Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment

Shi-Yang Shen,[1] Ming-Wei Dai,[2] Xue-Tao Zheng,[1] Qi-Yao Sun,[3] Guang-Can Guo,[1] and Zheng-Fu Han[1]
[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[2]*School of The Gifted Young, University of Science and Technology of China, Hefei 230026, China*
[3]*Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230026, China*

(Received 8 October 2018; published 16 July 2019)

An experiment evaluating continuous-variable quantum key distribution (CV-QKD) in an urban environment free-space channel has been accomplished using a single homodyne detector. This is based on Gaussian modulation with coherent states in the polarization degree of freedom. We achieved a QKD distance at 460 m at a repetition rate of 10 kHz. The secure key rate is 0.152 kbps at the typical reconciliation efficiency of 0.95. The experimental setup of this scheme is simplified, and the barrier for implementation has been remarkably reduced compared to that for traditional symmetric modulation protocols, for example, the GG02 protocol proposed in F. Grosshans and P. Grangier [Phys. Rev. Lett. **88**, 057902 (2002)]. The influence of the security key rate by asymmetric modulation is small for a relatively low channel loss condition in a free-space environment. This scheme is expected to have significance for future practical applications.

DOI: 10.1103/PhysRevA.100.012325

I. INTRODUCTION

Quantum key distribution allows two authorized distant parties, Alice and Bob, to share a common key via a potentially eavesdropped quantum channel. The first quantum key distribution (QKD) protocol was proposed in 1984 [1]. Continuous-variable (CV) QKD protocols, especially those with a coherent-state light source, have been focused on in recent decades [2–4]; these protocols utilize balanced homodyne detection techniques and light sources that are not at the single-photon level. Therefore, this approach has the advantages of higher detection efficiency, and thus a higher secure key rate, and antiphoton number attack. During the past few years of development, CV-QKD protocols and experiment have been simplified. First, the coherent-state protocols show substantial advantages against squeezed-state versions [5–8] in the preparation of a light source, and the theoretical secure distance improves remarkably, which has led to deep research on CV-QKD theory and the realization of variable experiment schemes. Regarding present experiments in the field of CV-QKD, the symmetrical Gaussian modulated coherent-state protocols have been well studied [9–14] since the composable security analysis has been revealed [15]. Second, instead of Gaussian modulation, the discrete modulation reduces the complexity of classical postprocessing, which causes a low signal-to-noise ratio due to the long-distance propagation loss. Finally, the coherent-state unidimensional CV-QKD protocol, proposed in 2015 [16], further simplified the apparatus in both preparation and detection since only one of the quadratures needs to be Gaussian modulated, instead of both being modulated simultaneously. The experimental scheme in fiber channels was illustrated in [17], and the security key rate in a finite-size scenario was proved [18].

The security of CV-QKD has been studied extensively in recent years. Reference [19] gives the extremality of Gaussian states, and as a consequence, the Gaussian collective attacks are optimal in the asymptotic region [20,21]. In 2010, the finite-size effect analysis of CV-QKD was given in Ref. [22]. The security against general attacks in the practical finite-size region was proven in 2013 [23] by exploiting the symmetry of modulation and postselection in phase space. Soon after, Leverrier [15] achieved the composable security for coherent CV-QKD protocols against collective attacks, which established the security of coherent protocols against general attacks. Furthermore, the composable security of unidimensional CV-QKD was revealed in [24].

In addition, a free-space channel is insensitive to polarization compared to a fiber channel, which results in the light polarization being nearly unchanged during propagation. Thus, the polarization controller on the receiver's side can be omitted. In other words, the system does not have to calibrate the polarization direction frequently, reducing the calibrating time of nonkey distribution, and thus increases the key rate. On the other hand, encoding with polarization avoids the nonsynchronous disturbance of the phase. Therefore, the phase locking between the local oscillator and signal is unnecessary since the polarization has been aligned to the same direction, significantly simplifying the difficulty of system implementation. The security distance of CV-QKD in free-space [8,10,11,25] channels can reach dozens of kilometers, making it compatible with communications in urban conditions. This is expected to play an important role in future practical applications.

This experiment uses the unidimensional CV-QKD scheme in the free-space channel, modulating the polarization quantum Stokes parameter with the Gaussian distribution. The resulting security key rate in a real urban environment condition is 460 m, the performance of which was slightly lower than expected; however, this approach was obviously simplified

and more adaptable to experimental environments compared to the GG02 protocol in the same conditions.

II. STOKES OPERATOR ENCODING

In this section, we describe the preparation-and-measurement configuration of the unidimensional protocol proposed in [16], which corresponds to the prepare-and-measurement experimental implementation. In symmetric CV-QKD protocols such as the GG02 protocol both quadratures, X and P, must be modulated simultaneously. However, in the unidimensional protocol only a single quadrature, without loss of generality, denoted X, will be modulated. Each coherent state sent by Alice is displaced by x in the phase space, which obeys a Gaussian distribution centered at zero and has the variance of V_M. Additionally, the variance of the other quadrature is 1, normalized at the shot-noise unit. Bob performs homodyne detection on the X quadrature in a certain time interval and randomly switches to monitoring the variance of the P quadrature as a covariance matrix parameter V_P. After Alice and Bob share a sufficiently long sequence of real-number raw key data, they estimate the channel parameters using a small random part of the data and perform reverse reconciliation [3].

