Phase-noise estimation using Bayesian inference for discretely modulated measurement-device-independent continuous-variable quantum key distribution

Wei Zhao,[1] Ronghua Shi,[1] Jinjing Shi,[1] Xinchao Ruan,[2] Ying Guo,[2] and Duan Huang[1,*]
[1]*School of Computer Science and Engineering, Central South University, Changsha 410083, China*
[2]*School of Automation, Central South University, Changsha 410083, China*

(Received 13 March 2020; accepted 7 August 2020; published 25 August 2020)

Measurement-device-independent continuous-variable quantum key distribution (MDI-CVQKD) protocol calibrates the phase reference frames by transmitting local oscillator pulses between two legitimate parties. The above implementation leaves massive loopholes; in particular, an eavesdropper can attack the system by manipulating the power of the local oscillator pulses. In this paper, a Bayesian phase-noise estimation model is proposed to estimate the phase drift and its uncertainty in the MDI-CVQKD protocol. The model employs the Bayesian estimation of the very weak quantum signal pulses and eliminates the necessity of transmitting local oscillator pulses between two legitimate parties. Moreover, the Bayesian inference algorithm has the characteristic of high robustness to noise and can achieve a well-motivated confidence interval of the estimated eigenphase. Comparing with its Gaussian counterpart, we adopt the discrete modulation in the MDI-CVQKD protocol, which allows a much better reconciliation efficiency at low signal-to-noise ratio. With simpler implementation, the proposed Bayesian phase-noise estimation model precisely avoids the security bottleneck due to the transmitted local oscillator pulses.

DOI: 10.1103/PhysRevA.102.022621

I. INTRODUCTION

Continuous-variable quantum key distribution (CVQKD) [1–5], as a competitor to the traditional discrete-variable counterpart, encodes the key information on the quadratures of the light field, and adopts coherent detection, such as homodyne and heterodyne detection, to measure the received signal. Its security of the shared keys is guaranteed by the laws of quantum physics [6–9]. From a practical point of view, the continuous variable enjoys a number of advantages for quantum key distribution: it has higher key generation rate and better compatibility with existing communication systems [10–13], which has developed rapidly in recent years. Significant efforts have been made to establish the system of CVQKD, such as the thermal-state protocol [14–17], unidimensional protocol [18,19], two-way protocol [20], finite-size aspect [7–9], quantum router [21,22] and quantum repeater [23], experimental [24–26], and postprocessing protocols [10,27,28].

With the rapid development and application of complex networks, researchers have progressively extended the field of continuous-variable quantum cryptography from point to point to a more robust end-to-end formulation. One of the most valuable measurements is the measurement-device-independent (MDI) CVQKD [29,30], which removes the loopholes of the practical detectors and solves all the side-channel attacks against detectors. MDI-CVQKD was proposed in Ref. [31] both theoretically and experimentally. In MDI-CVQKD protocol, a basic network topology is constructed where two legitimate parties (i.e., Alice and Bob) connect to a distrusted intermediate relay (i.e., Charlie) for communication via insecure links. The intermediate relay receives quantum states sent by Alice and Bob and then performs Bell-state measurement. Such measurement results will be used by two legitimate parties in a postprocessing step to generate secure keys. The MDI-CVQKD protocol has been modified with phase self-alignment [32], noiseless linear amplifiers [33], and squeezed states [34]. So far, the best decoding strategy is to guess which variable of the party is closer to the relay [31], though the maximal transmission distance of MDI-CVQKD is still unsatisfactory in the practical implementation. One of the main obstacles is that the MDI-CVQKD protocol is based on the Gaussian modulation and Gaussian states, which results in the lower reconciliation efficiency in the case of long distance transmission with low signal-to-noise ratio.

Compared with its Gaussian counterpart, the discrete modulation has the advantage of the simpler implementation and longer achievable maximal transmission distance [35]. The first discretely modulated CVQKD protocol was proposed in Ref. [36], which is based on a binary encoding of coherent states. Its security has been proven against Gaussian attacks [35] and general attacks [37]. Besides, the discrete modulation also has good compatibility with an efficient error correction code, which leads to higher reconciliation efficiency even at low signal-to-noise ratio. According to the above mentioned, in this manuscript, we continue to investigate the MDI-CVQKD protocol by employing the discrete modulation. It also has been demonstrated that the MDI-CVQKD protocol with the discrete modulation is secure against collective attacks in the asymptotic limit [37]. Without loss of generality,

*Corresponding author: duan.huang@foxmail.com

we mainly focus on the eight-state scheme [38]; in particular, the legitimate parties prepare eight nonorthogonal coherent states, and exploit the sign of measured quadratures of each state to encode the bits of the secret key rate.

In the practical system of MDI-CVQKD, the light sources of two legitimate parties are independent, so that the initial optical pulses they emit may not stay in the same phase reference frame. Therefore, the local oscillator pulses are employed as the phase reference light of signal pulses in the conventional MDI-CVQKD protocols [39]. First, Alice divides its local oscillator pulses into two beams; a fraction is sent to Charlie for Bell-state measurement and the other portion is sent to Bob. After receiving the local oscillator pulses sent by Alice, Bob interferes with his locally generated local oscillator pulses. Subsequently, Bob performs the relative phase estimation and correction, and then adds the phase difference to his quantum signal pulses. Hence the two legitimate parties stay in the same phase reference frame. Practically, the oscillator pulses are strong classical light, so that an eavesdropper can manipulate it to attack the system, such as intercept-resend attack [40], calibration attack [41], wavelength attack [42,43], jitter in clock synchronization attack [44], and polarization attack [45]. Therefore, transmitting local oscillator pulses from Alice to Bob leaves a massive loophole for eavesdroppers. In order to prevent LO attacks altogether, Qi *et al.* [46], Soh *et al.* [47], and Huang *et al.* [13] propose a self-reference scheme where Bob could generate the local oscillator locally. Nevertheless, the security would also be reduced when propagating the referenced pulse through the optical fiber. For instance, Ren *et al.* propose a reference pulse attack that even a local oscillator locally could be vulnerable to a hacking attack if the trusted parties assume that the phase noise is trusted, but cannot be used by Eve [48].

In the discretely modulated MDI-CVQKD protocol, we propose a Bayesian phase-noise estimation model to estimate the phase drift and its uncertainty. In the Bayesian model, at Alice's side, quantum signal pulses output from the laser splits into two portions, a fraction of which is sent to Charlie; the other portion is sent to Bob. At Bob's side, his quantum signal pulses are sent to Charlie, meanwhile, his local oscillator pulses also split into two portions, a fraction of which is sent to Charlie for Bell-state measurement; the other portion interferes with Alice's received quantum signal pulses to perform Bayesian phase estimation [49]. The model employs the Bayesian estimator of the very weak quantum signal pulses and eliminates the necessity of transmitting a local oscillator pulse from Alice to Bob. Hence the scheme could avoid the security vulnerabilities caused by transmitted local oscillator pulses. Besides, the Bayesian inference algorithm has the characteristic of high robustness to noise and can achieve a well-motivated confidence interval of the estimated eigenphase [50,51].

This paper is structured as follows. In Sec. II, it presents the eight-state MDI-CVQKD protocol, especially the prepare-and-measure version and entanglement-based version. Then it derives the secret key rate and gives the numerical simulation and performance analysis of the proposal. In Sec. III, to achieve the phase-noise estimation for the eight-state MDI-CVQKD protocol, how to utilize the Bayesian inference algorithm is discussed. Besides, the practical security of the proposal is analyzed. Finally, the conclusion is drawn in Sec. IV.

