Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution

Xuyang Wang,[1,2,*] Wenyuan Liu,[1] Pu Wang,[1] and Yongmin Li[1,2,†]

[1]*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, People's Republic of China*

[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, People's Republic of China*

(Received 17 April 2017; published 26 June 2017)

We experimentally demonstrated an all-fiber-based unidimensional continuous-variable quantum key distribution (CV QKD) protocol and analyzed its security under collective attack in realistic conditions. A pulsed balanced homodyne detector, which could not be accessed by eavesdroppers, with phase-insensitive efficiency and electronic noise, was considered. Furthermore, a modulation method and an improved relative phase-locking technique with one amplitude modulator and one phase modulator were designed. The relative phase could be locked precisely with a standard deviation of 0.5° and a mean of almost zero. Secret key bit rates of 5.4 kbps and 700 bps were achieved for transmission fiber lengths of 30 and 50 km, respectively. The protocol, which simplified the CV QKD system and reduced the cost, displayed a performance comparable to that of a symmetrical counterpart under realistic conditions. It is expected that the developed protocol can facilitate the practical application of the CV QKD.

DOI: 10.1103/PhysRevA.95.062330

I. INTRODUCTION

The unconditional security of a quantum key distribution (QKD) relies on quantum physics phenomena, for instance, the uncertainty principle and the quantum noncloning theorem. Various QKD protocols exist, which can generally be categorized as discrete-variable or continuous-variable (CV) QKD protocols [1–3]. The CV protocol promises higher key rates at a relatively short distance; this protocol encodes the key into continuous-spectrum quantum observables and utilizes homodyne detectors instead of single-photon detectors. As a result of continuous efforts from scientists and engineers, CV QKD theory and technology have developed rapidly over the past decade [4–24].

To promote the wide application of CV QKD, numerous approaches to further simplification have been proposed. For example, switching from squeezed-state to coherent-state protocols, from Gaussian-modulation to non-Gaussian-modulation coherent-state protocols, and from symmetrical to asymmetrical coherent-state protocols has been proposed. The recently proposed asymmetric unidimensional (UD) coherent-state protocol allows the sender, Alice, to use one modulator instead of two, thereby reducing the complexity and cost of Alice's apparatus [25]. Almost simultaneously to this development, UD CV QKD was realized experimentally with a continuous laser beam modulated in phase quadrature using one phase modulator [26]. However, the method employing one phase modulator only on Alice's side is not suitable for experiments involving pulsed laser beams. To achieve a UD Gaussian distribution with pulsed laser beams in the phase space, Alice should use a single-amplitude modulator instead; however, this leads to the problem of phase locking. To lock the relative phase, one amplitude and two phase modulators were used in previous CV QKD experiments with a pulsed laser [27]. The amplitude modulator and phase modulator on Alice's side were employed to modulate the test pulses used to lock the relative phase, while the phase modulator on the side of the receiver, Bob, was utilized to lock the relative phase using the feedback voltage.

In this paper, we analyze the security of the UD CV QKD protocol under realistic conditions, and experimentally demonstrate the protocol in a pulsed light regime with a single-amplitude modulator. To this end, we design an improved phase-locking method, which utilizes one amplitude modulator on Alice's side, one phase modulator on Bob's side, and a digital proportional-integral-derivative (PID) feedback control technique. The relative phase can be locked precisely with a standard deviation of 0.5° and a mean of almost 0°. Further, the UD modulation can occur in either the amplitude or phase quadrature, depending on the locked phase on Bob's side. The experimental results show that the performance of the UD protocol is comparable to those achievable using the symmetrical counterpart. Such an asymmetrical basis switch decreases the amount of information for the public declaration of Bob's measurement bases, while facilitating Alice's key sifting.

In Sec. II, the security of the UD CV QKD protocol under realistic conditions is analyzed using the entanglement-based (EB) scheme. Section III describes our all-fiber-based experimental setup designed to implement the UD protocol, and details the UD-modulation method and the improved relative phase-locking technique. Section IV presents the experimental results and analysis. Finally, Sec. V presents the conclusions.

II. UD PROTOCOL UNDER REALISTIC CONDITIONS

A. UD protocol model under realistic conditions

The prepare-and-measure scheme and the EB scheme of the UD protocol are illustrated in Figs. 1(a) and 1(b),

*wangxuyang@sxu.edu.cn
†yongmin@sxu.edu.cn

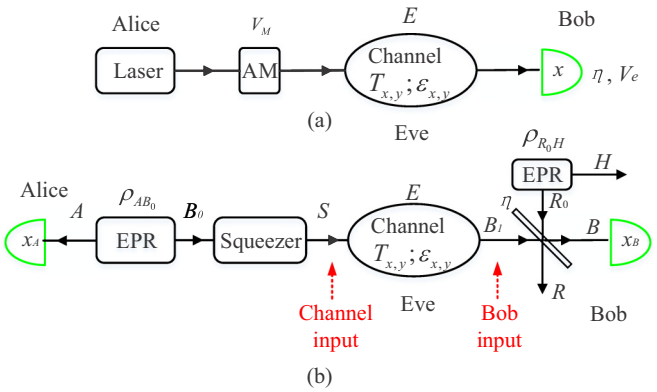

FIG. 1. UD protocol schemes. (a) Prepare-and-measure scheme. (b) EB scheme.