For polarization encoding, quantum Stokes operators are treated as quadratures, which are defined as [26]

$$\begin{aligned} \hat{S}_0 &= \hat{a}_H^\dagger \hat{a}_H + \hat{a}_V^\dagger \hat{a}_V, \quad \hat{S}_1 = \hat{a}_H^\dagger \hat{a}_H - \hat{a}_V^\dagger \hat{a}_V, \\ \hat{S}_2 &= \hat{a}_H^\dagger \hat{a}_V + \hat{a}_V^\dagger \hat{a}_H, \quad \hat{S}_3 = i(\hat{a}_V^\dagger \hat{a}_H - \hat{a}_H^\dagger \hat{a}_V), \end{aligned} \tag{1}$$

where subscripts H and V label the creation and annihilation operators along the horizontal and vertical polarization modes, respectively. These creation and annihilation operators both have the same commutation relations and Heisenberg uncertainty principle as quadratures X and P, except for a constant coefficient:

$$[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{jk}, \quad j,k = H,V \tag{2}$$

and

$$[\hat{S}_j, \hat{S}_k] = 2i\epsilon_{jkl}\hat{S}_l, \quad j,k,l = 1,2,3, \tag{3}$$

while the variance of the latter three Stokes operators satisfy

$$\mathrm{Var}[\hat{S}_2]\mathrm{Var}[\hat{S}_3] \geqslant |\langle \hat{S}_1 \rangle|^2. \tag{4}$$

In our experiment, we use the polarization degree to encode information. The S_1-polarized (vertical mode) coherent-state light plays the role of a local oscillator (LO). S_3- and S_2-polarized states are two orthogonal quadratures, and S_3 states are generated by an electro-optical modulation (EOM). Since the intensity of modulated light is far weaker (approximately 3 orders of magnitude lower; see Sec. IV) than LO, the loss of LO is negligible compared to its intensity $|\langle \hat{S}_1 \rangle|$, so it remains nearly unchanged. In other words, the right-hand side of Eq. (4) is approximately a constant. The output light is at a strong vertical polarized mode, with a superposition of a very weak circular mode. More explicitly, the shape of the polarization state in the H-V plane is an ellipse with an eccentricity of nearly 1, and its long and short axes are oriented in the vertical and horizontal directions. In this condition, the Stokes operators can be normalized as

$$\hat{S}_2' = \frac{\hat{S}_2}{\sqrt{S_1}}, \quad \hat{S}_3' = \frac{\hat{S}_3}{\sqrt{S_1}}. \tag{5}$$

They have the same commutation relations and Heisenberg uncertainty. For distinguishability and for simplicity, we still use the new symbols X and P instead of S_2' and S_3' below, unless otherwise mentioned.

To explain how the polarization changed in the setup, without loss of generality, except for a phase factor, we assume that the annihilation operator of incoming light is

$$\hat{a}_0 = a_{\mathrm{LO}} \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{6}$$

Passing through a half-wave plate whose slow axis is 22.5° to the horizontal direction, the annihilation operator of the output light is

$$\hat{a}_1 = \frac{a_{\mathrm{LO}}}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{7}$$

If the applied voltage of the EOM is U, the phase difference between ordinary and extraordinary light is $\phi = \pi U / V_\pi$, where V_π is the half-wave voltage of the EOM. Then the light is

$$\hat{a}_2 = \frac{a_{\mathrm{LO}}}{\sqrt{2}} \begin{bmatrix} 1 \\ e^{i\phi} \end{bmatrix}. \tag{8}$$

On the receiver's side, the light then passes through a half-wave plate (HWP) and a quarter-wave plate (QWP) whose slow axes are 22.5° and 45° to the horizontal direction, respectively. The Jones matrices of HWP and QWP are

$$\begin{aligned} J_H(\theta) &= \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}, \\ J_Q(\theta) &= \begin{bmatrix} \cos^2\theta + i\sin^2\theta & \cos\theta\sin\theta(1-i) \\ \cos\theta\sin\theta(1-i) & \sin^2\theta + i\cos^2\theta \end{bmatrix}, \end{aligned} \tag{9}$$

where θ is the angle between the QWP's slow axis and the horizontal direction. So the light through the QWP is

$$\begin{aligned} \hat{a}_3 &= [a_{3H},\ a_{3V}]^T = J_Q\left(\frac{\pi}{4}\right) J_H\left(\frac{\pi}{8}\right) \hat{a}_2 \\ &= \frac{a_{\mathrm{LO}}}{2} \begin{bmatrix} 1 + ie^{i\phi} \\ 1 - ie^{i\phi} \end{bmatrix}. \end{aligned} \tag{10}$$

After a 50:50 polarized beam splitter (PBS) and a balanced homodyne detector, the measurement result is the difference between the photon number transmitted from the PBS and that reflected from the PBS, which is

$$n_{\mathrm{meas}} = a_{3H}^\dagger a_{3H} - a_{3V}^\dagger a_{3V} = -a_{\mathrm{LO}}^2 \sin\frac{\pi U}{V_\pi}. \tag{11}$$

When $U \ll V_\pi$,

$$n_{\mathrm{meas}} \approx -a_{\mathrm{LO}}^2 \frac{\pi U}{V_\pi}. \tag{12}$$

According to Eq. (11), the EOM introduces a circularly polarized component that is measured by Bob's differential detector. If $U \sim N(0, \Sigma^2)$, then $n \sim N(0, \frac{a_{\mathrm{LO}}^4 \pi^2 \Sigma^2}{V_\pi^2})$. The relation between the applied voltage on the EOM and modulation