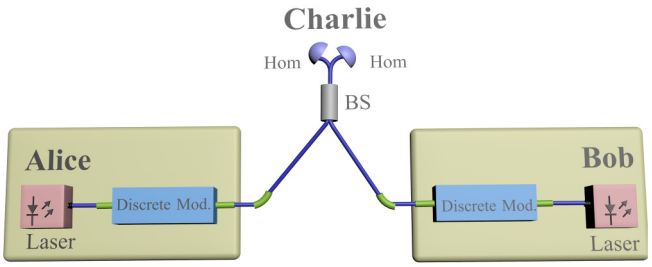


FIG. 1. PM scheme of the eight-state MDI-CVQKD protocol. BS, beam splitter; Discrete Mod., discrete modulation; Hom, homodyne detection.

II. Discretely modulated MDI-CVQKD protocol

In this section, we first review the basic notions related to the discrete modulation. Without loss of generality, we mainly focus on the eight-state scheme [38,52]. Then we present the discretely modulated MDI-CVQKD protocol, especially the prepare-and-measure (PM) version and entanglement-based (EB) version.

A. MDI-CVQKD with discrete modulation

In the MDI-CVQKD protocol, the PM version is equal to the EB version. To be specific, the PM version is applied to implementation, while the equivalent EB version is convenient for security analysis [53]. We introduce the PM version first, then the EB version. As shown in Fig. 1, the standard PM version description of the eight-state MDI-CVQKD protocol is described as follows.

Step 1. Alice randomly prepares coherent state $|\varrho\rangle = |\hat{q}_A + i\hat{p}_A\rangle$ from the data set

$$\{|\alpha_k\rangle | \alpha_k = \alpha\, e^{i\frac{k\pi}{4}}, \quad \text{for } k \in \{0, 1, 2, \ldots, 7\}\}, \tag{1}$$

while Bob randomly prepares another coherent state $|\varsigma\rangle = |\hat{q}_B + i\hat{p}_B\rangle$. Here, α is a positive number related to the modulation variance $V_M = 2\alpha^2$ of coherent states. The two modes are then sent to Charlie to perform a Bell-state measurement, the detection of which corresponds to measuring the quadrature operations $\hat{q}_- = (\hat{q}_A - i\hat{q}_B)/\sqrt{2}$ and $\hat{q}_+ = (\hat{p}_A + i\hat{p}_B)/\sqrt{2}$.

Step 2. The classical outcome χ is combined in a complex variable $\chi = (\hat{q}_- + i\hat{p}_+)/\sqrt{2}$, and then measurement results are publicly announced by Charlie.

Step 3. Bob infers the variable of Alice by simple post-processing such as $\varsigma^* + \chi = \rho$. Here, $*$ represents conjugate property of the complex number.

Step 4. Alice and Bob use an authenticated channel to achieve parameter estimation, information reconciliation, and privacy amplification.

In the EB version, as shown in Fig. 10, Alice and Bob prepare two-mode squeezed states (TMSSs) $|\Psi_8\rangle_{A_1A_2}$ and $|\Psi_8\rangle_{B_1B_2}$, respectively. Here, the variances of the two modes are $V_A = V_B = 1 + V_M$. The two-mode entangled state

prepared by Alice and Bob is

$$|\Psi_8\rangle = \sum_{k=0}^{7} \sqrt{\lambda_k}|\phi_k\rangle|\phi_k\rangle = \frac{1}{4}\sum_{k=0}^{7}|\Psi_k\rangle|\alpha_k\rangle, \tag{2}$$

with the notation

$$|\Psi_k\rangle = \frac{1}{2}\sum_{m=0}^{7} e^{\frac{i(4k+1)m\pi}{4}}|\phi_m\rangle, \tag{3}$$

with $m \in \{0, 1, 2, \ldots, 7\}$ and

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{i=0}^{\infty}\frac{\alpha^{8n+k}}{\sqrt{(8n+k)!}}|8n+k\rangle, \tag{4}$$

for $k \in \{0, 1, 2, \ldots, 7\}$ and

$$\begin{aligned}
\lambda_{0,4} &= \frac{1}{4}e^{-\alpha^2}\left(\cosh\alpha^2 + \cos\alpha^2 \pm 2\cos\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right),\\
\lambda_{1,5} &= \frac{1}{4}e^{-\alpha^2}\left(\sinh\alpha^2 + \sin\alpha^2 \pm \sqrt{2}\cos\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}}\right.\\
&\quad \left.\pm\sqrt{2}\sin\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right),\\
\lambda_{2,6} &= \frac{1}{4}e^{-\alpha^2}\left(\cosh\alpha^2 - \cos\alpha^2 \pm 2\sin\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}}\right),\\
\lambda_{3,7} &= \frac{1}{4}e^{-\alpha^2}\left(\sinh\alpha^2 - \sin\alpha^2 \mp \sqrt{2}\cos\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}}\right.\\
&\quad \left.\pm\sqrt{2}\sin\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right).
\end{aligned} \tag{5}$$

Accordingly, the covariance matrix $\Gamma_{A_1A_2}$ of the state $|\Psi_8\rangle$ can be expressed as

$$\Gamma_8 = \begin{pmatrix} X\mathbb{I}_2 & Z_8\sigma_Z \\ Z_8\sigma_Z & Y\mathbb{I}_2 \end{pmatrix}, \tag{6}$$

with the notation $X = 1 + 2\alpha^2$, $Y = 1 + 2\alpha^2$, $Z_8 = 2\alpha^2\sum_{k=0}^{7}\lambda_{k-1}^{3/2}\lambda_k^{-1/2}$, $\mathbb{I}_2 = \mathrm{diag}(1, 1)$, and $\sigma_Z = \mathrm{diag}(1, -1)$. Though the discretely modulated MDI-CVQKD protocol may extremely improve the transmission distances, however, the unconditional security proof of the discrete modulation relies on the linear channel assumption [54]. It is worth mentioning that utilizing the decoy states can solve the above assumption and avoid the states-discrimination attack in the discretely modulated MDI-CVQKD protocol [55]. Besides, the secret key rate of eight-state protocol is analyzed in Appendix A.

B. Performance analysis

In Eq. (A3), the covariance matrix $\Gamma_{A_1B_1'}$ has the same form as in the Gaussian modulation protocol, where Z_8 would be replaced by the correlation of a two-mode squeezed vacuum $Z_G = \sqrt{V_M^2 + 2V_M}$. As depicted in Fig. 2, when V_M is sufficiently low, Z_8 is very close to Z_G. For $V_M \leqslant 1$, Z_8 and Z_G are almost indistinguishable. That is to say, in the above region, the bound on the maximal information available to Eve is very similar in these two protocols. Hence the optimal regime of the modulation variance V_M is from 0 to 1. Besides, Fig. 2 also compares the correlation parameter Z_8 and Z_4. We can see that

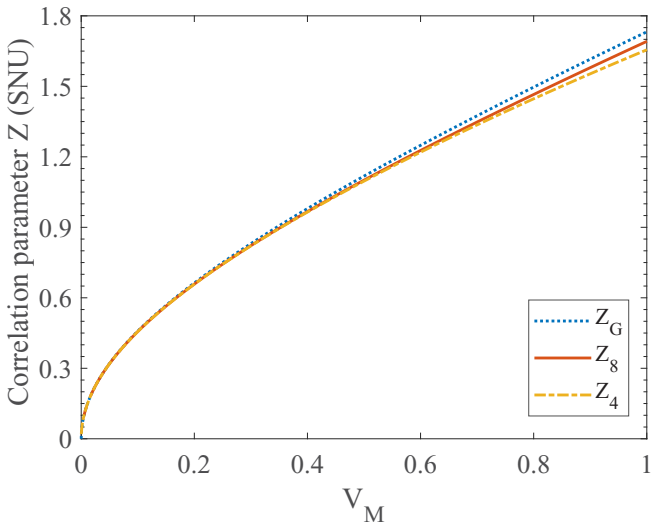


FIG. 2. Comparison of the correlation Z_8 for the eight-state protocol, Z_4 for the four-state protocol, and Z_G for the Gaussian modulation protocol as a function of the modulation variance V_M. SNU represents shot-noise units.

the amount of correlation between the trusted parties' signals of the eight-state protocol has been enhanced by four-state protocol. This may imply that eight-state protocol can achieve higher key rates in the optimal regime. In what follows, we will discuss the optimal regime in the simulation results when we optimize the secret key rate.