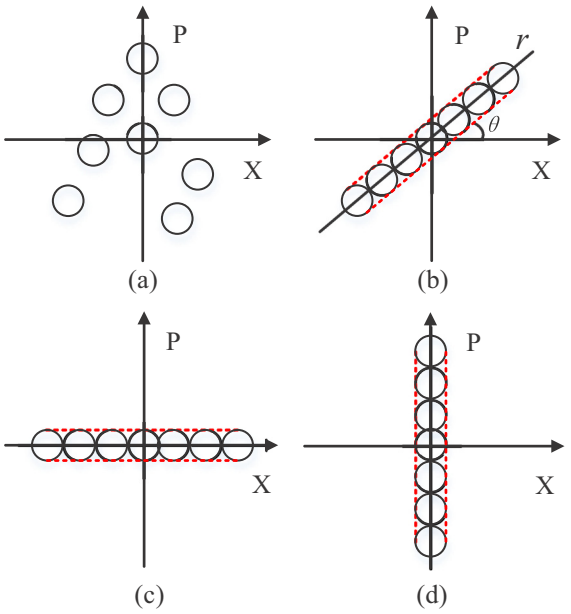

FIG. 2. Modulated coherent states of UD protocol in phase space (a) without relative phase locking and with relative phase locked to (b) θ, (c) zero, and (d) $\pi/2$.

respectively. In the prepare-and-measure scheme, the sender (Alice) produces a series of coherent states using a pulsed laser source, and then distributes the coherent states with modulation variance V_M utilizing the amplitude modulator. These states are sent to the remote, trusted party (Bob) through a phase-sensitive channel with transmittance $T_{x,y}$ and excess noise $\varepsilon_{x,y}$, where x and y represent the amplitude and phase quadratures, respectively. Bob then measures the modulated states using a pulsed balanced homodyne detector (PBHD) with detection efficiency η and electronic noise V_e. Under realistic conditions, it is assumed that the eavesdropper (Eve) is unable to access Bob's apparatus [14].

In CV QKD, the relative phase between the signal and local oscillator (LO) pulses should be locked using the phase modulator inside Bob's apparatus. The fundamental principle of relative phase locking is that the phase of the LO beam is delayed by a phase modulator, to which a feedback voltage is applied in real time. Thus the phase of the signal beam could be any value during transmission. It can be inferred that the dimension is in neither amplitude nor phase quadrature without relative phase locking, as shown in Fig. 2(a). Thus it is also supposed that η is unrelated to the relative phase or is phase insensitive under realistic conditions.

When the relative phase is locked to θ, the states lie only along the direction r with angle θ, as depicted in Fig. 2(b). When the relative phase is locked to zero, the states will be in amplitude quadrature x, as illustrated in Fig. 2(c). Similarly, when the relative phase is locked to $\pi/2$, the states will be in phase quadrature y, as shown in Fig. 2(d). Thus it can be inferred that the modulated quadrature does not depend on the amplitude modulator on Alice's side, but on the relative phase locked using the phase modulator on Bob's side. Without loss of generality, the modulated dimension in amplitude quadrature is used in the following discussion.

It is well known that a protocol in the prepare-and-measure scheme can be equivalent to a protocol in the EB scheme, which allows the explicit description of the modes [3]. The UD protocol in the EB scheme is illustrated in Fig. 1(b), where an Einstein-Podolsky-Rosen (EPR) source on Alice's side is used. In pulsed laser source experiments, an EPR source is equivalent to a two-mode squeezed vacuum state ρ_{AB_0} with variance V in shot noise units. Note that the variances in this paper are all normalized to shot noise units. The Gaussian state ρ_{AB_0} is completely determined by its covariance matrix γ_{AB_0}, with the following form:

$$\gamma_{AB_0} = \begin{bmatrix} VI & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & VI \end{bmatrix}, \tag{1}$$

where

$$\mathrm{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2}$$

Then the mode B_0 is squeezed using $r = \ln\sqrt{V}$, resulting in the covariance matrix γ_{AS}, which is given by

$$\gamma_{AS} = (I \oplus SQ)\gamma_{AB_0}(I \oplus SQ)^T = \begin{bmatrix} V & 0 & \sqrt{V(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\frac{V^2-1}{V}} \\ \sqrt{V(V^2-1)} & 0 & V^2 & 0 \\ 0 & -\sqrt{\frac{V^2-1}{V}} & 0 & 1 \end{bmatrix}, \tag{3}$$

where

$$SQ = \begin{bmatrix} e^{r} & 0 \\ 0 & e^{-r} \end{bmatrix} = \begin{bmatrix} \sqrt{V} & 0 \\ 0 & 1/\sqrt{V} \end{bmatrix}. \tag{4}$$

In the EB scheme, mode S has a variance of V^2 in the amplitude quadrature and a variance of 1 in phase quadrature. It is equivalent to the Gaussian modulation of coherent states with variance $V_M = V^2 - 1$ in amplitude quadrature and no modulation in phase quadrature in the prepare-and-measure scheme. After transmission through the channel characterized by efficiency $T_{x,y}$ and excess noise $\varepsilon_{x,y}$, the covariance matrix γ_{AB_1} achieves the following form:

$$\gamma_{AB_1} = \begin{bmatrix} V & 0 & \sqrt{T_x V(V^2-1)} & 0 \\ 0 & V & 0 & C_y \\ \sqrt{T_x V(V^2-1)} & 0 & T_x(V^2+\chi_{\text{linex}}) & 0 \\ 0 & C_y & 0 & V_y^{B_1} \end{bmatrix}, \tag{5}$$

where $\chi_{\text{linex}} = (1-T_x)/T_x + \varepsilon_x$ is the total noise added relative to the channel input in amplitude quadrature and $(1-T_x)/T_x$ is the noise due to losses. T_x and ε_x can be determined based on the public amplitude quadratures and $V_y^{B_1}$ is the output variance of mode B_1 in the phase quadrature. As the phase quadrature is not modulated, the correlation C_y between Alice and Bob in phase quadrature is unknown. Further, $V_y^{B_1}$ in the phase quadrature should be measured by randomly switching the detection bases to $\pi/2$. The unknowns $V_y^{B_1}$ and C_y are bounded by the Heisenberg uncertainty principle, which can be expressed in terms of covariance matrices as

$$\gamma_{AB_1} + i\Omega \geqslant 0, \tag{6}$$

where

$$\Omega = \bigoplus_{k=1}^{N=2} \omega \quad \text{and} \quad \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{7}$$

Fortunately, it has been proven that there exists a $V_y^{B_1}$ region in which the protocol is secure for any C_y bounded by the Heisenberg uncertainty principle. As C_y is not estimated, the pessimistic value C_y^p corresponding to the minimum secret key rate should be considered [25].

