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 Pan¹,²,§

¹National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
²The CAS Center for Excellence in QIQP and the Synergetic Innovation Center for QIQP, University of Science and Technology of China, Hefei, Anhui 230026, China
³State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China

(Dated: August 4, 2016)

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

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 (RSA) protocol [2], whose security is based on the mathematical complexity of 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 the random key with information-theoretical security [4, 5]. Similarly, one can expect to exploit the laws of quantum mechanics to sign a message with the information-theoretical security, which is called quantum digital signature (QDS).

A basic digital signature model will introduce at least three authorized parties, in addition, the three authorized parties cannot be assumed all honest. By contrast, a conventional QKD system has two authorized and honest parties. This is why QKD has entered practical application and networking deployment [6], while the QDS is still on the stage of the security analysis and the proof-of-principle experimental demonstration.

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 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 towards this direction [13–16]. To name a few, Clarke et al. [13] utilize coherent states and linear optics to avoid the nondestructive operation and provides the first experimental try. Collins et al. [14] present a realization without the need of quantum memory, which, however, still needs the assumption of secure quantum channel. Secure quantum channel means that the quantum channel should not be tampered. 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 and tampered with. Therefore, the secure quantum channel is an unrealistic assumption and limits the application of QDS. Meanwhile, the Mach-Zehnder interferometer configuration 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 [18, 19] have been proposed to remove the assumption of secure quantum channel. A kilometer range demonstration for the new protocols is provided [15], which however introduces another assumption of secure classical channel. In this Letter, we provide a complete QDS experiment without quantum or classical secure channel assumption over 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 [18] used in this work. In a digital signature protocol, Alice, the sender, will send a message with a digital signature to two recipients, Bob and Charlie. Without loss of generality, we take Bob as the authenticator. 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 two steps, quantum stage and signature stage. In the quantum stage, for each future possible message \( m = 0, 1 \), Alice exploits weak coherent states (WCS) to randomly prepare two identical qubit states from the BB84 states [20], \(|H\rangle, |V\rangle, |+\rangle\text{ and } |−\rangle\), where \(|H\rangle, |V\rangle\) represent horizontal and vertical polarization states, \(|+\rangle = (1/\sqrt{2})(|H\rangle + |V\rangle)\text{ and } |−\rangle = (1/\sqrt{2})(|H\rangle − |V\rangle)\). In or-
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 beamsplitter, $\frac{\pi}{4}$ 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.

To avoid photon-number splitting attack, Alice exploits the decoy-state method by randomly varying the intensity of the pulses. She chooses three intensities $\mu, \nu, \omega$, one as signal and two as decoy states. Then, Alice randomly sends one qubit state with intensity of $\alpha$ to Bob and the other with intensity of $\beta$ to Charlie, where, $(\alpha, \beta) \in (\mu, \nu, \omega)$. Note that, the polarization states for Bob and Charlie are identical, while the intensities are not necessary to be the same.

Bob and Charlie independently and randomly exploit 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 [21] are used to identify the conclusive outcome and inconclusive outcome. For each quantum state, Bob (Charlie) compares his measurement outcomes with two nonorthogonal states announced by Alice. 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.

Then, the signature process starts. Alice announces the nine intensity sets and also the bit information of six intensity sets, $\mu\omega, \mu\nu, \nu\mu, \nu\omega, \omega\nu$ and $\omega\omega$. Charlie, as the verifier, estimates the yield, $Y_{11}^{C}$ and the quantum bit error rate $e_{11}^{C}$ for single-photon pairs of his conclusive results [18], where a single-photon pair represents that one photon is sent to Bob and one photon is sent to Charlie. Exploiting the entanglement distillation technique [18, 22, 23], the min-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 the Supplemental Material for details). Given the bound of the min-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 [18, 19],

$$1 - H(e_{p11}^{C} | e_{11}^{C}) - H(S_{11}) = 0,$$

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.