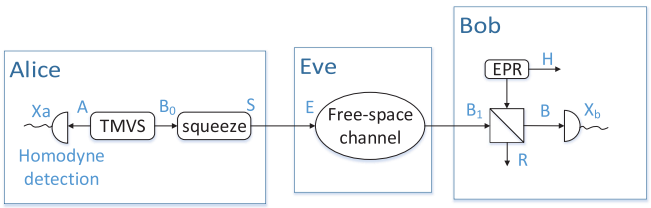

FIG. 1. Entanglement-based description of unidimensional CV-QKD. Alice prepares a two-mode squeezed vacuum state, then measures mode A using homodyne detection; then the remaining part, mode B_0, is sent through the channel. Bob's nonideal detector equals a PBS followed by an ideal detector.

variance V_M is

$$V_M = \frac{\pi^2 \Sigma^2 V_{\mathrm{LO}}^2}{V_\pi^2 N_0}, \tag{13}$$

where V_{LO} is the voltage of the local oscillator on Alice's side generated and applied by the data acquisition module (DAQ) and N_0 is the shot noise in SI units. According to the definition of the Stokes operators, the expectation values of $\hat{S}_3$ and $\hat{S}_1$ are $\langle \hat{S}_3 \rangle = n_{\mathrm{meas}}$ and $\langle \hat{S}_1 \rangle = a_{\mathrm{LO}}^2 \cos\phi \approx a_{\mathrm{LO}}^2$, respectively. Thus, the quadratures defined in Eq. (5) can be expressed using the measurement data n_{meas} and prepared data n_{prep} as follows:

$$X_a = \frac{n_{\mathrm{prep}}}{\sqrt{n_a}}, \quad X_b = \frac{n_{\mathrm{meas}}}{\sqrt{n_b}}, \tag{14}$$

where $n_a = a_{\mathrm{LO}}^2$ and $n_b = T\eta n_a$ are the average numbers of photons of the local oscillators of Alice and Bob, respectively, which can be monitored by a power meter or oscilloscope in units of voltage. n_{prep} can be expressed using the applied voltages $n_{\mathrm{prep}} = n_a \sin\phi = n_a \sin\frac{\pi U}{V_\pi}$. Additionally, T and η are the overall transmittance and detection efficiency of the homodyne, respectively. Since the photodiodes work linearly, X_a and X_b are proportional to the average number of photons and thus proportional to the voltages measured by DAQs.

III. SECURITY ANALYSIS

The security key rate for the unidimensional protocol is computed in [16,18] against collective attacks in asymptotic and finite-size regions, respectively. In the equivalent entanglement-based description, as shown in Fig. 1 [18], Alice prepares a two-mode squeezed vacuum state and measures one of its modes using homodyne detection. The other mode, B_0, is sent to Bob through a quantum channel with the potential of Eve. As is already known, the lower-bound key rate is given by

$$K = \beta I_{AB} - \chi_{BE}, \tag{15}$$

where

$$\chi_{BE} = S(E) - S(E|x_b) \tag{16}$$

is the Holevo information [16,27] between Bob and the eavesdropper in the scheme of reverse reconciliation and β is the reconciliation efficiency. Since the eavesdropper holds the purification of state ρ_{AB_1E} [18,28], and state ρ_{ARHB} is pure, the von Neumann entropy can be expressed as

$$S(E) = S(AB_1), \quad S(E|x_b) = S(ARH|x_b), \tag{17}$$

which can be calculated through the covariance matrix Γ_{AB_1} and conditioned entropy $\Gamma_{ARH|x_b}$, respectively. More explicitly,

$$\chi_{BE} = G(\lambda_1) + G(\lambda_2) - G(\lambda_3) - G(\lambda_4), \tag{18}$$

where the function $G(x)$ is defined as

$$G(x) = \frac{1+x}{2}\log_2\frac{1+x}{2} - \frac{1-x}{2}\log_2\frac{1-x}{2} \tag{19}$$

and $\lambda_{1,2}$ and $\lambda_{3,4}$ are symplectic eigenvalues of Γ_{AB_1} and $\Gamma_{ARH|x_b}$, respectively [18].

In the description of the entanglement-based scheme, the covariance matrix of a two-mode squeezed vacuum state is

$$\gamma_{\mathrm{TMVS}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{V^2-1} \\ \sigma_z\sqrt{V^2-1}\sigma_z & V\mathbb{I}_2 \end{bmatrix}, \tag{20}$$

where σ_z is one of the Pauli matrices. The variance V is equal to $\sqrt{V_M+1}$ in the prepare-and-measure scheme with the modulation variance of V_M. According to [16], the covariance matrix for a unidimensional protocol is built by a squeeze operation on one of its modes; for example, for mode A, with a squeezing parameter of $r = -\ln\sqrt{V}$, the following covariance matrix results:

$$\gamma_{AB_0} = S\gamma_{\mathrm{TMVS}}S^T = \begin{bmatrix} V & 0 & \sqrt{V(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\frac{V^2-1}{V}} \\ \sqrt{V(V^2-1)} & 0 & V^2 & 0 \\ 0 & -\sqrt{\frac{V^2-1}{V}} & 0 & 1 \end{bmatrix}, \tag{21}$$

where the squeezing operator S is

$$S = \mathbb{I}_2 \bigoplus \begin{bmatrix} \sqrt{V} & 0 \\ 0 & \frac{1}{\sqrt{V}} \end{bmatrix}. \tag{22}$$