In the EB scheme, the detector can be modeled as a beam splitter with transmission η and a perfect PBHD. The electronic noise V_e of the PBHD can be modeled by a thermal state ρ_{R_0} with variance V_N entering the other input port of the beam splitter; V_N is given by

$$V_N = 1 + V_e/(1-\eta). \tag{8}$$

The thermal state ρ_{R_0} could be considered as the reduced state obtained from a two-mode squeezed vacuum state $\rho_{R_0 H}$. Then the covariance matrix γ_{AB} characterizing the state ρ_{AB} after the beam splitter is given by

$$\gamma_{AB} = \begin{bmatrix} V & 0 & \sqrt{\eta T_x V(V^2-1)} & 0 \\ 0 & V & 0 & C_y\sqrt{\eta} \\ \sqrt{\eta T_x V(V^2-1)} & 0 & \eta T_x(V^2+\chi_{\text{tot}}) & 0 \\ 0 & C_y\sqrt{\eta} & 0 & \eta V_y^{B_1} + V_N(1-\eta) \end{bmatrix}, \tag{9}$$

where $\chi_{\text{tot}} = \chi_{\text{linex}} + \chi_{\text{hom}}/T_x$ is the total noise added between Alice and Bob relative to the channel input in the amplitude quadrature, and $\chi_{\text{hom}} = (1-\eta)/\eta + V_e/\eta$ is the total noise introduced by the realistic PBHD relative to Bob's input in the amplitude quadrature.

B. Secret key rate under collective attack

In the calculations presented in this section, a collective attack from Eve is considered to determine the lower bound of the secret key rate ΔI. The expression for calculating ΔI in the case of reverse reconciliation is

$$\Delta I = \beta I_{AB} - \chi_{BE}, \tag{10}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, β is the reverse reconciliation efficiency, and χ_{BE} is the maximum information accessed by Eve bounded by the Holevo quantity. I_{AB} can be calculated directly using Shannon's equation as follows:

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}, \tag{11}$$

where V_A is the amplitude quadrature variance for Alice, being the first diagonal element of matrix γ_A describing mode A. Further, $V_{A|B}$ is the conditional variance in amplitude quadrature and is the first diagonal element of the conditional matrix $\gamma_{A|B}$, which is given by

$$\gamma_{A|B} = \gamma_A - \sigma_{AB}(X\gamma_B X)^{MP}\sigma_{AB}^T, \tag{12}$$

where

$$X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}; \tag{13}$$

γ_A, γ_B, and σ_{AB} are all submatrices of the covariance matrix γ_{AB} and appear in the decomposition of matrix γ_{AB} in Eq. (14); and MP represents the Moore-Penrose matrix inverse.

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB}^T & \gamma_B \end{bmatrix}. \tag{14}$$

Eve's accessible information can be calculated using

$$\chi_{BE} = S(\rho_E) - S\left(\rho_E^{x_B}\right), \tag{15}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ. For an n-mode Gaussian state ρ, this entropy can be calculated

using the symplectic eigenvalues of the covariance matrix γ characterizing ρ as follows:

$$S(\rho) = \sum_i G\left(\frac{\lambda_i - 1}{2}\right), \tag{16}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. Usually, the symplectic eigenvalues of a covariance matrix γ with N modes can be calculated by finding the absolute eigenvalues of matrix $i\Omega\gamma$.

As states ρ_{AB_1E} and $\rho^{x_B}_{\mathrm{ARHE}}$ are pure, $S(\rho_E) = S(\rho_{AB_1})$ and $S(\rho^{x_B}_{\mathrm{ARH}}) = S(\rho^{x_B}_E)$ [14]. The entropy $S(\rho_{AB})$ can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ of the covariance matrix γ_{AB_1}. Similarly, the entropy $S(\rho^{x_B}_{\mathrm{ARH}})$ can be determined from the symplectic eigenvalues $\lambda_{3,4,5}$ of the covariance matrix $\gamma^{x_B}_{\mathrm{ARH}}$. Matrix $\gamma^{x_B}_{\mathrm{ARH}}$ characterizing state $\rho^{x_B}_{\mathrm{ARH}}$ after Bob's projective measurement can be determined using the following equation:

$$\gamma^{x_B}_{\mathrm{ARH}} = \gamma_{\mathrm{ARH}} - \sigma_{\mathrm{ARH};B}(X\gamma_B X)^{MP}\sigma^T_{\mathrm{ARH};B}. \tag{17}$$

Matrices γ_{ARH}, γ_B, and $\sigma_{\mathrm{ARH};B}$ appear in the decomposition of matrix γ_{ARHB}, i.e.,

$$\gamma_{\mathrm{ARHB}} = \begin{bmatrix} \gamma_{\mathrm{ARH}} & \sigma_{\mathrm{ARH};B} \\ \sigma^T_{\mathrm{ARH};B} & \gamma_B \end{bmatrix}, \tag{18}$$

which can be obtained by rearranging the lines and columns of matrix γ_{ABRH} describing state ρ_{ABRH}. Specifically, γ_{ABRH} can be obtained by applying a beam splitter transformation $S_{B_1R_0}$ to modes B_1 and R_0, as follows:

$$\gamma_{\mathrm{ABRH}} = \left[I \oplus S_{B_1R_0} \oplus I\right]\left[\gamma_{AB_1} \oplus \gamma_{R_0H}\right]\left[I \oplus S_{B_1R_0} \oplus I\right]^T, \tag{19}$$

where

$$S_{B_1R_0} = \begin{bmatrix} \sqrt{\eta}I & \sqrt{1-\eta}I \\ -\sqrt{1-\eta}I & \sqrt{\eta}I \end{bmatrix}. \tag{20}$$

III. IMPLEMENTATION OF UD CV QKD PROTOCOL

A. Experimental setup of UD protocol

Figure 3 depicts the all-fiber-based experimental setup designed by the authors. A 1550-nm continuous laser beam was generated by a narrow-bandwidth fiber laser on Alice's side and modulated into 80-dB high-extinction-ratio light pulses using two cascaded 40-dB high-extinction-ratio Mach-Zehnder (MZ) amplitude modulators (MXER-LN-10, Photline) [28]. The modulated pulse width was 100 ns and the repetition rate was 500 kHz. An asymmetric 10:90 polarization-maintaining (PM) fiber coupler was used to split the pulses into signal and local pulses. In the signal path, Alice used the single-MZ amplitude modulator to encode the information. The method of realizing the UD Gaussian modulation is described in detail in Sec. III B.