On the other hand, the data string under the case of three intensity sets $\mu\mu, \mu\nu, \nu\mu$ constitute an overall data string. Charlie randomly chooses some data from the overall data string as the sampling data string and informs to Alice and Bob. They compare the bit value for the sampling string and estimate the quantum bit error rate of conclusive results, $E_{B}^{C}$ and $E_{C}^{C}$, which are utilized to restrict repudiation from Alice. The remaining data string of Alice, Bob and Charlie are kept for the digital signature, denoted as $S_{Am}$, $S_{Bm}$ and $S_{Cm}$, respectively.
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) do not announce the position of conclusive result. By random sampling, the upper bound of the difference between the data owned by Bob and Charlie can be bounded. With this restrict, 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 [24–27], 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 the robustness. Detailed analysis can be found in the Supplemental Material.

To sign 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 \( T_v \). 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 \( T_v \).

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. We combine the four laser diodes with two PBS and one 45 degree RBS into a single fiber. An electrical variable optical attenuator (EVOA) is used to attenuate the average photon number per pulse to the experimental level. The dense wavelength division multiplexer (DWDM) 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 [28–30] by varying the injection electrical current for the laser diodes. We set the intensities of signal states \( \mu = 0.22 \), decay states \( \nu = 0.066 \) and vacuum states \( \omega = 0 \) and their corresponding probability distributions are \( P_\mu = 65\% \), \( P_\nu = 35\% \) and \( P_\omega = 5\% \), respectively. All random signals for choosing polarization states or intensities are all 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 [31].

In Bob’s side, the detector system contains four superconducting nanowire single-photon detectors (SNSPD) that provide the detection efficiency of 52% at the dark count rate of 10 counts per second. A polarization measurement module is connected to the detector system via single-mode fibers and consists of one beam splitter (BS), two electric polarization controllers (EPC) and two PBS. The EPCs are used for compensation of the polarization fluctuation in the fiber spool. The optical pulses go through the polarization measurement module to be detected by the SNSPD. 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 system. Bob sends synchronization laser pulses (SLP) at 1570 nm modulated by the 500 KHz electric signals to Alice through an additional fiber. A photoelectric detector (PD) 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. Alice exploits the same setup to send quantum states to Charlie.

In our experiment, we perform a symmetrical case that each fiber length from Alice to Bob and Alice to Charlie are almost the same. The length of fiber spool are 25 km, 51 km, 76 km 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 for bit \( m = 1 \). All the parameter estimation and the message signature are implemented in a local area network connecting the three users.

| Distance | 25 km | 51 km | 76 km | 102 km |
|----------|-------|-------|-------|--------|
| Attenuation | 4.9 dB | 9.8 dB | 14.8 dB | 19.8 dB |
| \( T_v \) | 2.0% | 2.0% | 1.9% | 2.2% |
| \( T_a \) | 0.6% | 0.6% | 0.55% | 0.7% |

Note: \( \varepsilon_{\text{rep}} \) represents the probability of successful repudiation (forgery) attack. \( \varepsilon_{\text{for}} \) represents the probability of inconclusive outcome is less than 0.02. \( \varepsilon_{\text{rob}} \) represents the probability of successful forgery attack.
The bit error rates $E_B^B$ and $E_B^C$ of Bob’s and Charlie’s conclusive results in the sampling data string are listed in Table 2. Exploiting the decoy-state method [18], 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. (2) which is shown in Table 2. 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 2. More details of experimental results can be found in the Supplemental Material.

Except for proof-of-principle demonstration of a one-bit QDS like all previous experimental demonstrations, we also implement QDS for a longer message. We continuously collect 64 groups and each group has 180 seconds at the distance of 51 km. The bit error rates of Bob’s and Charlie’s conclusive results $E_B^B$ and $E_B^C$ 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 32 bit message since two groups need to be used to sign 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”. The process of signing the message can be found in Fig. 3.

In summary, 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 one bit message through 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 needs 360 seconds to sign 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 [32], combined with the six-state encoding [18], the signature rate will increase obviously with more than two orders of magnitude.

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

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

[1] W. Diffie and M. Hellman, IEEE Transactions on Information Theory 22, 644 (1976).
[2] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM 21, 120 (1978).
[3] P. W. Shor, in 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 508, 441 (2014).
The conditional Shannon entropy function can be given by
\[
J(x) = \sum_{n,m} p(n|m) \log_2 \frac{1}{p(n|m)},
\]
where \(p(n|m)\) is the probability that Bob observes outcome \(n\) given that Charlie observes outcome \(m\).