Now assume that the channel transmittance and noise in X (or, equivalently, S_1) are T and ϵ, respectively. After transmission through the noisy channel, the covariance matrix becomes

$$\gamma_{AB_1} = \begin{bmatrix} V & 0 & \sqrt{TV(V^2-1)} & 0 \\ 0 & V & 0 & C_{P1} \\ \sqrt{TV(V^2-1)} & 0 & 1+T(V^2+\chi_{\mathrm{line}}) & 0 \\ 0 & C_{P1} & 0 & V_{P1} \end{bmatrix}, \tag{23}$$

where V_{P1} and C_{P1} are the P quadrature variance and correlation between the X (or S_3) and P (or S_2) quadratures on the B_1 side and $\chi_{\mathrm{line}} = \frac{1-T}{T} + \epsilon$ is the equivalent noise introduced by channel loss and excess noise ϵ. Since the P (or S_2) quadrature is unmodulated, V_{P1} and C_{P1} remain unknown to all communication parties, including the eavesdropper. V_{P1} can be monitored on Bob's side. Considering the realized model of balanced homodyne detectors (BHDs), it has a nonunity detection efficiency η and electronic noise V_e in shot-noise units. It is modeled as an ideal BHD, followed by a PBS of a transmittance efficiency η. A thermal state H

whose noise variance is $V_{th} = 1 + \frac{V_e}{1-\eta}$ is injected from one of the ports of the PBS. In this case, the covariance of Alice and Bob is [18]

$$\gamma_{AB} = \begin{bmatrix} V & 0 & \sqrt{\eta T V(V^2-1)} & 0 \\ 0 & V & 0 & \sqrt{\eta} C_{P1} \\ \sqrt{\eta T V(V^2-1)} & 0 & 1+\eta T(V+\chi_{\text{tot}}) & 0 \\ 0 & \sqrt{\eta} C_{P1} & 0 & \eta(V_{P1}+\chi_{\text{hom}}) \end{bmatrix}, \tag{24}$$

where the equivalence noises are

$$\chi_{\text{hom}} = \frac{1+V_e}{\eta} - 1, \quad \chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T. \tag{25}$$

Since the unknown parameters C_{P1} and V_{P1} must be physical, the Heisenberg uncertainty principle gives their bound,

$$\gamma_{AB1} + i\Omega \geqslant 0, \tag{26}$$

where

$$\Omega = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}. \tag{27}$$

In the assumption of a reverse reconciliation [3], Alice guesses Bob's measurement, so she holds the conditioned covariance matrix:

$$\gamma_{A|x_B} = \begin{bmatrix} \frac{\sqrt{V_M+1}(1+\eta\epsilon)}{1+\eta(V_M+\epsilon)} & 0 \\ 0 & \sqrt{V_M+1} \end{bmatrix}. \tag{28}$$

The conditioned covariance matrix $\gamma_{ARH|x_B}$ can be derived using a partial measurement of γ_{ARHB}, which is the rearrangement of the rows and columns of matrix γ_{ABRH} [28],

$$\gamma_{ABRH} = Y_{\text{PBS}}^T(\gamma_{AB_1} \oplus \gamma_{\text{EPR}})Y_{\text{PBS}}, \tag{29}$$

where Y_{PBS} is the symplectic transformation matrix of the PBS and γ_{EPR} is the covariance matrix of the Einstein-Podolsky-Rosen (EPR) entangled state,

$$Y_{\text{PBS}} = \mathbb{I}_2 \oplus \begin{bmatrix} \sqrt{\eta}\mathbb{I}_2 & \sqrt{1-\eta}\mathbb{I}_2 \\ \sqrt{1-\eta}\mathbb{I}_2 & \sqrt{\eta}\mathbb{I}_2 \end{bmatrix} \oplus \mathbb{I}_2,$$

$$\gamma_{\text{EPR}} = \begin{bmatrix} V_{th}\mathbb{I}_2 & \sqrt{V_{th}^2-1}\sigma_z \\ \sqrt{V_{th}^2-1}\sigma_z & V_{th}\mathbb{I}_2 \end{bmatrix}. \tag{30}$$

$\lambda_{1,2,3,4}$ can be expressed by parameters of transmittance T, excess noise ϵ, P quadrature variance V_{P1}, modulation variance V_M, and correlation C_{P1}, which should be scanned in the physical region to minimize the secret key rate [18]:

$$\lambda_{1,2}^2 = \tfrac{1}{2}(A \pm \sqrt{A^2-4B}), \quad \lambda_{3,4}^2 = \tfrac{1}{2}(C \pm \sqrt{C^2-4D}), \tag{31}$$

where the symbols A, B, C, and D are

$$\begin{aligned} A &= 1 + V_{P1} + V_M + V_{P1}(\epsilon + V_M)T \\ &\quad + 2C_P(1+V_M)^{1/4}\sqrt{V_M T}, \\ B &= \left[V_{P1}(1+V_M) - C_{P1}^2\sqrt{1+V_M}\right](1+\epsilon T), \\ C &= \frac{A(1+V_e) + [(\epsilon T+1)(V_M+2) + V_M T - A]}{1+\epsilon T\eta + V_M T\eta + V_e}, \\ D &= \frac{B(1+V_e-\eta) + (1+V_M)(1+\epsilon T)\eta}{1+\epsilon T\eta + V_M T\eta + V_e}. \end{aligned} \tag{32, 33}$$

IV. EXPERIMENTAL SETUP

The experimental setup for the unidimensional CV-QKD system in free space is shown in Fig. 2.