To realize a long-distance transmission of the signal and local pulses together and without interference through a single-mode (SM) fiber tens of kilometers in length, time and polarization multiplexing were adopted. To realize time multiplexing, an 80-m-long PM fiber was used in the signal path on Alice's side; this fiber allowed the signal pulses to follow the local pulses through the long transmission fiber with a delay of approximately 400 ns. On Bob's side, another 80-m-long PM fiber was employed to cause the signal pulses and local pulses to arrive simultaneously at the 50:50 PM fiber coupler before the PBHD. To realize polarization multiplexing, the signal and LO pulses were inserted into a PM fiber combiner perpendicular to each other on Alice's side and separated by a PM fiber splitter on Bob's side. The polarization isolation degree was 30 dB. Thus the total isolation degree in the long transmission fiber, which included an 80-dB high-extinction-ratio isolation degree and the 30-dB polarization isolation degree, was 110 dB. The LO-pulse intensity was 10^7 photons per pulse, and the mean intensity of the signal pulses was several photons per pulse. Thus the isolation degree was sufficient to prevent leakage of the LO pulses into the signal pulses.

The variable attenuator on Alice's side was used to tune the signal beam's quadrature variance, while the phase modulator on Bob's side was used to lock the relative phase between the signal and LO paths. The 10:90 SM fiber coupler and detector 1 were employed to recover the clock signal. Thus Alice and Bob could share the synchronous clock signal. As the beam polarization could be rotated because of the stress-induced birefringence of the fibers after transmission over a long distance, a dynamic polarization controller (DPC) was used to rotate the polarization of the combined signal and LO pulses back to linear polarization. The 10:90 PM fiber coupler and detector 2 were utilized to ensure that the intensity of the LO pulses was maximized; in this case, the LO pulses output by the DPC were linearly polarized. The quadratures of the signal pulses were measured by the PBHD [29,30].

A quantum random number generator (QRNG) 1 on Alice's side was used to generate random Gaussian numbers, which were then utilized to modulate the coherent states. QRNG 2 on Bob's side provided the random number to switch the detection bases randomly. Two optical 1.25-Gbps (gigabits per second) small form-factor pluggable fiber switches located on each side created a bidirectional classical communication link between Alice and Bob. The classical channel was mainly used for synchronization, parameter estimation, reverse reconciliation, privacy amplification, etc.

B. UD protocol modulation method

The obvious difference between the UD and symmetrical coherent-state protocols is that there is no phase modulator on Alice's side in the UD protocol. Consequently, the modulation method is also significantly different, especially the method used to lock the relative phase. In the symmetrical coherent-state protocol, Alice randomly prepared a coherent state centered on two numbers (x_A, y_A) from a Gaussian distribution. Essentially, Alice randomly modulated the intensity r^2 from a central $\chi^2(2)$ distribution using an amplitude modulator and randomly modulated the phase θ from a uniform distribution in $[0,2\pi)$ with a phase modulator [27]. The numbers (r,θ) in spherical coordinates map to the numbers (x_A, y_A) in rectangular coordinates. Meanwhile, in the UD protocol, there is no phase modulator; thus Alice should modulate the amplitude r according to a Gaussian distribution using the amplitude modulator.

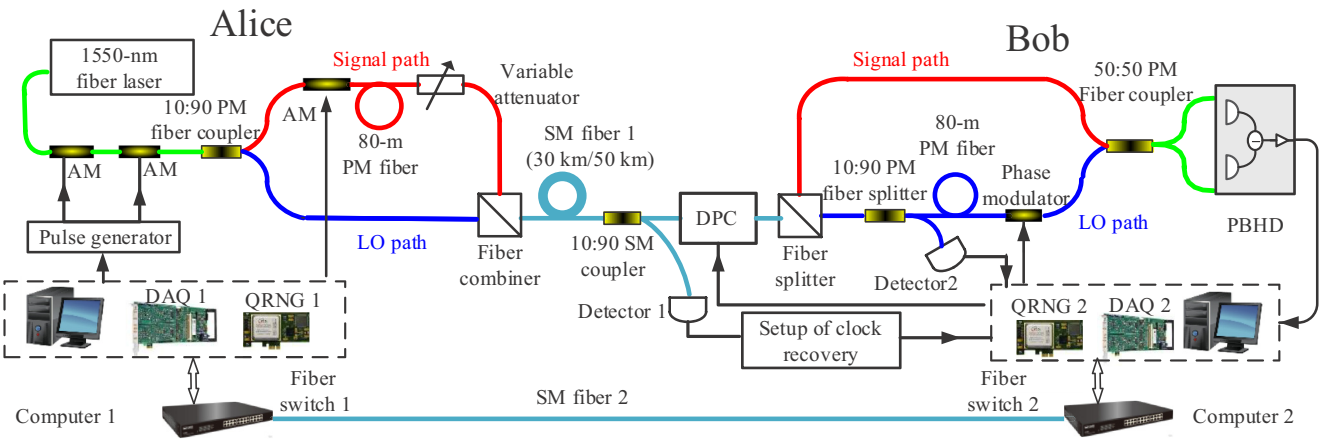

FIG. 3. Experimental setup. AM: amplitude modulator; SM: single mode; PM fiber: polarization-maintaining fiber; DAQ: data acquisition card; QRNG: quantum random number generator; DPC: dynamic polarization controller; PBHD: pulsed balanced homodyne detector.