In the section, we will review the probability of repudiation and forgery attack calculations for the quantum digital signature (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 min-entropy of Bob about Charlie’s conclusive results acquired by the nonorthogonal state encoding scheme [21] can be quantified by the entanglement distillation technique [18, 22, 23]. The relationship between phase error rate \(e_p\) and the bit error rate \(e_b\) is given by
\[
e_p = \min_x \left\{ xe_b + f(x) \right\}, \quad \forall x, \quad \frac{2 - \sqrt{2}}{4} e_b \leq a \leq \frac{2 + \sqrt{2}}{4} e_b,
\]
and
\[
f(x) = \frac{3 - 2x + \sqrt{6 - 6\sqrt{2}x + 4x^2}}{6},
\]
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 [18]
\[
H(e_p|e_b) = -(1 + a - e_b - e_p) \log_2 \frac{1 + a - e_b - e_p}{1 - e_b} - (e_p - a) \log_2 \frac{e_p - a}{1 - e_b} - (e_b - a) \log_2 \frac{e_b - a}{e_b} - a \log_2 \frac{a}{e_b}.
\]

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. \(M_{\alpha\beta}^{\text{C}}(M_{\alpha\beta})\) is the number of
effective detection events given that Bob (Charlie) has the conclusive results. The gain $Q_{\alpha\beta}^{C}$ is the ratio of $M_{\alpha\beta}^{C}$ to $N_{\alpha\beta}$. $E_{\alpha\beta}^{C}$ is the quantum bit error rate in $M_{\alpha\beta}^{C}$ events.

Denote $Y_{11}^{C}$ ($e_{11}^{C}$) as the yield (bit error rate) of Alice sending single-photon pairs and Charlie having conclusive results. Exploiting the decoy-state method [18], the lower bound of yield $Y_{11}^{C}$ and the upper bound of $e_{11}^{C}$ with analytic form can be written as

$$Y_{11}^{C} \geq \frac{1}{\mu^{2}\nu^{2}(\mu - \nu)} \times \left\{ \mu^{3} [e^{2\nu}Q_{\nu \nu}^{C} - e^{\nu}(Q_{\nu \nu}^{C} + Q_{\nu 0}^{C})] - \nu^{3} [e^{2\mu}Q_{\mu \mu}^{C} - e^{\mu}(Q_{\mu 0}^{C} + Q_{0 0}^{C})] + (\mu^{3} - \nu^{3})Q_{0 0}^{C} \right\}$$ (6)

and

$$e_{11}^{C} \leq \frac{1}{\nu^{2}Y_{11}^{C}} \left[ e^{2\nu}E_{\nu \nu}^{C}Q_{\nu \nu}^{C} - e^{\nu}(E_{\nu 0}^{C}Q_{\nu 0}^{C} + E_{0 0}^{C}Q_{0 0}^{C}) + E_{0 0}^{C}Q_{0 0}^{C} \right].$$ (7)

We exploit the standard error analysis method [24] to calculate the finite-size effect of decoy state estimation. Thus, we have

$$Q_{\mu \nu}^{CU} = Q_{\mu \nu}^{C} \left( 1 + \frac{\gamma}{\sqrt{N_{\mu \nu}Q_{\mu \nu}^{C}}} \right), \quad Q_{\mu \nu}^{CL} = Q_{\mu \nu}^{C} \left( 1 - \frac{\gamma}{\sqrt{N_{\mu \nu}Q_{\mu \nu}^{C}}} \right).$$ (8)

where $\gamma$ is the number of standard deviations, and

$$e' = \frac{1}{\sqrt{2\pi}} \int_{\gamma}^{\infty} e^{-t^{2}/2} dt,$$ (9)

where $e'$ is the failure probability for each estimation.

The data string of $\mu 0, 0\mu, \nu \nu, \nu 0, 0\nu$ and 00 are all announced publicly to estimate the bit error rate of single-photon pairs in Eq. (7). Therefore, the data string under the case of three intensity sets $\mu \mu, \nu \nu$ and $\nu 0$ constitutes an overall data string $M$, i.e., $M = M_{\mu\mu} + M_{\nu\nu} + M_{\nu 0}$. Similarly, $M^{C} = M_{\mu\mu}^{C} + M_{\nu\nu}^{C} + M_{\nu 0}^{C}$ and $M^{B} = M_{\mu\mu}^{B} + M_{\nu\nu}^{B} + M_{\nu 0}^{B}$ 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 rest data string, $M_{s}^{B}$ and $M_{s}^{C}$ to be the numbers of Bob’s and Charlie’s conclusive results in the sampling data string $M_{s}$, $M_{r}^{B} = M^{B} - M_{s}^{B}$ and $M_{r}^{C} = M^{C} - M_{s}^{C}$ to be the numbers of Bob’s and Charlie’s conclusive results in the rest data string $M_{r}$. We denote $E_{s}^{B}$ and $E_{s}^{C}$ to be the quantum bit error rates in $M_{s}^{B}$ and $M_{s}^{C}$, 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’s and Charlie’s in the sampling data string can be given by