The continuous-wave laser centered at 786 nm, approximately 1 nm of the FWHM, is fiber pigtailed and coupled to the free space in the Gaussian mode. The signal is modulated by the EOM (Thorlabs, EO-AM C1, wavelength of 600–900 nm) at a pulse repetition frequency of 10 kHz and a sample rate of 1 MHz, which is mainly limited by the maximum sample rate of the DAQ (NI PCIe-6363, maximum acquisition rate is 2 MHz). Thus, each pulse contains 100 sample data, and the duty cycle of the signal pulse is 10%.

The output intensity is 15 mW, and it is first attenuated by a sandwich structure consisting of two half-wave plates (HWPs) and two PBSs (Thorlabs PBS252). As the extinction ratio of the PBSs is larger than 30 dB, by rotating the polarization with the HWPs, the final intensity output from PBS2 in Fig. 2(a) is at the level of 100 μW, corresponding to 10^{14} photons per pulse. The polarization state of this output is vertical, as shown in Eq. (6). HWP3 rotates the linearly polarized light into 45° polarization, as shown in Eq. (7). Then the polarization state is modulated in the EOM, whose modulation bandwidth is 100 MHz [29], after which the state is as shown in Eq. (8). The applied voltage is controlled by a computer, and a Gaussian distributed random intensity whose variance is Σ^2 is used, as mentioned in Sec. II, which is approximately 165 times the shot noise. The width of the modulation signal pulses is 10 μs, which is much longer than the time difference of the light distance between the two arms of the BHD (approximately 10^{-11} s). Since the applied voltage is at the level of about 1 to 1000 mV, which is about 3 orders of magnitude weaker than the half-wave voltage, 284 V, the intensity of the signal light (circularly polarized) is far weaker than the local oscillator light (vertically polarized), satisfying the condition of Eq. (5).

The $1/e^2$ diameter of the output beam from the EOM is 2.1 mm, and the full divergence angle is 4.5×10^{-4} rad. A Galileo beam expander (Thorlabs, GBE10-B, expansion ratio is 10×) is used to decrease the full divergence to 4.5×10^{-5} rad so that the beam diameter at the receiver's aperture is about 4 cm after propagating through a 460-m free-space channel.

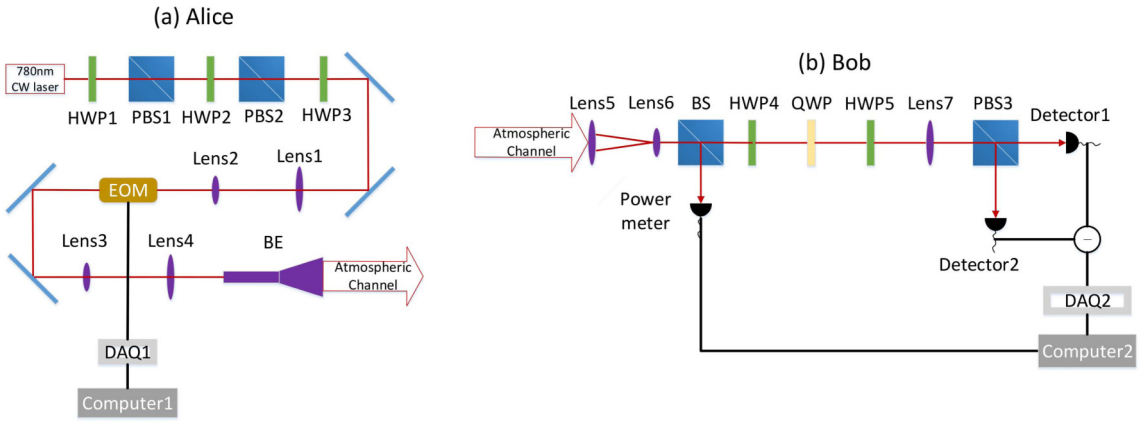

FIG. 2. (a) Sender's side of the free-space CV-QKD experimental setup for a unidimensional protocol. HWP: half-wave plate. EOM: electro-optical modulator. BE: 10× beam expander. Lenses 1 and 4: focus = 100 mm, diameter = 25 mm. Lenses 2 and 3: focus = 50 mm, diameter = 25 mm. DAQ: data acquisition. (b) Receiver's side of the free-space CV-QKD experimental setup for a unidimensional protocol. HWP: half-wave plate. QWP: quarter-wave plate. Lens 5: focus = 200 mm, diameter = 100 mm (uncoated). Lens 6: focus = 60 mm, diameter = 50 mm. Lens 7: focus = 150 mm, diameter = 50 mm. BS: beam splitter. PBS: polarized beam splitter. DAQ: data acquisition.