For an MZ amplitude modulator, the output optical power I_{out} can be expressed in terms of the input optical power I_{in} as

$$I_{\text{out}} = I_{\text{in}} T\{\cos[\pi(V - V_{\max})/V_\pi] + 1\}/2, \qquad (21)$$

where T is the maximum transmission coefficient of the modulator considering the intrinsic insertion loss, V is the modulation voltage applied to the modulator, $V_{\max}$ is the voltage corresponding to the maximum transmission, and V_π is the half-wave voltage. The minimum transmission voltage $V_{\min}$ satisfies $V_{\min} = V_{\max} + V_\pi$.

In Fig. 4, the green dashed curve represents the output intensity I_{out} versus V, where $I_{\text{in}}T$ has been normalized to 1 and $V_{\max}$ has been set to $-V_\pi$. The red solid curve represents the output amplitude E_{out} versus V. The relation between them can be written as

$$E_{\text{out}} = |E_{\text{in}}|\sqrt{T}\cos[\pi(V - V_{\max})/2V_\pi]e^{i\theta}, \qquad (22)$$

where E_{in} is the amplitude of the input beam and θ is the phase of the output beam. It is obvious that the period of the red solid curve is twice that of the green dashed curve.

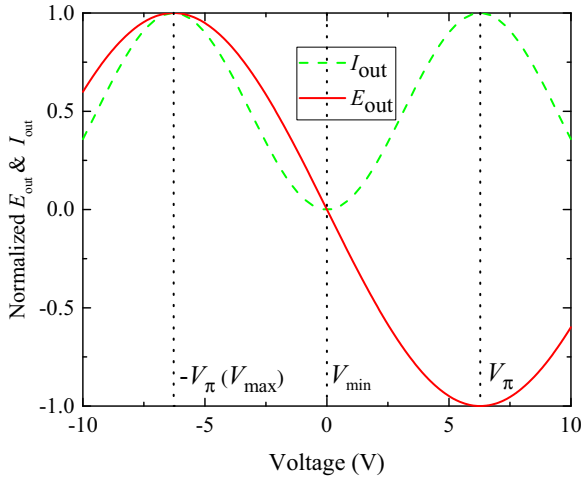

FIG. 4. Intensity and amplitude output of amplitude modulator versus modulated voltage.

In the symmetrical coherent-state protocol, only the voltages from $V_{\max}$ to $V_{\min}$ are needed. However, as there is no phase modulator on Alice's side in the UD protocol, the voltages from $-V_\pi$ to V_π are necessary.

To modulate the states obeying a Gaussian distribution in one dimension, a data group Z following a Gaussian distribution centered at zero should first be prepared. The Box-Muller method can be used to transform the random numbers generated by QRNG 1 into numbers following a Gaussian distribution. The modulation voltage can be calculated using the transformation equation, Eq. (23), obtained from Eq. (22):

$$V = \frac{2V_\pi}{\pi}\arccos Z + V_{\max}, \qquad (23)$$

where Z should satisfy $Z = E_{\text{out}}/(|E_{\text{in}}|\sqrt{T})$ and $\theta = 0$.

Note that there is a phase jump from $-V_\pi$ to V_π at $V_{\min}$. Thus the amplitude modulator also causes phase modulation from $\theta + 0$ to $\theta + \pi$. When using the UD protocol in amplitude quadrature, this phase modulation can change the amplitude quadratures of the states from positive to negative.

C. Relative phase-locking method

The pulses sent by Alice are mainly divided into two parts: data pulses that carry information, which are usually modulated into a Gaussian distribution as described earlier, and test pulses that are used for relative phase locking. To lock the relative phase between the signal pulses and LO pulses in the symmetrical coherent-state protocol, one amplitude modulator and two phase modulators are used. One phase modulator is on Alice's side, whereas the other is on Bob's side. On Alice's side, the test pulses are first modulated into the same amplitude via the amplitude modulator under applied voltages $V_{\max}$. The test pulses are then modulated, using the phase modulator, into three states, that is, ψ_1, ψ_2, and ψ_3, with phases of $\theta + 0$, $\theta + 2\pi/3$, and $\theta + 4\pi/3$ and phase-modulation voltages of V_1, V_2, and V_3, respectively. Here, θ is the current relative phase. Bob measures the amplitude quadratures x_1, x_2, and x_3

of the test pulses, and calculates the relative phase using the following equations:

$$r = \sqrt{\frac{2}{3}\left(\bar{x}_1^2 + \bar{x}_2^2 + \bar{x}_3^2\right)}, \quad \bar{x}_i = \frac{1}{n}\sum_n (x_{i1} + x_{i2} + \cdots + x_{in}), \tag{24}$$

and

$$\theta = \arccos\left[\frac{1}{3r}(2\bar{x}_1 - \bar{x}_2 - \bar{x}_3)\right] \quad \text{when} \quad \sin(\theta) = \frac{1}{-\sqrt{3}r}(\bar{x}_3 - \bar{x}_2) \geqslant 0\,, \quad \theta \in [0,\pi]$$
$$\theta = -\arccos\left[\frac{1}{3r}(2\bar{x}_1 - \bar{x}_2 - \bar{x}_3)\right] \quad \text{when} \quad \sin(\theta) = \frac{1}{-\sqrt{3}r}(\bar{x}_3 - \bar{x}_2) < 0\,, \quad \theta \in (-\pi,0)\,, \tag{25}$$

where r is the amplitude of the test pulses and $\bar{x}_i$ $(i = 1,2,3)$ is the mean of the quadratures [27]. To prevent shot noise from influencing the quadrature measurement precision, in our experiment, thousands of test pulses were measured to determine the mean in each data block. Further, high-intensity test pulses were utilized. The drifting period of the relative phase was several seconds, and the time during which the data in each block were acquired was tens of microseconds. Thus the relative phase was approximately constant in each block. After calculating the relative phase, the feedback voltage $V(\theta) = V_\pi\theta/\pi$ was fed back to the phase modulator on Bob's side to lock the relative phase. This relative phase-locking method is called the compensation method.