Numerical simulations are employed to reveal how parameter V_M affects the performance. In order to find an optimal V_M to maximize the secret key rate in the asymmetric scenario, we need to scan V_M within a legitimate region. Figure 3 shows

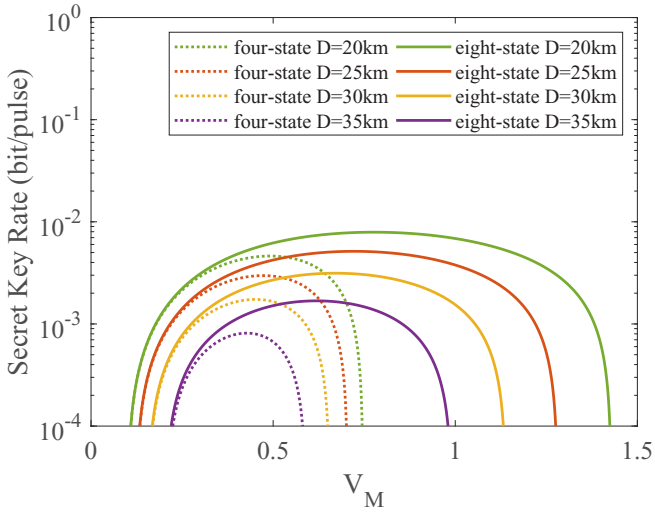


FIG. 3. Compressed variation trend of modulation variance V_M optimal interval of the eight-state and four-state MDI-CVQKD protocol with different transmission distance in the asymmetric scenario. Here, Charlie is extremely to Bob in the asymmetric scenario ($L_{BC} = 0$) [34,53,56,57]. Transmission distance from Alice to Charlie is set as 20 km, 25 km, 30 km, and 35 km, respectively. Other parameters are set as $\varepsilon_A = \varepsilon_B = 0.002$ and $\beta = 0.99$.

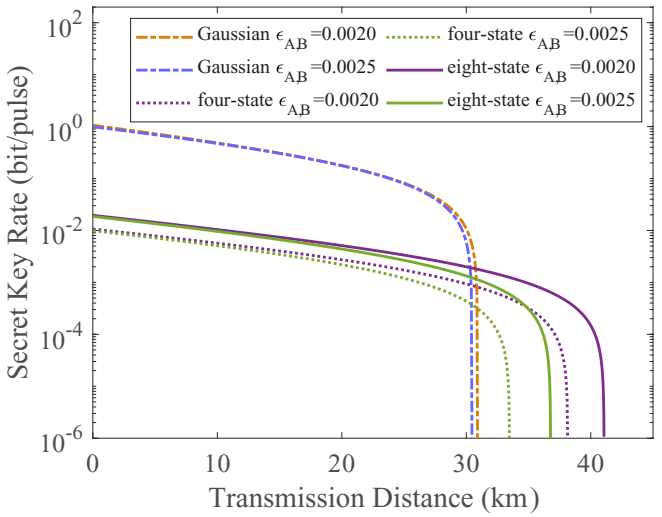
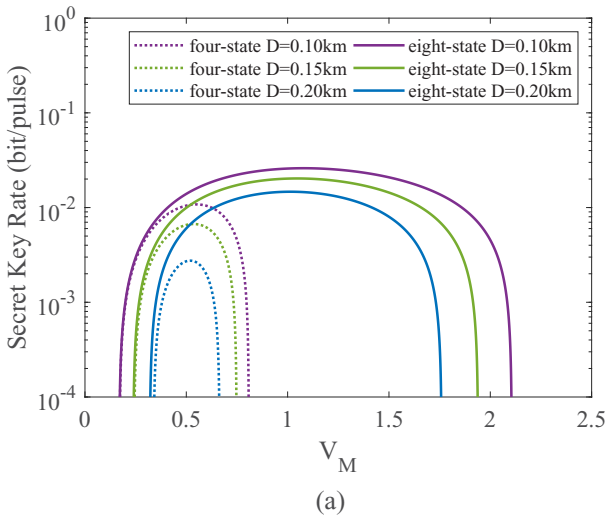


FIG. 4. Secret key rates as a function of the transmission distance in the asymmetric scenario. Here, Charlie is extremely to Bob in the asymmetric scenario ($L_{BC} = 0$). The solid lines denote the eight-state protocol, the dot-dashed lines denote the four-state protocol [58], and the dashed lines denote the Gaussian-modulated protocol [31].

the secret key rates as a function of the modulation V_M in the asymmetric scenario, for both the eight-state and four-state protocol. The eight-state protocol is denoted by solid lines and the four-state protocol is denoted by dashed lines. As shown in Fig. 3, it is obvious that there exists a global optimal V_M that makes key rates achieve the maximum value with different transmission distance in the asymmetric scenario. To be specific, the optimal value of the modulation variance V_M is approximately 0.8 and 0.45 in the eight-state and four-state protocol, respectively. By comparing, we can also conclude that the modulation variance range of the eight-state protocol is wider than that of the four-state protocol. Moreover, the maximum key rates and the optimal modulation variance of the eight-state protocol are both larger than that of the four-state protocol under the same scenarios. Besides, from the simulation results shown in Fig. 3, the numerical areas of V_M that make key rates achieve maximum are gradually compressed when the transmission distance increases.

Figure 4 depicts the relationship between the secret key rates and the transmission distance in the asymmetric scenario, for eight-state, four-state, and Gaussian-modulated protocol. The eight-state protocol is denoted by solid lines, while the four-state and Gaussian-modulated protocols are denoted by dot-dashed lines and dashed lines, respectively. For one thing, the maximum transmission distance of discretely modulated protocol, such as the eight state and four state, is always longer than that of the Gaussian-modulated protocol. For another, the eight-state protocol is obviously outperformed by the four-state protocol, which can achieve higher secret key rates and longer transmission distance.

Subsequently, we consider the performance of the symmetric scenario, where the length of two independent quantum channels is equal. As we mentioned above, in order to find an optimal modulation variance V_M to maximize the secret key rate in the symmetric scenario, we need to scan V_M within a legitimate region. Figure 5(a) shows the secret key rates as a function of the V_M in the symmetric scenario, for both eight-state and four-state protocols. In particular, the optimal value of the V_M is approximately 1 and 0.5 in the eight-state and four-state protocols, respectively. The maximum key rates and the optimal modulation variance of the eight state and four state are both larger than that of the four-state protocol in the symmetric scenario, which is similar to what is shown in Fig. 3. Figure 5(b) depicts the relationship between the secret key rates and the transmission distance in the symmetric scenario with different excess noise, for both eight-state and