On the receiver side, as shown in Fig. 2(b), a 10-cm-diameter reflection mirror is used to adjust the beam direction. Two convex lenses, whose diameters and foci are 10 and 20 cm and 5 and 6 cm, respectively, reduce the beam diameter to approximately 1 cm. HWP4 is used to calibrate the polarization direction such that the receiving local oscillator is polarized along the vertical direction. The QWP changes linearly polarized light to circular polarization so that the difference in photon numbers between the two outputs of PBS3 corresponds to the Stokes parameter S_3, as in Eq. (10). Then HWP5 placed between the QWP and PBS3 acts as a basis switcher to monitor the variance of the P (i.e., S_2) quadrature. When its axis is along the PBS3 axis, the number of photons measured corresponds to the X quadrature (i.e., S_3), and when the angle between their axes is $\pi/8$, the number of photons measured corresponds to the P quadrature. A convex lens (diameter = 50 mm, focuslength = 150 mm) focuses the beam into photon diodes (Hamamatsu, S3883), whose photon sensitivity is 0.58 A/W at 780 nm, equal to a detection efficiency of 0.872 for each individual diode [30]. Another DAQ module is used to acquire the output of the voltage differences of two diodes for every pulse, at a sampling rate of 1 MHz. Since the modulated rate is 10 kHz and the duty cycle is 10%, as mentioned in the beginning of this section, for each pulse, the number of sample data is 10. The average voltage of these ten samples is the raw key value for Bob. A consecutive string of five large pulses (10 V) marks the start of each communication; in other words, the pulses that follow the start pulses are the distributed keys.

V. EXPERIMENT RESULT

First, we record the beam-spot behaviors caused by beam wandering and by vibrations of the buildings. On the receiver's side, a CCD camera beam profiler (Thorlabs, BC106N-VIS/M) at the lens focus records the profile and jitter of the beam, as shown in Fig. 3. The sensitive area of the photodiodes is approximately 1.5 mm in diameter, which is much larger than the beam diameter so that it can collect the entire light intensity. However, the intensities still fluctuate due to atmospheric turbulence.

The sender's side is placed on the 9th floor of a building, while the receiver's side is on the 16th floor of another building. Since the height of both buildings is high, their vibration is not negligible. The jitter of the beam spot and trace of the spot center are shown in Figs. 4 and 5, respectively. The peak position is where the maximum light intensity is, which corresponds to the beam jitter, while the centroid position is the mean value of the beam-spot distribution, which is

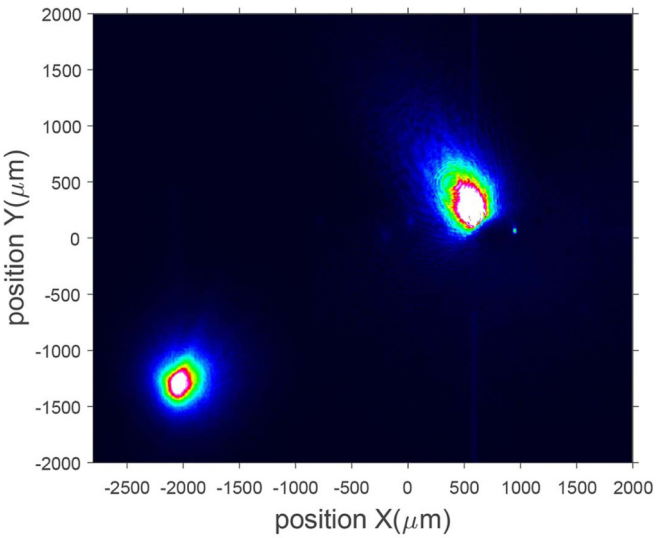

FIG. 3. Beam profiles are recorded by a CCD camera after two output ports of a PBS, on Bob's side and at the lens focus: vertically polarized (left) and horizontally polarized (right). For convenience, the two beam profiles are displayed in one figure. The horizontal and vertical axes are the position of the beam, in units of micrometers. The diameters of the two beams are not exactly the same, as the CCD deviates from the lens focus in the two directions. The profiles are nearly Gaussian in both the x and y directions, but the shape changes with time.

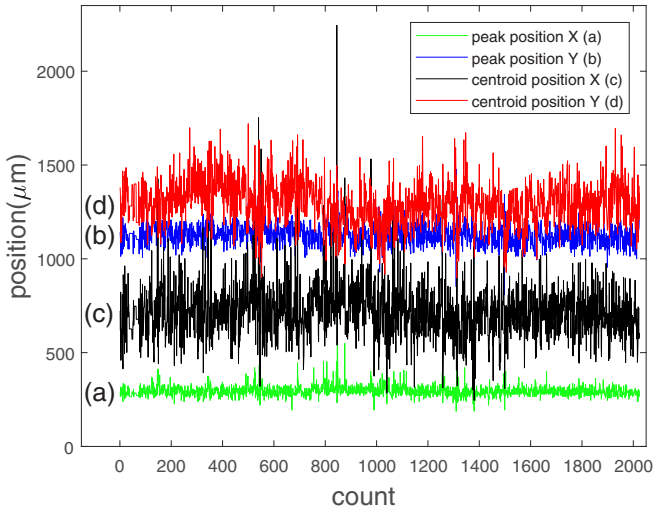

FIG. 4. The center of the horizontal (X) and vertical (Y) directions as a function of time of the beam at the transmission port of the PBS. Measurement time is 21 min. Black: peak position in the x direction. Red: peak position in the y direction. Green: the position of the intensity center in the x direction. Blue: the position of the intensity center in the y direction. The average jitter in both directions is approximately 200 μm (blue and green lines).

the result of beam distortion. The jitters in both directions are mainly caused by beam wandering, while the buildings' vibration contributes a small portion of the jitter in the horizontal direction. The frequency of the buildings' vibration is much lower than the beam wandering due to atmospheric turbulence. According to Fig. 4, the standard deviations of horizontal and vertical jitters are 146 and 114 μm, respectively, almost at the same level.