However, in the UD protocol, there is only one amplitude modulator on Alice's side and one phase modulator on Bob's side. To lock the relative phase in this protocol, a more elaborate method was designed. On Alice's side, all the test pulses were modulated into the same amplitude using an amplitude modulator with an applied voltage $V_{\max}$ to minimize the influence of the shot noise. On Bob's side, the test pulses were modulated using the phase modulator into three states, ψ_1, ψ_2, and ψ_3, with phases $\theta + 0$, $\theta + 2\pi/3$, and $\theta + 4\pi/3$ and modulation voltages of $V_1 + V_b$, $V_2 + V_b$, and $V_3 + V_b$, respectively. We first added the modulation voltages (V_1, V_2, V_3) and bias voltage V_b using a computer, and then applied the sums of the voltages (Fig. 5, short green solid lines) to the phase modulator during the test pulses. The bias voltage (Fig. 5, black solid lines) in each block was a constant value. For example, in the $(k+1)$th block, the bias voltage was $V_b(\theta'_k)$, where θ'_k is the accumulated relative phase θ' at the kth block. Note that θ' is the relative phase of the signal and LO

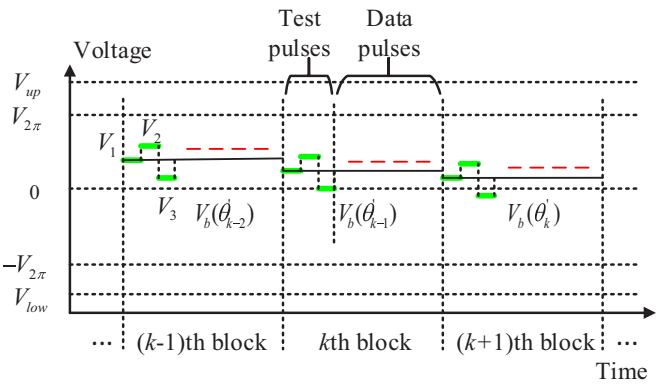

FIG. 5. Sums of modulated voltages and bias voltages applied to phase modulator on Bob's side.

pulses when no bias voltage is applied on the phase modulator. The sums of the voltages could complete not only the test pulse modulation, but also the feedback process. Note that, during the time occupied by the data pulses, the modulated voltages $V_{\pi/2}$ used to switch the detection bases were randomly added to the bias voltage (Fig. 5, red dashed lines).

During the compensation-locking process, the feedback voltage can be expressed as

$$V(\theta_k) = \frac{V_\pi}{\pi}\theta_k = K_p\theta_k, \tag{26}$$

where K_p is the coefficient of the proportional term. Usually, the $V(\theta_k)$ of the kth block is fed back to the $(k+1)$th block, introducing a residual steady-state error. To improve the phase locking, the equation used to calculate the feedback voltage can be extended to

$$V(\theta_k) = K_P\theta_k + K_I\sum_{i=1}^{k}\theta_i + K_D(\theta_k - \theta_{k-1}), \tag{27}$$

where K_I and K_D are the coefficients of the integral and derivative terms, respectively. The integral term accelerates the movement of the process toward a set phase and eliminates the residual steady-state error that would occur if a pure proportional controller were used. The derivative term predicts the system behavior, and thus improves the settling time and stability of the system. It is obvious that the modified method, usually called the digital PID method, will improve the relative phase locking compared with that achievable if compensation locking or pure proportional locking were used.

The phase-locking process using the digital PID method can be described as follows.

(1) First block: The bias voltage $V_b(\theta'_0)$ applied on the phase modulator is set to zero, and the initial accumulated relative phase θ'_0 is also zero. The relative phase θ_1 can be calculated using the test pulses of the first block and Eq. (25). Then the accumulated relative phase θ'_1 can be calculated via $\theta'_1 = \theta'_0 + \theta_1$. The feedback voltage $V(\theta_1)$, which will be fed back to the second block, can be calculated using Eq. (27). The bias voltage $V_b(\theta'_1)$, which will be applied on the phase modulator at the second block, can be calculated from $V_b(\theta'_1) = V_b(\theta'_0) + V(\theta_1)$.

(2) Second block: $V_b(\theta'_1)$ is applied on the phase modulator at the second block. The relative phase θ_2 can be calculated using the test pulses of the second block and Eq. (25). The accumulated relative phase θ'_2 can then be calculated via $\theta'_2 = \theta'_1 + \theta_2$. The feedback voltage $V(\theta_2)$, which will be fed

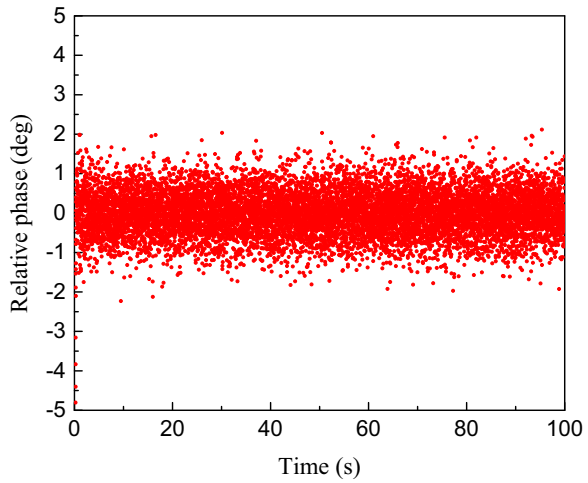

FIG. 6. Locked relative phase over 100 s.

back to the third block, can be calculated using Eq. (27). The bias voltage $V_b(\theta'_2)$, which will be applied on the third block, is $V_b(\theta'_2) = V_b(\theta'_1) + V(\theta_2)$.