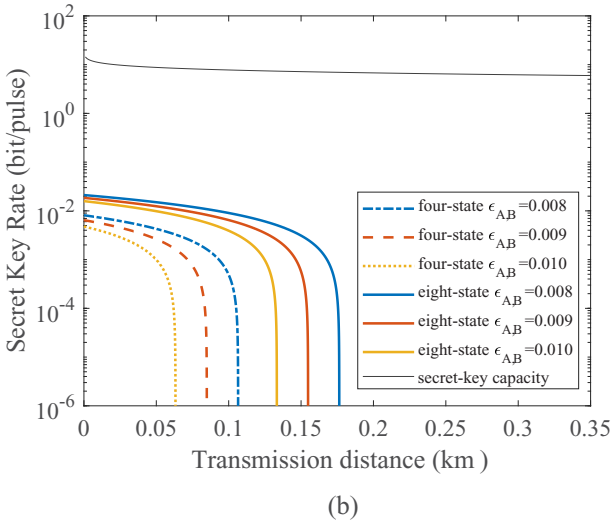


FIG. 5. (a) The compressed variation trend of modulation variance V_M optimal interval of the eight-state and four-state protocol with different transmission distance in the symmetric scenario. Here, the length of two independent quantum channels is equal. Other parameters are set as $\varepsilon_A = \varepsilon_B = 0.002$ and $\beta = 0.99$. (b) Secret key rates as a function of the transmission distance in the symmetric scenario with different excess noise. The optimal modulation V_M of eight-state and four-state protocols is set as 1 and 0.5, respectively. Here, the black solid line represents the secret-key capacity [60].

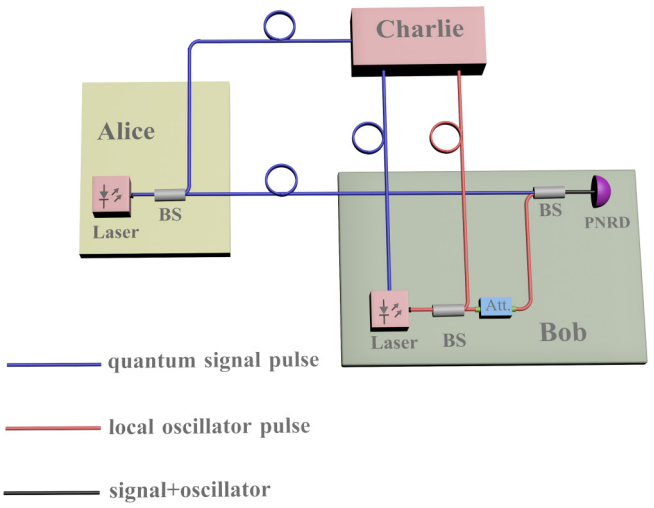


FIG. 6. Schematic structure of Bayesian phase-noise estimation. BS, beam splitter; Att., attenuator; PNRD, photon number resolving detector.

four-state protocol. As we mentioned above, we let V_M of eight state equal 1 and four state equal 0.5 in the symmetric scenario, which leads to the maximum secret key rates. The performance of discretely modulated MDI-CVQKD protocol in the symmetric scenario is far worse than that in the asymmetric scenario. Though we cannot achieve the secret key in longer distance of the symmetric scenario, it is still meaningful to analyze for a practical topology network where several players are roughly equidistant from the intermediate router.

III. DISCRETELY MODULATED MDI-CVQKD WITH BAYESIAN PHASE-NOISE ESTIMATION

A. Bayesian phase-noise estimation

In this section, we mainly discuss how to utilize the Bayesian inference algorithm to achieve the phase reference calibration in discretely modulated MDI-CVQKD protocol. For the sake of simplicity, we mainly focus on the eight-state MDI-CVQKD protocol. As depicted in Fig. 6, at Alice's side, quantum signal pulses' output from the laser splits into two portions with an intensity ratio of 50:50, a fraction of which is sent to Charlie; the other portion is sent to Bob. At Bob's side, his local oscillator pulses also split into two portions with an intensity ratio of 50:50, a fraction of which is sent to Charlie; the other portion interferes with Alice's quantum signal pulses received through the beam splitter. By interfering with Alice's quantum signal pulses and Bob's oscillator pulses, the phase drift and phase variance can be measured with a photon number resolving detector (PNRD) and Bayesian inference algorithm. At Charlie's side, he splits the received local oscillator pulses into two beams to interfere with the two received quantum signal pulses. And then Charlie uses two homodyne detection for Bell-state measurement and publicly announces the measurement results. The proposed Bayesian phase estimation model, which is depicted in Fig. 6, executes the following steps.

Step 1. Bayesian approach requires an initial prior distribution $\mathcal{P}(\phi)$ representing the confidence that the current hypotheses is the correct eigenphase. We achieve this by using a Gaussian with mean μ and variance σ^2 to model the initial prior distribution. The Gaussian with mean μ and variance σ^2 can be denoted as $\mathbb{N}(\phi|\mu,\sigma^2)$.

Step 2. The result of each new measurement $\rceil$ is used to update the mean and standard derivation based on the Bayes' rule that the probability distribution for ϕ after observing the datum is

$$\mathcal{P}(\phi|\rceil) = \frac{\mathcal{P}(\rceil|\phi)\mathcal{P}(\phi)}{\int \mathcal{P}(\rceil|\phi)\mathcal{P}(\phi)d\phi}. \tag{7}$$

Note. First, we perform experiment and achieve outcome $\rceil$. Then we draw m samples from $\mathbb{N}(\phi|\mu,\sigma^2)$. As for each sample ϕ_i, we assign ϕ_i to Φ with the likelihood function $\mathcal{P}(\rceil|\phi_i)$, while a host of samples are probabilistically discarded due to the fact that they do not match the likelihood function. Finally, we can update mean and variance with $\mu = \mathbb{E}(\Phi)$ and $\sigma^2 = \mathbb{V}(\Phi)$. Here, we have $\mathcal{P}(\rceil|\phi_i)\mathbb{N}(\phi|\mu,\sigma^2) \propto \mathcal{P}(\phi|\rceil)$, which denotes that the accepted samples are drawn from the posterior distribution [49–51].

Step 3. After updating the posterior distribution in Eq. (7), we then set the prior distribution to equal the posterior distribution. It is an iterative process which repeated for each of the experiments in the data sets. The likelihood function is defined as follows:

$$\begin{aligned}
\mathcal{P}(|\alpha_0\rangle|\phi) &= \tfrac{1}{8}[1 + e^{-\delta^2}\cos(\phi)\sin(\phi)],\\
\mathcal{P}(|\alpha_1\rangle|\phi) &= \tfrac{1}{8}[1 + e^{-\delta^2}\cos(\phi)\cos(\phi)],\\
\mathcal{P}(|\alpha_2\rangle|\phi) &= \tfrac{1}{8}[1 - e^{-\delta^2}\sin(\phi)\cos(\phi)],\\
\mathcal{P}(|\alpha_3\rangle|\phi) &= \tfrac{1}{8}[1 + e^{-\delta^2}\sin(\phi)\sin(\phi)],\\
\mathcal{P}(|\alpha_4\rangle|\phi) &= \tfrac{1}{8}[1 + e^{-\delta^2}\cos(\phi)\sin(\phi)],\\
\mathcal{P}(|\alpha_5\rangle|\phi) &= \tfrac{1}{8}[1 - e^{-\delta^2}\cos(\phi)\cos(\phi)],\\
\mathcal{P}(|\alpha_6\rangle|\phi) &= \tfrac{1}{8}[1 - e^{-\delta^2}\sin(\phi)\cos(\phi)],\\
\mathcal{P}(|\alpha_7\rangle|\phi) &= \tfrac{1}{8}[1 - e^{-\delta^2}\sin(\phi)\sin(\phi)].
\end{aligned} \tag{8}$$