$$\Delta_{s}^{B} = E_{s}^{B}M_{s}^{B}/M_{s}, \quad \Delta_{s}^{C} = E_{s}^{C}M_{s}^{C}/M_{s}.$$ (10)

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 [25], the upper bound of the difference between the data owned by Bob and by Charlie in the rest data string can be given by

$$\Delta = \Delta_{s} + \delta, \quad \Delta_{s} = \Delta_{s}^{B} + \Delta_{s}^{C}, \quad \delta = g[M_{s}, M_{r}, \Delta_{s}, \epsilon],$$ (11)

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

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

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

By using the Chernoff Bound [26, 27], the optimal probability of Alice’s repudiation attack can be written as [18]

$$\varepsilon_{rep} = \exp \left[ - \frac{(A - M_{r}^{BT_{a}}/M_{r})^{2}}{2A} \right].$$ (13)
where \( A \) is the physical solution of the following equation and inequalities,

\[
\frac{(A - M^B_T a/M_r)^2}{2A} = \left[ \frac{M^C_T v/M_r - (A + \Delta)}{3(A + \Delta)} \right]^2, \\
M^B_T a/M_r < A < (M^C_T v/M_r - \Delta).
\] (14)

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

\[
M_{11r}^C = (M_r/M)(N_{\mu\mu}e^{-2\mu\mu} + N_{\mu\nu}e^{-\mu\nu}M_r^C + N_{\nu\mu}e^{-\nu\mu}M_r^C)Y_{11}^C.
\] (15)

We assume that Bob can guess the information of Charlie’s conclusive results without error unless 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

\[
1 - H(e_{p11}^C|e_{11}^C) - H(S_{11}) = 0,
\] (16)

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. (2) and \( a = \frac{2 - \sqrt{2}}{4} \). The optimal probability of Bob’s forgery attack is [18]

\[
\varepsilon_{\text{for}} = \exp \left[ -\frac{(S_{11} - T_{v11})^2}{2S_{11}}M_r^C \right],
\] (17)

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

\[
\varepsilon_{\text{sec}} = \varepsilon_{\text{for}} + \varepsilon_{\text{rep}} + \epsilon + 11\epsilon'.
\] (18)

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

The probability of the robustness is [18]

\[
\varepsilon_{\text{rob}} = h[M_r, M_a, \Delta^B_a, M^B_T a/M_r - \Delta^B_a].
\] (19)

where

\[
h(n, k, \lambda, t) = \frac{\exp \left[ -\frac{nk^2}{2(n+k)\lambda} \right]}{\sqrt{2\pi nk\lambda(1-\lambda)}/(n+k)}.
\] (20)

**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 km, 51 km, 76 km and 102 km fiber spools. Therefore, the maximum distances between Bob and Charlie can be about 50 km, 102 km, 152 km, 204 km. The secure parameters and important results at different distances in the experiment are shown in Table 2. Tables 3-6 show the details of the total pulses \( N_{\alpha\beta} \), the total counts \( M_{\alpha\beta} \), \( M^B_{\alpha\beta} \), 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 7 shows the case of the random sampling with the probability of 30%.
TABLE 2: The secure parameters at different distances in the experiment.