(3) kth block: The bias voltage $V_b(\theta'_{k-1})$ is applied on the phase modulator at the kth block. The relative phase θ_k can be calculated using the test pulses of the kth block and Eq. (25). The accumulated relative phase θ'_k can then be calculated via $\theta'_k = \theta'_{k-1} + \theta_k$. The feedback voltage $V(\theta_k)$, which will be fed back to the $(k+1)$th block, can be calculated using Eq. (27). The bias voltage $V_b(\theta'_k)$, which will be applied on the $(k+1)$th block, is $V_b(\theta'_k) = V_b(\theta'_{k-1}) + V(\theta_k)$.

As time passes, θ' will randomly drift. Thus the bias voltage applied on the phase modulator $V_b(\theta')$ will randomly drift and eventually exceed one of the output voltage bounds V_{up} or V_{low} of the data acquisition card (shown in Fig. 5). Thus the following method of adding or subtracting $V_{2\pi}$ is applied. If $V_b(\theta')$ is larger than $V_{2\pi}$, $V_{2\pi}$ is subtracted, and θ' is replaced by a new corresponding value $\theta' = \theta' - 2\pi$. In contrast, if $V_b(\theta')$ is smaller than $-V_{2\pi}$, $V_{2\pi}$ is added, and θ' is replaced by a new corresponding value $\theta' = \theta' + 2\pi$. Through application of this procedure, the relative phase remains stably locked for a long period of time.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Figure 6 presents the relative phase resulting from application of the improved phase-locking method, recorded in real time for 100 s. Each point represents the relative phase of a data block, which was the unit used to calculate the relative phase, each having a duration of 10 ms. Evidently, the relative phase can be locked to within approximately $\pm 0.5^\circ$ (standard deviation) and the mean is $6.5\times10^{-4^\circ}$. It is obvious that the relative phase fluctuates slightly and the residual steady-state error due to phase locking is almost zero.

One important step in achieving the secret key is calibrating the experimental parameters carefully. In our experiment, the efficiency of the PBHD was 65% and the electronic noise was 0.03. A reverse reconciliation efficiency of 95.2% was achieved [31]. The transmission efficiency T_x and excess noise ε_x were evaluated in real time based on the public amplitude quadratures.

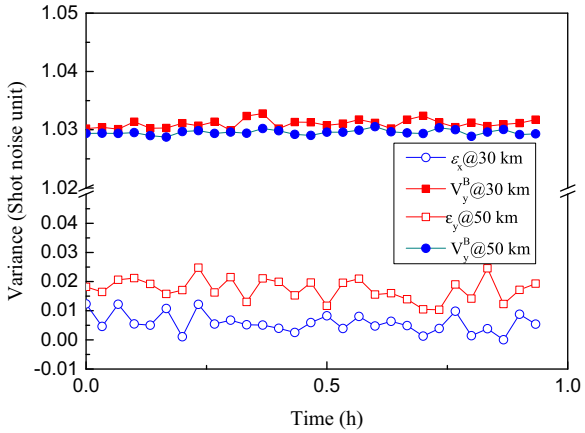

FIG. 7. Variances of excess noise and phase quadrature V_y^B over 1 h and transmission lengths of 30 and 50 km.

Figure 7 presents the excess noise values at 30 and 50 km obtained with $V_M = 2.8$. When the transmission length is 30 km, the excess noise is approximately 0.01. Further, when the transmission length is 50 km, the excess noise is approximately 0.02. To obtain each excess noise point, a burst of data including 10 000 blocks was used, where each block contained 5 K points of data. Thus a total of 50 M points were collected, of which 10 M points were from test pulses, 10 M points were utilized to evaluate the excess noise, 10 M points were employed to evaluate $V_y^{B_1}$, and 20 M points were used to extract the secret key.

In our experiment, we randomly switched the bases of the data pulses in each block in order to measure the variance of the phase quadrature V_y^B using QRNG 2, as shown in Fig. 7. The relation between $V_y^{B_1}$ and V_y^B provided in Eq. (28) can be used to evaluate $V_y^{B_1}$, where

$$V_y^B = \eta V_y^{B_1} + V_N(1-\eta) = \eta\left(V_y^{B_1} - 1\right) + 1 + V_e. \quad (28)$$

After $V_y^{B_1}$ is determined, Eqs. (6) and (10) can be applied to calculate C_y^p and ΔI [25].

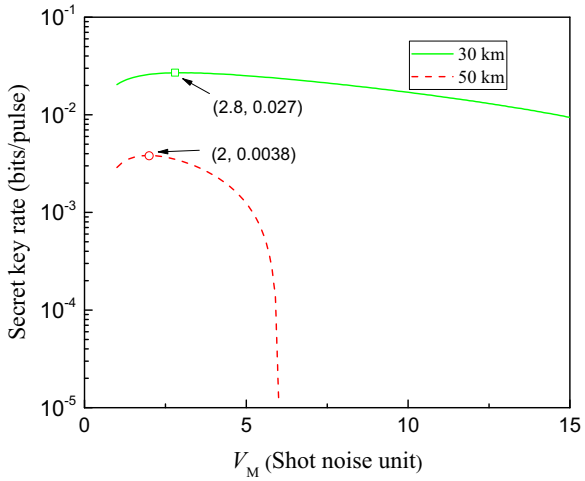

FIG. 8. Secret key rate versus modulation variance curves corresponding to transmission lengths of 30 and 50 km.