Although the distribution of the beam spot always varies, the centroid position is at about 500 μm, according to Fig. 4 (red and black lines), and the beam diameter focused by the lens is approximately 500 μm, according to Fig. 3.

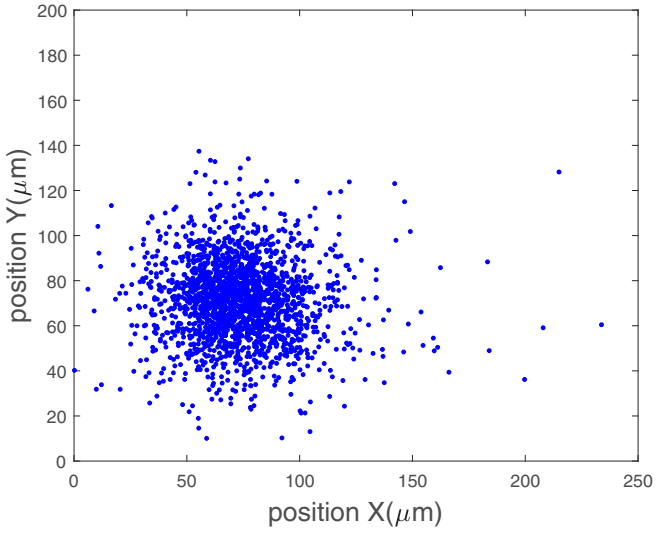

FIG. 5. Relative positions of peak intensity of the beam spot. Jitters in both directions are close.

Therefore, the whole intensity cannot always impinge on the sensitive area of the photodiodes, which has a 1 mm diameter. Since the homodyne detector subtracts the two intensities of the transmission and reflection output of the PBS, the jitter of the differential intensity should be suppressed; however, in practice, the situation is not ideal because the distance between detector 1 and the transmittance port of PBS3 is not exactly the same as the distance between detector 2 and the reflection port of PBS3. Therefore, the beam-spot distributions on two photodiodes are not always the same, causing the differential intensity to vary with time and thus an error in measuring the local oscillator intensity.

Before modulating the signal, the shot noise and electronic noise must be measured by a DAQ. The intensity of the laser output from the EOM is 100 μW, while there is a 65-μW input to the photodiodes. When the laser is turned off, the variance of the measured data is the electronic noise $V_e N_0$, having units of square volts. After turning on the light, when the detection is balanced, the variance is $N_0(1+V_e)$. Subtracting the two variances results in the shot noise $N_0 = 15.4\ \mathrm{mV}^2$, and thus, $V_e = 0.0219$. Then, a 5×10^5 Gaussian distributed (pseudo)random variable, centered at zero, with a variance of $1\ \mathrm{V}^2$, is generated by computer software. These random numbers are used as the pulse amplitudes, which are generated by the output of the DAQ, in volts. The modulation variance $V_M = 165$ when $\Sigma = 1$ V. However, a smaller V_M would be comparable to the leaked light from the local oscillator since the isolation ratio of a single PBS is only approximately 33 dB. The total transmittance measured with a power meter is 0.65, including the optical components reflecting loss and channel loss.

The block size of the sampled data is 2.1×10^7, including 2.1×10^5 pulses, and the period between two consecutive blocks is 1 min. Finally, five data blocks were acquired, including 1.05×10^6 pulse amplitudes as n_{meas}, mentioned in Eq. (12). A randomly chosen portion, approximately 1/5 of the data, 2×10^5 pulse amplitudes, is used to estimate the channel parameters T and ϵ based on the following equations:

$$\tilde{T} = \left[\frac{\mathrm{Cov}(X_a, X_b)}{V_M}\right]^2,$$
$$\tilde{\epsilon} = \frac{\mathrm{Var}(X_b) - V_e - 1}{\eta\tilde{T}} - V_M, \tag{34}$$

where X_a and X_b are Alice's and Bob's chosen strings of data. The excess noise $\tilde{\epsilon} = 0.0375$, and $\tilde{T} = 0.575$, and the latter is lower than that measured by the power meter since the sensitive area of the power meter is much larger than that of the photodiodes. Another 1/5 of the total data is used to monitor the variance of the P quadrature, controlled by HWP4. When the rotation angle is 22.5°, the polarization direction changes by 45° to measure S_2 modes. Therefore, V_{P1} of Eq. (23) is 1.00.

With all the parameters achieved above, the security key rate can be evaluated. At a distance of 460 m in an atmospheric environment, the secret key rate is 0.0254 bit per pulse at a typical reconciliation efficiency of 0.95, corresponding to 0.152 kbps, while the secret key rate is 0.23 bit per pulse in a laboratory environment at the same modulation voltage and electronic noise but at a lower local oscillator intensity

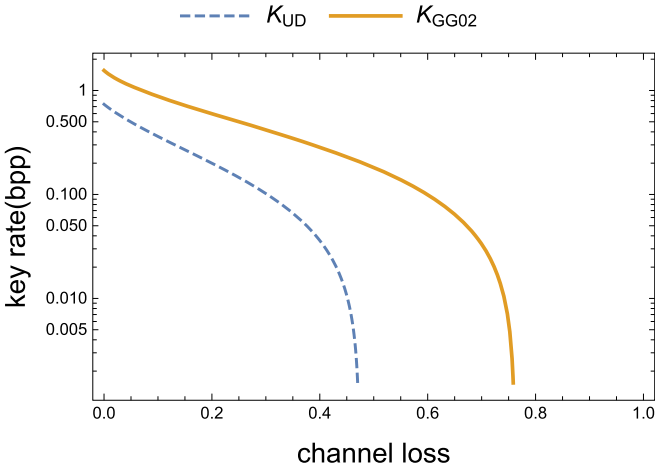

FIG. 6. They key rate at different channel transmittances. Solid line: GG02; dashed line: unidimensional protocol. Main parameters: $V_M = 165$, $\epsilon = 0.0375$, $V_{P1} = 1.0$, $V_e = 0.0219$, $\eta = 0.872$; bpp: bit per pulse.