Generally, we assume that quantum states undergo a phase diffusion process during propagation, whose amplitude is characterized by the parameter δ. In what follows, we express the definition of the probability density function to illustrate the relation between the phase drift and the detected photons N. The probability density function has the form

$$\mathcal{P}_{pdf}(\phi|N) = \frac{\sum_{i=0}^{7}\mathcal{P}(|\alpha_i\rangle|\phi)^{n_i}}{\mathcal{M}}, \tag{9}$$

where $\mathcal{M}$ is the normalization factor satisfying

$$\int_0^{2\pi} \mathcal{P}_{pdf}(\phi|N)d\phi = 1. \tag{10}$$

Here, N represents the total number of detected photons with $N = \sum_{i=0}^{7} n_i$, where n_i denotes the number of detected photons for state $|\alpha_i\rangle$. Considering the eight-state MDI-CVQKD protocol, the encoding phase includes eight kinds of condi-

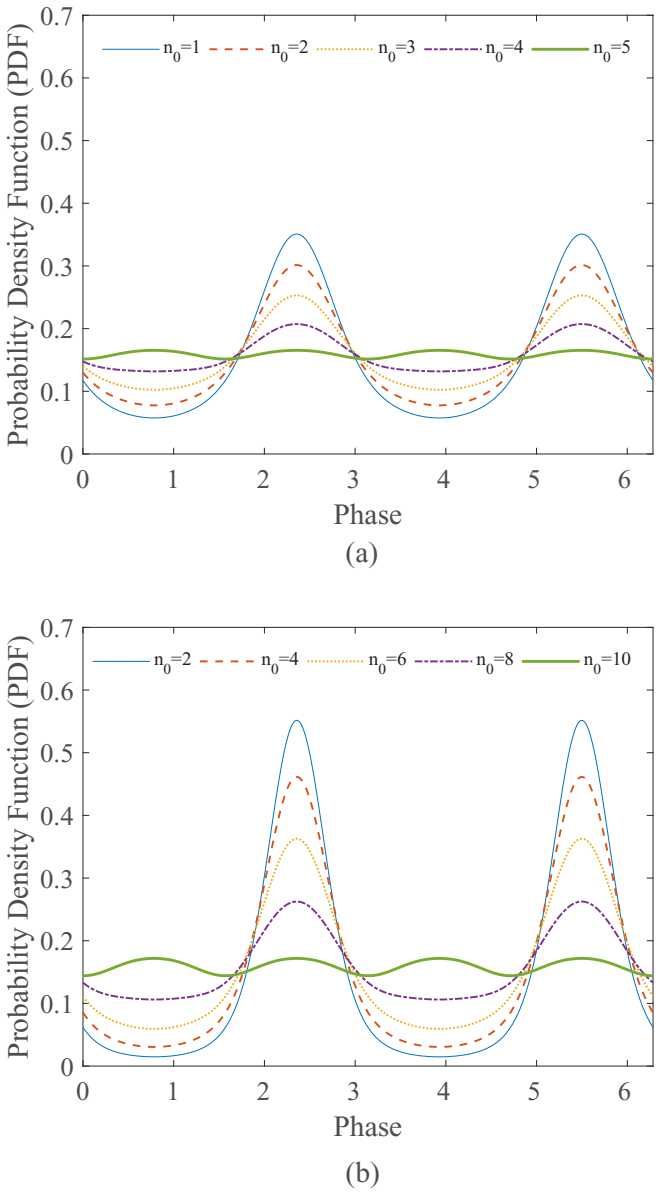


FIG. 7. Probability density function versus the phase drift with different number of detected photons. (a) The number of detected photon state $|\alpha_0\rangle$ is set as $n_0 = 1, 2, 3, 4, 5$, while other detected photon states $|\alpha_i\rangle$ are set as $n_i = 5$ with $i \in \{1, 2, \ldots, 7\}$, respectively. (b) The number of detected photon state $|\alpha_0\rangle$ is set as $n_0 = 2, 4, 6, 8, 10$, while other detected photon states $|\alpha_i\rangle$ are set as $n_i = 10$ with $i \in \{1, 2, \ldots, 7\}$, respectively. Here, we assume that quantum states undergo a phase diffusion process characterized by the amplitude parameter $\delta = 0.9$.

tions with $\phi_i = \frac{k\pi}{4}$ for $k \in \{0, 1, 2, \ldots, 7\}$. In Eq. (8), we have

$$\sum_{j=0}^{7} \mathcal{P}(|\alpha_i\rangle|\phi_j) = 1, \tag{11}$$

for each likelihood function.

The number of detected photons is a parameter that will profoundly affect the performance of the probability density function. As depicted in Fig. 7, we plot the probability density as a function of the phase drift with different detected photons. In Fig. 7(a), the number of detected photon states $|\alpha_0\rangle$ is set as $n_0 = 1, 2, 3, 4, 5$, while other detected photon states $|\alpha_i\rangle$ are set as $n_i = 5$ with $i \in \{1, 2, \ldots, 7\}$, respectively. In Fig. 7(a), the number of detected photon states $|\alpha_0\rangle$ is set as $n_0 = 2, 4, 6, 8, 10$, while other detected photon states $|\alpha_i\rangle$ are set as $n_i = 10$ with $i \in \{1, 2, \ldots, 7\}$, respectively. It is obvious that the probability density is gradually compressed when the number of photons n_0 increases, and the trend of the probability density gradually trends gently with the increase of n_0. In addition, as depicted in Fig. 7(a) and Fig. 7(b), when detected photons n_0 increase, the mean value of the received phase drift probability density function moves towards a uniformly distributed density function. Figure 8 shows the probability density distribution of phase drift with different detected photons n_0. Figures 8(a)–8(c) are three-dimensional numerical simulations, while Figs. 8(d)–8(f) are contour maps. It is obvious that, in the bottom right-hand corner of the above subgraphs, the bright yellow region has gradually expanded with increasing detected photons n_0, which is similar to what is shown in Fig. 7. Consequently, increasing the detected photons can reduce the possibility of phase drift and then improve the accuracy of phase estimation.

B. Security analysis

In Sec. III A, we present the idea and basic notions of the Bayesian inference algorithm. In the following, we utilize the model of phase estimation to analyze the practical security of the eight-state MDI-CVQKD protocol. In general, the actual phase compensation error has the following form [59]:

$$V_e = V_{ch} - V_{Baye}. \tag{12}$$

Here, the phase noise of the quantum channel is zero mean with variance V_{ch}; meanwhile, the phase noise reduced by the Bayesian inference algorithm is zero mean with variance V_{Baye}. Considering the imperfect phase compensation, the actual transmittance can be calculated as

$$\eta_\tau = \tau\eta, \tag{13}$$

where τ denotes the phase estimation accuracy with the notation $\tau = (1 - \frac{1}{2}V_e)^2$ [59]. Consequently, the actual excess noise ε_τ and actual channel-added noise χ_t^τ can be obtained as

$$\varepsilon_\tau = \frac{\varepsilon + (1-\tau)(X-1)}{\tau} \tag{14}$$

and

$$\chi_t^\tau = \frac{1}{\eta_\tau} + \varepsilon_\tau - 1. \tag{15}$$

Considering the actual phase compensation error, the final covariance matrix of state $\rho_{A_1B_1'}$ is redefined as

$$\Gamma'_{A_1B_1'} = \begin{pmatrix} a\mathbb{I}_2 & c'\sigma_Z \\ c'\sigma_Z & b'\mathbb{I}_2 \end{pmatrix} = \begin{pmatrix} X\mathbb{I}_2 & \sqrt{\eta_\tau}Z_8\sigma_Z \\ \sqrt{\eta_\tau}Z_8\sigma_Z & \eta_\tau(Y+\chi_t)\mathbb{I}_2 \end{pmatrix}, \tag{16}$$

where X, Y, and Z_8 have been mentioned in Eq. (6). In the case of reverse reconciliation, the secret key rate under collective attacks is defined in Eq. (A4), where the Shannon mutual