| Distance | 25km | 51km | 76km | 102km |
|----------|------|------|------|-------|
| Attenuation | 4.9dB | 9.8dB | 14.8dB | 19.8dB |
| $T_v$ | 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 |
| Total pulse | 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 |
| Time | 20s | 20s | 180s | 180s | 1620s | 1620s | 33420s | 33420s |
| $e_{11}^C$ | 1.12% | 1.20% | 1.16% | 1.10% | 1.15% | 1.29% | 1.03% | 1.05% |
| $Y_{11}^C$ | 2.74 × 10^{-3} | 2.55 × 10^{-3} | 3.20 × 10^{-4} | 3.09 × 10^{-4} | 3.29 × 10^{-5} | 3.42 × 10^{-5} | 3.42 × 10^{-6} | 3.48 × 10^{-6} |
| $S_{11}$ | 4.33% | 4.21% | 4.27% | 4.35% | 4.28% | 4.10% | 4.46% | 4.42% |
| $\varepsilon_{\text{rep}}$ | 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} |
| $\varepsilon_{\text{tot}}$ | 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} |
| $\varepsilon_{\text{rob}}$ | 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} |

TABLE 3: List of the total pulses, the total counts and the error counts in the case of 25 km in the laboratory.

| 25km | m=0 | m=1 | m=0 | m=1 | m=0 | m=1 | m=0 | m=1 |
|------|------|------|------|------|------|------|------|------|
| $N_{\mu\nu}$ | 0 | 4.13E+06 | 2.62E+07 | 4.47E+07 | 0 | 4.13E+06 | 2.62E+07 | 4.47E+07 |
| $\mu$ | 2.64E+07 | 1.85E+08 | 3.14E+08 | 0 | 2.64E+07 | 1.85E+08 | 3.14E+08 |
| $\nu$ | 4.45E+07 | 3.14E+08 | 5.42E+08 | 0 | 4.45E+07 | 3.14E+08 | 5.42E+08 |
| $M_{\mu\nu}$ | 0 | 1 | 13 | 0 | 2 | 13 |
| $\nu$ | 3 | 10743 | 59590 | 2 | 10206 | 56841 |
| $\mu$ | 4 | 59339 | 340524 | 9 | 56775 | 323515 |
| $M_B^{\mu\nu}$ | 0 | 0 | 7 | 0 | 0 | 6 |
| $\nu$ | 1 | 2715 | 14937 | 1 | 2545 | 14330 |
| $\mu$ | 3 | 14778 | 85049 | 0 | 14320 | 81006 |
| $M_C^{\mu\nu}$ | 0 | 1 | 4 | 0 | 1 | 6 |
| $\nu$ | 1 | 2768 | 14839 | 1 | 2614 | 14215 |
| $\mu$ | 2 | 14990 | 84844 | 4 | 14108 | 80513 |
| $E_B^{\mu\nu}M_B^{\mu\nu}$ | 0 | 0 | 1 | 0 | 1 | 4 |
| $\nu$ | 0 | 13 | 61 | 0 | 10 | 83 |
| $\mu$ | 0 | 52 | 283 | 0 | 48 | 335 |
| $E_C^{\mu\nu}M_C^{\mu\nu}$ | 0 | 0 | 0 | 0 | 0 | 0 |
| $\nu$ | 1 | 8 | 31 | 1 | 8 | 43 |
| $\mu$ | 1 | 58 | 188 | 3 | 53 | 212 |
TABLE 4: List of the total pulses, the total counts and the error counts in the case of 51 km in the laboratory.

| 51km | m=0 | m=1 |
|------|-----|-----|
|      | ν | µ | ν | µ |
| \(N_{νμ}\) | 0 | 3.72E+07 | 2.35E+08 | 4.02E+08 | 3.72E+07 | 2.35E+08 | 4.02E+08 |
|      | ν | 3.72E+07 | 2.35E+08 | 4.02E+08 | 3.72E+07 | 2.35E+08 | 4.02E+08 |
|      | µ | 4.02E+08 | 2.35E+08 | 4.02E+08 | 4.02E+08 | 2.35E+08 | 4.02E+08 |
| \(M_{νμ}\) | 0 | 0 | 2 | 4 | 0 | 0 | 5 |
|      | ν | 0 | 10958 | 62904 | 0 | 11334 | 62323 |
|      | µ | 2 | 61726 | 359788 | 2 | 61619 | 356586 |
| \(M_{νμ}^B\) | 0 | 0 | 0 | 2 | 0 | 0 | 2 |
|      | ν | 0 | 2805 | 15806 | 0 | 2923 | 15695 |
|      | µ | 2 | 15312 | 89669 | 0 | 15506 | 89527 |
| \(M_{νμ}^C\) | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|      | ν | 0 | 2835 | 15877 | 1 | 2818 | 15491 |
|      | µ | 0 | 15518 | 90300 | 0 | 15382 | 89748 |
| \(E_{νμ}^B M_{νμ}^B\) | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
|      | ν | 0 | 12 | 57 | 0 | 15 | 54 |
|      | µ | 0 | 70 | 372 | 0 | 59 | 294 |
| \(E_{νμ}^C M_{νμ}^C\) | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|      | ν | 0 | 9 | 44 | 0 | 8 | 30 |
|      | µ | 0 | 40 | 204 | 0 | 31 | 192 |