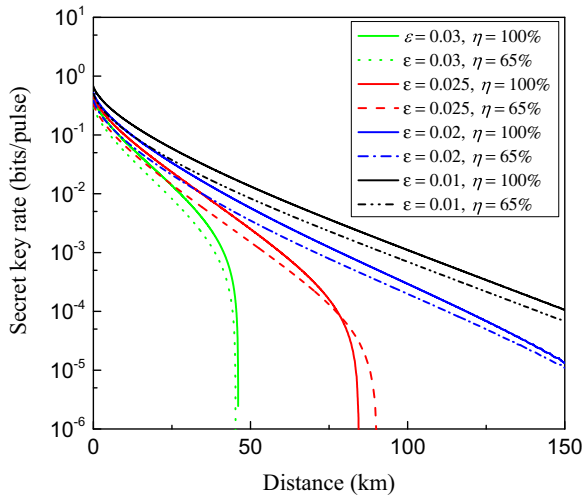

FIG. 9. Secret key rate versus transmission distance curves corresponding to different amounts of excess noise.

Although it is not necessary to evaluate T_y or ε_y, in some situations, such as the prediction of the best variance shown in Fig. 8 and analysis of the secret key rate versus distance shown in Fig. 9, it is very useful to assume that $T_y = T_x$ and $\varepsilon_y = \varepsilon_x$. In these scenarios, $V_y^{B_1}$ can be calculated using

$$V_y^{B_1} = 1 + T_x \varepsilon_x. \tag{29}$$

In the experiment, we assumed that $T_y = T_x = T$ and used the equation $V_y^{B_1} = 1 + T_y \varepsilon_y$ to calculate ε_y; this value was found to be approximately the same as ε_x, but sometimes slightly smaller.

By assuming that $T_y = T_x$ and $\varepsilon_y = \varepsilon_x$, the best modulation variances V_M^b (represented as circles) were calculated, as shown in Fig. 9. The figure indicates that, when the transmission length is 30 km and the excess noise is 0.01, V_M^b is 2.8 (green circle). The secret key rate is 0.027 bits/pulse, corresponding to a bit rate of 5.4 kbps when the repetition rate is 500 kHz and 40% quadratures are used to calculate the secret key rate. In addition, V_M^b is 2 (red circle) when the excess noise is 0.02 and the transmission length is 50 km, corresponding to a secret key bit rate of 760 bps. As the tops of the V_M curves are flat, it is possible to adjust V_M without decreasing the secret key rate noticeably. In our experiment, V_M was set to 2.8 at a transmission length of 50 km to facilitate comparison with the results for the 30-km transmission length, yielding a secret key bit rate of 700 bps.

Figure 9 presents the secret key rate versus distance at different excess noise levels, assuming that $V_y^{B_1} = 1 + T_x \varepsilon_x$. The solid lines correspond to the scenario in which the efficiency of the PBHD on Bob's side is 100%. The dashed lines correspond to the realistic condition in which the calibrated detection efficiency is 65%. From left to right, the excess noise values are 0.03, 0.025, 0.02, and 0.01, and $V_M = 2.8$. It is evident that the UD protocol is very sensitive to excess noise, as is the symmetrical coherent-state protocol. From the red dashed curve, it is apparent that a maximum distance greater than 70 km can be achieved with an excess noise value of 0.025. However, when the transmission distance is greater, greater excess noise will be obtained. The comparison of the solid and dashed red curves shows the phenomenon of noise counteracting noise; thus the transmission length could be extended because of the realistic efficiency and electronic noise [32].

V. CONCLUSION

This paper presented a complete experimental demonstration of an all-fiber-based UD CV QKD system as well as a security analysis of the UD coherent-state protocol under realistic conditions. The phenomenon of noise counteracting noise was observed, enabling the transmission length to be extended with a phase-insensitive efficiency η and electronic noise V_e. Furthermore, a modulation method and an improved relative phase-locking technique were proposed. The standard deviation of the locked relative phase was found to be 0.5°. Secret key bit rates of 5.4 kbps and 700 bps were achieved in a single-mode fiber at distances of 30 and 50 km, respectively.

Higher secret key rates and longer distances can be expected following reduction of the excess noise and an increase of the reconciliation efficiency [33]. Further theoretical analysis of the protocol will include finite-size effects [34] and composable security [35]. The UD protocol simplifies the CV QKD system and reduces the cost. Although the protocol is more sensitive to the excess noise [25], it displays a comparable performance to the symmetrical counterpart under realistic conditions. It is expected that the presented system can find potential applications in various scenarios, such as in QKD local area networks, where the transmission distance between users is usually short and cost is a key concern.

ACKNOWLEDGMENTS

This research was supported by the National Natural Science Foundation of China (NSFC) (Grants No. 11504219 and No. 61378010), the Key Project of the Ministry of Science and Technology of China (2016YFA0301403), and the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[4] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
[5] M. Hillery, Phys. Rev. A **61**, 022309(R) (2000).
[6] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[7] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[8] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[10] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[11] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[12] M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).
[13] B. Qi, L. L. Huang, L. Qian, and H. K. Lo, Phys. Rev. A **76**, 052323 (2007).
[14] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
[15] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[16] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[17] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).
[18] Y. B. Zhao, M. Heid, J. Rigas, and N. Lutkenhaus, Phys. Rev. A **79**, 012307 (2009).
[19] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Opt. Express **20**, 14030 (2012).
[20] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[21] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).
[22] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, Sci. Rep. **5**, 14607 (2015).
[23] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).
[24] Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, and K.-C. Peng, Chin. Phys. B **26**, 040303 (2017).
[25] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[26] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Quant. Inf. Comput. **16**, 1081 (2016).
[27] J. Lodewyck, Ph.D. thesis, University of Paris XI, 2006.
[28] X. Wang, J. Liu, X. Li, and Y. Li, IEEE J. Quantum Electron. **51**, 5200206 (2015).
[29] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, Opt. Lett. **26**, 1714 (2001).
[30] X.-Y. Wang, Z.-L. Bai, P.-Y. Du, Y.-M. Li, and K.-C. Peng, Chin. Phys. Lett. **29**, 124202 (2012).
[31] Z. L. Bai, S. S. Yang, and Y. M. Li, Jpn. J. Appl. Phys. **56**, 044401 (2015).
[32] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[33] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[34] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[35] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).