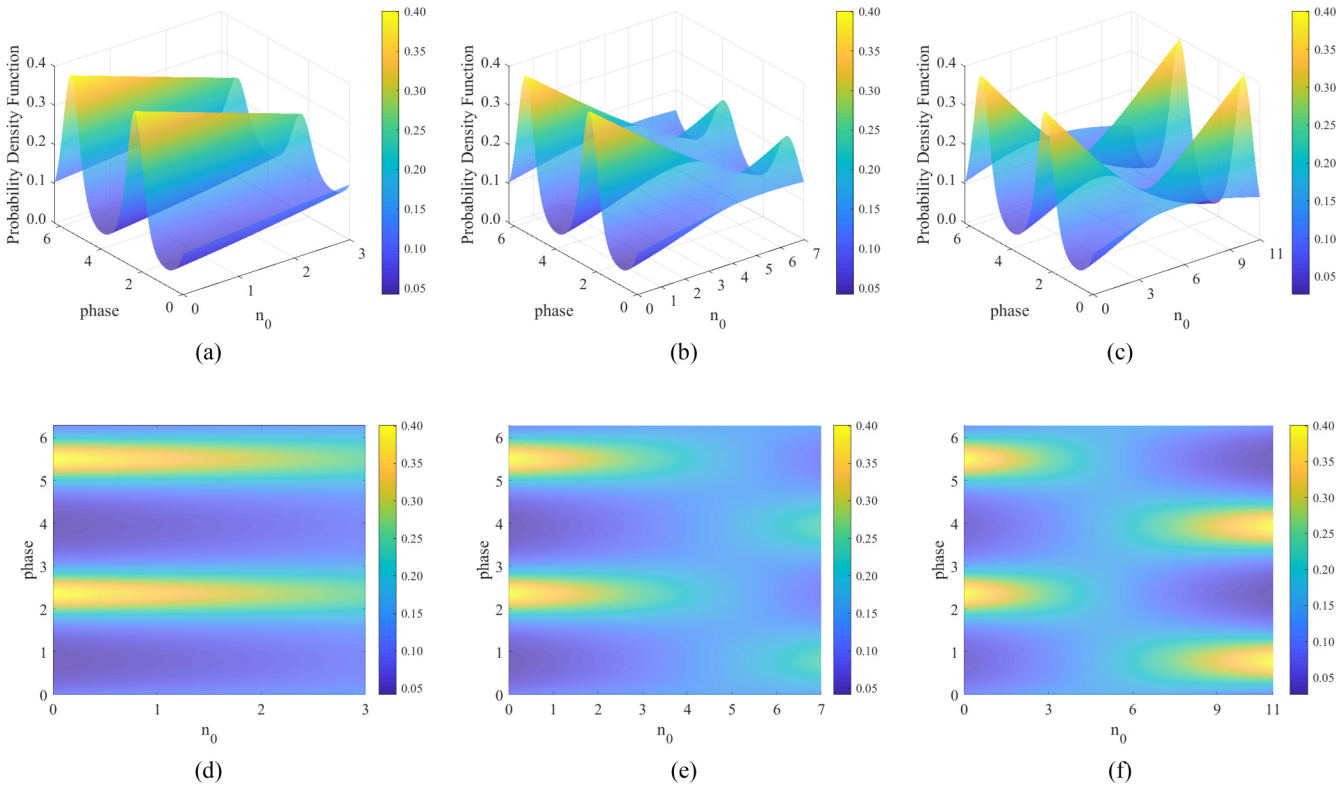


FIG. 8. Secret key rate versus phase drift and detected photons. The number of detected photon state $|\alpha_0\rangle$ is set to (a) and (d) $n_0 = 3$, (b) and (e) $n_0 = 7$, and (c) and (f) $n_0 = 11$, respectively. Other detected photon states $|\alpha_i\rangle$ are set as $n_i = 5$ with $i \in \{1, 2, \ldots, 7\}$, respectively.

information between Alice and Bob is redefined as

$$I'_{AB} = \log_2\left[\frac{a+1}{a+1-(c')^2/(b'+1)}\right]. \tag{17}$$

The Holevo quantity χ_{BE} has been expressed in Eq. (A6); in particular, the three symplectic eigenvalues are redefined as

$$k'_{1,2} = \sqrt{\frac{A' \pm \sqrt{(A')^2 - 4(B')^2}}{2}} \tag{18}$$

and

$$k'_3 = a - (c')^2/(b'+1), \tag{19}$$

where $A' = a^2 + (b')^2 - 2(c')^2$ and $B = ab' - (c')^2$.

The plot of Fig. 9 shows the practical and ideal secret key rates as a function of the transmission distance in the asymmetric scenario for the eight-state MDI-CVQKD protocol. As shown in Fig. 9(a), it is assumed that the phase noise of quantum channel V_{ch} is normally distributed with variance 0.1 (rad^2) and the phase noise V_{Baye} reduced by Bayesian inference algorithm (see Appendix B for details) is normally distributed with variance 0.094 (rad^2). Therefore, the actual deviation of phase compensation error V_{e} on quantum signals is 0.006 (rad^2). As depicted in Fig. 9(b), the practical secret key rate of the eight-state MDI-CVQKD protocol without phase estimation is denoted by dashed yellow line and the secret key rate with considering the Bayesian phase compensation is denoted by dotted red line. It is obvious that increasing accuracy of the Bayesian estimation can obviously improve the secret key rate and extend the maximum transmission distance. Accordingly, Bayesian inference algorithm can effectively reduce the phase compensation error and thereby increase the maximum transmission and secret key rate.

IV. Discussion and Conclusion

In this paper, we have investigated the phase reference calibration of MDI-CVQKD protocol. In the conventional MDI-CVQKD protocol, the light sources of two legitimates are independent, so that the initial optical pulses they emit may not stay in the same phase reference frame. The local oscillator pulses are employed as the phase reference light of signal pulses for the need of Bell-state measurement, which leaves a massive loophole for eavesdroppers. In this paper, we propose the Bayesian phase-noise estimation model to estimate the phase drift and its uncertainty of the MDI-CVQKD protocol. The model employs the Bayesian estimator of the very weak quantum signal pulse and eliminates the need for transmitting the local oscillator pulse from Alice to Bob. Hence the schematic could avoid the security vulnerabilities caused by transmitting local oscillator pulses in the MDI-CVQKD protocol. Considering large excess noise and low reconciliation efficiency are two drawbacks of CVQKD, we adopt the discrete modulation in the MDI-CVQKD protocol, which outperforms the Gaussian modulation. According to the numerical simulations, the Bayesian inference algorithm can achieve a well-motivated confidence interval of the estimated eigenphase. In our manuscript, we are working on the assumption that the quantum channel is a linear quantum channel

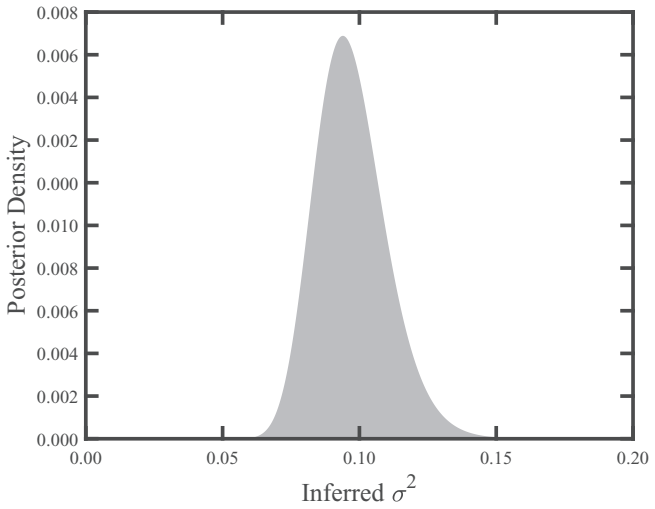


FIG. 9. (a) Phase noise of quantum channel V_{ch} is normally distributed with variance 0.1 (rad^2) and the phase noise V_{Baye} reduced by Bayesian inference algorithm is normally distributed with variance 0.094 (rad^2). (b) The practical and ideal secret key rates of the eight-state MDI-CVQKD protocol in the asymmetric scenario. The solid blue line represents the ideal secret key rate ($V_e = 0$). The solid red line represents the practical secret key rate with Bayesian phase estimation ($V_e = 0.1 - 0.094 = 0.006$). The solid yellow line represents the practical secret key rate without phase estimation ($V_e = 0.1$). Other parameters are set as $V_M = 0.5$, and $\varepsilon_{A,B} = 0.002$, and $\beta = 0.99$. Here, the black solid line represents the secret-key capacity [60].