TABLE 5: List of the total pulses, the total counts and the error counts in the case of 76 km in the laboratory.

| 76km | m=0 | m=1 |
|------|-----|-----|
|      | ν | µ | ν | µ |
| \(N_{νμ}\) | 0 | 3.34E+08 | 2.12E+09 | 3.62E+09 | 3.34E+08 | 2.12E+09 | 3.62E+09 |
|      | ν | 2.12E+09 | 1.50E+10 | 2.54E+10 | 2.12E+09 | 1.50E+10 | 2.54E+10 |
|      | µ | 3.62E+09 | 2.54E+10 | 4.39E+10 | 3.62E+09 | 2.54E+10 | 4.39E+10 |
| \(M_{νμ}\) | 0 | 0 | 4 | 0 | 0 | 6 |
|      | ν | 2 | 10912 | 62070 | 1 | 10794 | 61148 |
|      | µ | 6 | 62252 | 363460 | 3 | 62362 | 360661 |
| \(M_{νμ}^B\) | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
|      | ν | 1 | 2681 | 15491 | 1 | 2722 | 15346 |
|      | µ | 2 | 15781 | 91014 | 0 | 15670 | 90341 |
| \(M_{νμ}^C\) | 0 | 0 | 0 | 3 | 0 | 0 | 1 |
|      | ν | 0 | 2741 | 15779 | 0 | 2785 | 15198 |
|      | µ | 2 | 15716 | 91624 | 0 | 15543 | 90804 |
| \(E_{νμ}^B M_{νμ}^B\) | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
|      | ν | 0 | 14 | 50 | 0 | 12 | 44 |
|      | µ | 0 | 52 | 297 | 0 | 45 | 261 |
| \(E_{νμ}^C M_{νμ}^C\) | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|      | ν | 0 | 8 | 63 | 0 | 10 | 35 |
|      | µ | 1 | 45 | 272 | 0 | 60 | 265 |
TABLE 6: List of the total pulses, the total counts and the error counts in the case of 102 km in the laboratory.

| 102km | m=0 |  | m=1 |  |  |  | m=0 |  | m=1 |  |  |  | m=0 |  | m=1 |  |  |  |
|-------|-----|---|-----|---|---|---|-----|---|-----|---|---|---|-----|---|-----|---|---|---|
|       |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |
| $N_{\mu\nu}$ |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |
| $M_{\mu\nu}$ |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |
| $M_{\mu\nu}^B$ |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |
| $M_{\mu\nu}^C$ |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |
| $E_{\mu\nu}B_{\mu\nu}$ |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |
| $E_{\mu\nu}C_{\mu\nu}$ |     |   |     |   |   |   |     |   |     |   |   |   |     |   |     |   |   |   |

TABLE 7: The counts and error rates of the random sampling.

| Distance | 25km  | 51km  | 76km  | 102km |
|----------|-------|-------|-------|-------|
|          | 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|
| $M_{B,s}$| 34378 | 32689 | 36542 | 36247 | 36650 | 36634 | 70967 | 74697 |
| $M_{B,r}$| 80386 | 76967 | 84245 | 84481 | 85636 | 84723 | 164674| 175128|
| $M_{C,s}$| 34203 | 32660 | 36491 | 36226 | 36754 | 36529 | 70616 | 74828 |
| $M_{C,r}$| 80470 | 76176 | 85204 | 84395 | 86365 | 85016 | 165071| 174852|
| $E_{B,s}^BM_{B,s}$ | 119 | 127 | 136 | 134 | 132 | 106 | 364 | 336 |
| $E_{C,s}^CM_{C,s}$ | 90 | 95 | 90 | 80 | 110 | 94 | 297 | 300 |