frac{\gamma}{\sqrt{N_{\alpha\beta}Q^C_{\alpha\beta}}}\right). \tag{A8}$$

where γ is the number of standard deviations, and

$$\epsilon' = \frac{1}{\sqrt{2\pi}}\int_{\gamma}^{\infty} e^{-\frac{t^2}{2}}dt, \tag{A9}$$

where ϵ' is the failure probability for each estimation.

The data string of $\mu 0$, 0μ, $\nu\nu$, $\nu 0$, 0ν, and 00 are all announced publicly to estimate the bit error rate of single-photon pairs in Eq. (A6). Therefore, the data string under the case of three intensity sets $\mu\mu$, $\mu\nu$, and $\nu\mu$ constitutes an overall data string M, i.e., $M = M_{\mu\mu} + M_{\mu\nu} + M_{\nu\mu}$. Similarly, $M^C = M^C_{\mu\mu} + M^C_{\mu\nu} + M^C_{\nu\mu}$ and $M^B = M^B_{\mu\mu} + M^B_{\mu\nu} + M^B_{\nu\mu}$ are the numbers of Bob's and Charlie's conclusive results in the overall data string M, respectively. We denote M_s to be the sampling data string, $M_r = M - M_s$ to be the other data string, M^B_s and M^C_s to be the numbers of Bob's and Charlie's conclusive results in the sampling data string M_s, $M^B_r = M^B - M^B_s$ and $M^C_r = M^C - M^C_s$ to be the numbers of Bob's and Charlie's conclusive results in the other data string M_r. We denote E^B_s and E^C_s to be the quantum bit error rates in M^B_s and M^C_s, respectively.

From the view of Bob and Charlie, only the conclusive results can be used to detect the error (mismatching), while the inconclusive results can only be assumed without mismatching. The mismatching rates of Bob and Charlie in the sampling data string can be given by

$$\Delta^B_s = E^B_s M^B_s/M_s,\ \ \Delta^C_s = E^C_s M^C_s/M_s. \tag{A10}$$

However, from the view of Alice, the status of all data owned by Bob (Charlie) in the data string M could be regarded as the same, since Bob (Charlie) does not announce the position of conclusive results. By using the random sampling without replacement [26], the upper bound of the difference between the data owned by Bob and by Charlie in the other data string can be given by

$$\begin{aligned}&\Delta = \Delta_s + \delta, \quad \Delta_s = \Delta^B_s + \Delta^C_s,\\ &\delta = g[M_s, M_r, \Delta_s, \epsilon],\end{aligned} \tag{A11}$$

where $\epsilon = 10^{-6}$ is the failure probability and

$$g(n,k,\lambda,\epsilon) = \sqrt{\frac{2(n+k)\lambda(1-\lambda)}{nk}\ln\frac{\sqrt{n+k}C(n,k,\lambda)}{\sqrt{2\pi nk\lambda(1-\lambda)}\epsilon}}, \tag{A12}$$

$$C(n,k,\lambda) = \exp\left(\frac{1}{8(n+k)} + \frac{1}{12k} - \frac{1}{12k\lambda+1} - \frac{1}{12k(1-\lambda)+1}\right). \tag{A13}$$

TABLE VI. The counts and error counts of the random sampling.

	25 km		51 km		76 km		102 km	
	$m=0$	$m=1$	$m=0$	$m=1$	$m=0$	$m=1$	$m=0$	$m=1$
M_s	137597	131162	145683	144388	146108	145195	281435	298206
M_r	321856	305969	338735	336140	341674	338976	656962	696951
M_s^B	34378	32689	36542	36247	36650	36634	70967	74697
M_r^B	80386	76967	84245	84481	85636	84723	164674	175128
M_s^C	34203	32660	36491	36226	36754	36529	70616	74828
M_r^C	80470	76176	85204	84395	86365	85016	165071	174852
$E_s^B M_s^B$	119	127	136	134	132	106	364	336
$E_s^C M_s^C$	90	95	90	80	110	94	297	300

By using the Chernoff bound [27,28], the optimal probability of Alice's repudiation attack can be written as [19]

$$\varepsilon_{\text{rep}} = \exp\left[-\frac{\left(A - M_r^B T_a/M_r\right)^2}{2A} M_r\right], \tag{A14}$$

where A is the physical solution of the following equation and inequalities:

$$\frac{\left(A - M_r^B T_a/M_r\right)^2}{2A} = \frac{\left[M_r^C T_v/M_r - (A+\Delta)\right]^2}{3(A+\Delta)},$$
$$M_r^B T_a/M_r < A < \left(M_r^C T_v/M_r - \Delta\right). \tag{A15}$$