[61–63]. That is to say, we restrict Eve's attack performed to a linear quantum channel. Fortunately, Shouvik *et al.* establish a lower bound on the asymptotic secret key rate of CVQKD with a discrete modulation of coherent states [37]. The bound is valid to collective attacks. This work is a major step towards establishing the full security of continuous-variable protocol with a discrete modulation. We hope the proposed scheme could further improve the security of the MDI-CVQKD protocol.

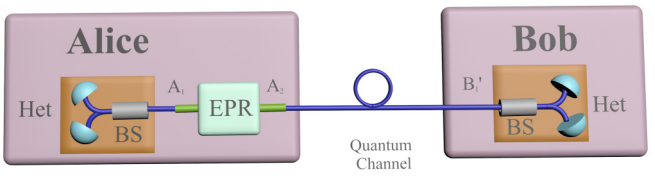


FIG. 10. Equivalent one-way protocol of the eight-state MDICVQKD protocol in EB schematic.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grants No. 61801522 and No. 61872390) and the National Natural Science Foundation of Hunan Province, China (Grant No. 2019JJ40352).

APPENDIX A: SECRET KEY RATE

In the EB scheme, if one further assumes Bob's initial two-mode squeezed state and the displacement operation is untrusted, the protocol can be converted into a well-known one-way CVQKD protocol [53]. The equivalent one-way schematic is depicted in Fig. 10. Accordingly, the secret key rate of the one-way protocol $\mathcal{K}_{\text{one}}$ can be a lower bound of the EB scheme $\mathcal{K}_{\text{EB}}$. Without loss generality, we use the method to calculated secret key rate of one-way protocol to achieve $\mathcal{K}_{\text{EB}}$.

As shown in Fig. 11, the channels from Alice to Charlie and Bob to Charlie are two independent quantum channels. We set each quantum loss as $\alpha = 0.2$ dB/km, and the channel transmittance is calculated as $\eta_A = 10^{-\alpha L_{AC}/10}$ and $\eta_B = 10^{-\alpha L_{BC}/10}$, respectively. Hence the equivalent excess noise of the one-way protocol can be expressed as [58]

$$\varepsilon = 1 + \chi_A + \frac{\eta_B}{\eta_A}(\chi_B + 1) + \frac{\eta_B}{\eta_A}\left[\sqrt{\frac{2}{\eta_B g^2}}\sqrt{V_B - 1} - \sqrt{V_B + 1}\right]^2, \tag{A1}$$

with the notation $\chi_A = \frac{1}{\eta_A} - 1 + \varepsilon_A$ and $\chi_B = \frac{1}{\eta_B} - 1 + \varepsilon_B$. Here, g represents the gain of displacement. In order to min-

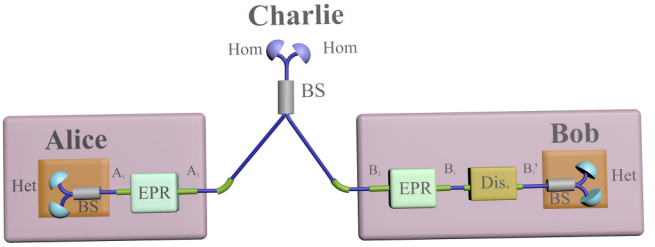


FIG. 11. EB scheme of the eight-state MDI-CVQKD protocol. BS, beam splitter; EPR, two-mode squeezed state; Dis., displacement operation; Het, heterodyne detection; Hom, homodyne detection.

Algorithm 1. Bayesian phase estimation.

Input: Initial prior probability distribution $\mathcal{N}(\mu_0, \sigma_0)$, constant $\mathcal{K}_E$.
Output: the phase estimation mean μ and phase standard derivation σ.

$\mu = \mu_0, \sigma = \sigma_0$. % Initialization data.
for $i \in 1 \longrightarrow m$ **do**
  Obtain the measurement outcome $\mathcal{E}$ from the experiment.
  $(\mu, \sigma) = \text{Update}(\mathcal{E}, \mu, \sigma, \mathcal{K}_E)$. % Update the prior distribution based on the likelihood function.
end for
return (μ, σ).

imize the equivalent excess noise, we choose $g = \sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B+1}}$ [53]; then we obtain

$$\varepsilon = \frac{\eta_B}{\eta_A}(\chi_B - 1) + 1 + \chi_A. \tag{A2}$$

We assume the homodyne detectors are ideal apparatuses, so that the total channel added noise can be expressed as $\chi_t = \frac{1}{\eta} - 1 + \varepsilon$, where $\eta = \frac{\eta_A g^2}{2}$ is a normalized parameter. According to that mentioned above, the final covariance matrix of state $\rho_{A_1B_1'}$ is

$$\Gamma_{A_1B_1'} = \begin{pmatrix} a\mathbb{I}_2 & c\sigma_Z \\ c\sigma_Z & b\mathbb{I}_2 \end{pmatrix} = \begin{pmatrix} X\mathbb{I}_2 & \sqrt{\eta}Z_8\sigma_Z \\ \sqrt{\eta}Z_8\sigma_Z & \eta(Y+\chi_t)\mathbb{I}_2 \end{pmatrix}, \tag{A3}$$

where X, Y, and Z_8 have been mentioned in Eq. (6). The secret key rate under collective attacks can be defined as

$$\mathcal{K}_{EB} = \beta I_{AB} - \chi_{BE}, \tag{A4}$$

where β represents the reconciliation efficiency, I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} denotes the Holevo quantity between Eve and Bob. Here, I_{AB} and χ_{BE} can be expressed as

$$I_{AB} = \log_2\left[\frac{a+1}{a+1-c^2/(b+1)}\right] \tag{A5}$$

and

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{k_i - 1}{2}\right) - G\left(\frac{k_3 - 1}{2}\right), \tag{A6}$$

with the notation

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{A7}$$

Algorithm 2. Bayesian prior distribution updating function.