(30 μW). We measured the data at 2:30 a.m., when the atmospheric turbulence was relatively low, on 29 September. The beam was centered at the receiver's aperture, and most of the wandering occurred within the reflection mirror and lens. In this condition, the loss caused by atmospheric turbulence is approximately 20%, while the system insertion loss of approximately 20% is due to the optical instrument reflection. We also measured data the following day at noon and in the afternoon. Since the beam always wanders, after several hours, part of the beam escapes the reflection mirror and lens. In such a condition, the maximum transmittance is only 41% and 50%, and the modulated wave form is nearly buried in quantum noise, so the DAQ cannot recognize the rising edge of the pulses, giving an inaccuracy value of X_b. Therefore, when the beam center cannot be calibrated in the daytime, the secret key rate falls to zero. Figure 6 shows the expected secret key rate of the unidimensional versus GG02 protocols at different total loss values with the experimentally measured parameters V_M, ϵ, V_e, and V_{P1}. At low channel loss, the unidimensional performs close to the GG02 protocol, but when the transmittance is less than approximately 0.6, the performance is an order of magnitude lower than that of GG02.

The presented work achieved the feasibility of a unidimensional CV-QKD experiment in a city-environment free-space channel. Although the key rate is lower than that of the GG02 protocol, it is less complex and is expected to be compatible with GG02 protocols, especially when channel loss is at a low level after further improvement.

In our experiment, the main factor to restrict the secret key rate per second is the sample rate of the DAQ and the polarization fluctuation of the laser. As mentioned above, the sample rate of DAQs is limited up to 1 MHz, and modulation frequency is even lower, far less than the response bandwidth of the EOM, 100 MHz. In addition, the memory and CPU of the computer on Bob's side are unable to process much of the key data (over 10^7), and the key rate, considering the finite-sized region, is expected to be even lower than the asymptotic limit [18]. Another restriction is the aperture of our detector-sensitive areas. Due to atmospheric turbulence, the measured intensity strongly fluctuated, bringing error into the estimate channel transmittance and thus excess noise. Finally, the fiber pigtailed laser, coupled to free space, may cause the polarization direction to change in the fiber and become unstable, leading to polarization noise and thus intensity fluctuations of 0.1%. With improvements in these aspects, the experiment of CV-QKD in such an urban environment is expected to be stabler and have higher secure key rates and extend the secure distance.

VI. CONCLUSIONS

To conclude, we achieved a free-space unidimensional CV-QKD experiment in a real urban environment, through a 460-m atmospheric channel. In such a condition, the variance of the unmodulated quadrature S_2 barely remains unchanged. With the correlation of two quadratures being unknown, the pessimistic raw key rate against collective attacks reaches 0.0254 bit per pulse, at a modulation repetition of 10 kHz. Although lower than the GG02 protocols, the unidimensional protocols can still have a positive security key rate in free space and simplified experiment setups. However, since the beam wanders at any time, the average transmittance could fall to a sufficiently low level to cause the secret key rate to vanish. The system performance is expected to improve in future works.

[1] C. Bennett and G. Brassard, An update on quantum cryptography, in *Advances in Cryptology, CRYPTO*, edited by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science (Springer, Berlin, Heidelberg, 1984), Vol. 196, pp. 475–480.
[2] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[4] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[5] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[6] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[7] J. Heersink, V. Josse, G. Leuchs, and U. Andersen, Opt. Lett. **30**, 1192 (2005).
[8] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).
[9] 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).
[10] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).
[11] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, and G. Leuchs, New J. Phys. **11**, 045014 (2009).

[12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, and P. Grangier, Nat. Photonics **7**, 378 (2013).
[13] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[14] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).
[15] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[16] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[17] X. Wang, W. Liu, P. Wang, and Y. Li, Phys. Rev. A **95**, 062330 (2017).
[18] P. Wang, X. Wang, J. Li, and Y. Li, Opt. Express **25**, 27995 (2017).
[19] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[20] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[21] M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).
[22] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[23] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[24] Q. Liao, Y. Guo, C. Xie, D. Huang, P. Huang, and G. Zeng, Quantum Inf. Process. **17**, 113 (2018).
[25] S. Wang, P. Huang, T. Wang, and G. Zeng, New J. Phys. **20**, 083037 (2018).
[26] N. Korolkova, G. Leuchs, R. Loudon, T. C. Ralph, and C. Silberhorn, Phys. Rev. A **65**, 052306 (2002).
[27] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).
[28] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).
[29] https://www.thorlabschina.cn/thorproduct.cfm?partnumber=EO-AM-NR-C1.
[30] http://www.hamamatsu.com/jp/en/S3883.html?_ga=2.225910483.817825542.1517410830-81292748.1517410830.