The number of the single-photon pairs of Charlie's conclusive results in the other data string can be given by

$$M_{11r}^C = (N_{\mu\mu} e^{-2\mu}\mu^2 + N_{\mu\nu} e^{-\mu-\nu}\mu\nu + N_{\nu\mu} e^{-\mu-\nu}\mu\nu) Y_{11}^C (M_r/M). \tag{A16}$$

We assume that Bob can guess the information of Charlie's conclusive results without error except the single-photon pairs. The lower bound of mismatching rate S_{11} between Bob's declaration and Charlie's conclusive results with single-photon pairs can be given by

$$1 - H\left(e_{p11}^C | e_{11}^C\right) - H(S_{11}) = 0, \tag{A17}$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy function, the phase error rate e_{p11}^C of single-photon pairs can be calculated by Eq. (A1), and $a = \frac{2-\sqrt{2}}{4}$. The optimal probability of Bob's forgery attack is [19]

$$\varepsilon_{\text{for}} = \exp\left[-\frac{(S_{11} - T_{v11})^2}{2S_{11}} M_{r11}^C\right], \tag{A18}$$

where $T_{v11} = T_v M_r^C / M_{r11}^C$ is the error rate threshold of single-photon pairs of Charlie's conclusive results. The secure bound of the protocol can be written as

$$\varepsilon_{\text{sec}} = \varepsilon_{\text{for}} + \varepsilon_{\text{rep}} + \epsilon + 11\epsilon', \tag{A19}$$

where $11\epsilon' = 7 \times 10^{-6}$ is the failure probability due to the decoy state method.

The probability of the robustness is [19]

$$\varepsilon_{\text{rob}} = h\left[M_r, M_s, \Delta_s^B, M_r^B T_a/M_r - \Delta_s^B\right], \tag{A20}$$

where

$$h(n,k,\lambda,t) = \frac{\exp\left[-\frac{nkt^2}{2(n+k)\lambda(1-\lambda)}\right] C(n,k,\lambda)}{\sqrt{2\pi nk\lambda(1-\lambda)/(n+k)}}. \tag{A21}$$

APPENDIX B: EXPERIMENTAL RESULTS

We have performed the QDS experiment in the laboratory. The distances form Alice to Bob (Alice to Charlie) are performed with four cases, i.e., 25-, 51-, 76-, and 102-km fiber spools. Therefore, the maximum distances between Bob and Charlie can be about 50, 102, 152, and 204 km. The secure parameters and important results at different distances in the experiment are shown in Table I. Tables II–V show the details of the total pulses $N_{\alpha\beta}$; the total counts $M_{\alpha\beta}$, $M_{\alpha\beta}^B$, and $M_{\alpha\beta}^C$; and the error rates $E_{\alpha\beta}^B$ and $E_{\alpha\beta}^C$. From the experimental results, we can see that the probabilities of Bob's and Charlie's conclusive results are all approximately 0.25 and in accordance with the theory. Table VI shows the case of random sampling with the probability of 30%.

[1] W. Diffie and M. Hellman, IEEE Trans. Inf. Theory **22**, 644 (1976).
[2] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
[3] P. W. Shor, *Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on* (IEEE, 1994), pp. 124–134.
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[6] J. Qiu, Nature (London) **508**, 441 (2014).
[7] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032.
[8] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[9] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[10] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **90**, 042335 (2014).
[11] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A **91**, 042304 (2015).

[12] J. M. Arrazola, P. Wallden, and E. Andersson, Quantum Inf. Comput. **6**, 0435 (2016).
[13] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[14] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).
[15] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, Phys. Rev. A **93**, 012329 (2016).
[16] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, Phys. Rev. Lett. **117**, 100503 (2016).
[17] M. Hillery, V. Bužek, and A. Berthiaume, Phy. Rev. A **59**, 1829 (1999).
[18] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, Opt. Lett. **41**, 4883 (2016).
[19] H.-L. Yin, Y. Fu, and Z.-B. Chen, Phys. Rev. A **93**, 032316 (2016).
[20] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).
[21] C. H. Bennett and G. Brassard, *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984), pp. 175–179.
[22] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[23] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302 (2006).
[24] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, Sci. Rep. **6**, 29482 (2016).
[25] X. Ma, C.-H. Fred Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[26] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photon. **9**, 163 (2015).
[27] H. Chernoff, Ann. Math. Stat. **23**, 493 (1952).
[28] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[29] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[30] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[31] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[32] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. Fred Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).
[33] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 8587 (2010).
[34] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).