Input: phase mean μ and standard derivation σ, measurement outcome $\mathcal{E}$, constant $\mathcal{K}_E$.
Output: phase estimation mean μ' and phase standard derivation σ' of the posterior distribution.

function Update$(\mathcal{E}, \mu, \sigma, \mathcal{K}_E)$
  $\mu_{acc}, \mu'_{acc}, V_{acc}, V'_{acc} = 0$.
  for $i \in 1 \longrightarrow n$ **do**
    $x \sim \mathcal{N}(\mu, \sigma)$
    $x = x \bmod 2\pi$.
    $x' = x + \pi \bmod 2\pi$.
    $u \sim$ Uniform $(0, 1)$. % The probability $\mathcal{P}(\mathcal{E}|x)$ of the acceptable particle.
    if $\mathcal{P}(\mathcal{E}|x) \geqslant \mathcal{K}_E u$ **then**
      $\mu_{acc} = \mu_{acc} + x$.
      $V_{acc} = V_{acc} + x^2$.
      $V'_{acc} = V'_{acc} + x'^2$.
      $N_{acc} = N_{acc} + 1$.
    end if
  end for
  $\mu' = \mu_{acc}/N_{acc}$.
  $\sigma' = \min[\sqrt{(V_{acc} - \mu_{acc}^2)/(N_{acc} - 1)}, \sqrt{(V'_{acc} - \mu_{acc}^2)/(N_{acc} - 1)}]$.
  return (μ', σ').
end function

and

$$k_{1,2} = \sqrt{\frac{A \pm \sqrt{A^2 - 4B^2}}{2}}, \quad k_3 = a - c^2/(b+1), \tag{A8}$$

where $A = a^2 + b^2 - 2c^2$ and $B = ab - c^2$.

APPENDIX B: BAYESIAN INFERENCE ALGORITHM

In this section, we focus on the implementation steps of the Bayesian inference algorithm [49,51,64]. The main idea is described and shown in Algorithm 1 and Algorithm 2.

[1] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photon. **13**, 839 (2019).

[2] D. Huang, P. Huang, D. K. Lin, and G. H. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[3] C. Weedbrook, S. Pirandola, R. Garcá-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[4] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, High performance reconciliation for continuous-variable quantum key distribution with LDPC code, Int. J. Quantum Inf. **13**, 1550010 (2015).

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck *et al.*, Advances in quantum cryptography, arXiv:1906.01645v1 (2019).

[6] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, Phys. Rev. Lett. **114**, 070501 (2015).

[7] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).

[8] L. Ruppert, V. C. Usenko, and R. Filip, Long-distance continuous-variable quantum key distribution with efficient channel estimation, Phys. Rev. A **90**, 062310 (2014).

[9] O. Thearle, S. M. Assad, and T. Symul, Estimation of output-channel noise for continuous-variable quantum key distribution, Phys. Rev. A **93**, 042343 (2016).

[10] X. Wang, Y. Zhang, S. Yu, and H. Guo, High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code, Sci. Rep. **8**, 10543 (2018).

[11] Z. Qu and I. B. Djordjevic, High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing, Opt. Express **25**, 7919 (2017).

[12] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, Opt. Lett. **40**, 3695 (2015).

[13] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, and G. Zeng, Continuous-variable quantum key distribution with 1 Mbps secure key rate, Opt. Express **23**, 17511 (2015).

[14] R. Filip, Continuous-variable quantum key distribution with noisy coherent states, Phys. Rev. A **77**, 022310 (2008).

[15] V. C. Usenko and R. Filip, Feasibility of continuous variable quantum key distribution with noisy coherent states, Phys. Rev. A **81**, 022318 (2010).

[16] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Quantum Cryptography Approaching the Classical Limit, Phys. Rev. Lett. **105**, 110501 (2010).

[17] C. Weedbrook, S. Pirandola, and T. C. Ralph, Continuous-variable quantum key distribution using thermal states, Phys. Rev. A **86**, 022318 (2012).

[18] V. C. Usenko and F. Grosshans, Unidimensional continuous-variable quantum key distribution, Phys. Rev. A **92**, 062337 (2015).

[19] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Single-quadrature continuous-variable quantum key distribution, Quantum Inf. Comput. **16**, 1081 (2016).

[20] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous variable quantum cryptography using two-way quantum communication, Nat. Phys. **4**, 726 (2008).

[21] K. Lemr, K. Bartkiewicz, A. Cernoch, and J. Soubusta, Resource-efficient linear-optical quantum router, Phys. Rev. A **87**, 062333 (2013).

[22] S. Wang, W. Chen, Z. Q. Yin, Y. Zhang, and Z. F. Han, Field test of wavelength-saving quantum key distribution network, Opt. Lett. **35**, 2454 (2010).

[23] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).

[24] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alleaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Field test of classical symmetric encryption with continuous variable quantum key distribution, Opt. Express **20**, 14030 (2012).

[25] F. Karinou, Toward the integration of CV quantum key distribution in deployed optical networks, IEEE Photon. Tech. Lett. **30**, 1041 (2018).

[26] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, and Z. Wang, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[27] X. Wang, Y. Zhang, S. Li, B. Xu, S. Yu, and H. Guo, Efficient rate-adaptive reconciliation for continuous variable quantum key distribution, Quantum Inf. Comput. **17**, 1123 (2017).

[28] M. Milicevic, C. Feng, M. Lei, and P. Glenn Gulak, Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography, npj Quantum Inf. **4**, 21 (2017).

[29] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[30] H. K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[31] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. L. Lloyd, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photon. **9**, 397 (2015).

[32] H. L. Yin, W. Zhu, and Y. Fu, Phase self-aligned continuous-variable measurement-device-independent quantum key distribution, Sci. Rep. **9**, 49 (2019).

[33] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution, Entropy **17**, 4547 (2015).

[34] Y. C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution using squeezed states, Phys. Rev. A **90**, 052325 (2014).

[35] A. Leverrier and P. Grangier, Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, Phys. Rev. A **83**, 042312 (2011).

[36] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit, Phys. Rev. Lett. **89**, 167901 (2002).

[37] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation, Phys. Rev. X **9**, 021059 (2019).

[38] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, Continuous-variable quantum key distribution protocols with eight-state discrete modulation, Int. J. Quantum Inf. **10**, 1250004 (2012).

[39] X. C. Ma, S. H. Sun, M. S. Jiang, M. Gui, L. M. Liang, Gaussian-modulated coherent-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 042335 (2014).

[40] J. Lin, H. Y. Tseng, and T. Hwang, Intercept-resend attacks on Chen 's quantum private comparison protocol and the improvements, Opt. Commun. **284**, 2412 (2011).

[41] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous variable quantum key distribution, Phys. Rev. A **87**, 062313 (2013).

[42] J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking on continuous-variable quantum key distribution system using a wavelength attack, Phys. Rev. A **87**, 062329 (2013).

[43] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Wavelength attack on practical continuous-variable quantum key distribution system with a heterodyne protocol, Phys. Rev. A **87**, 052309 (2013).

[44] C. Xie, Y. Guo, Q. Liao, W. Zhao, D. Huang, L. Zhang, and G. Zeng, Practical security analysis of continuous variable quantum key distribution with jitter in clock synchronization, Phys. Lett. A **382**, 811 (2018).

[45] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, Polarization attack on continuous-variable quantum key distribution, J. Phys. B: At., Mol., Opt. Phys. **52**, 015501 (2019).

[46] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection, Phys. Rev. X **5**, 041009 (2015).

[47] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-Referenced Continuous-Variable Quantum Key Distribution Protocol, Phys. Rev. X **5**, 041010 (2015).

[48] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, Reference pulse attack on continuous-variable quantum key distribution with local local oscillator under trusted phase noise, J. Opt. Soc. Am. B **36**, B7 (2019).

[49] N. Wiebe and C. Granade, Efficient Bayesian Phase Estimation, Phys. Rev. Lett. **117**, 010503 (2016).

[50] F. Daneshgaran, M. T. Delgado, and M. Mondin, Improved key rates for quantum key distribution employing soft metrics using Bayesian inference with photon counting detectors, Quantum Commun. Quantum Imag. IX **8163**, 113 (2011).

[51] S. Paesani, A. A. Gentile, R. Santagati, J. Wang, N. Wiebe, D. Tew, and M. G. Thompson, Experimental Bayesian Quantum Phase Estimation on a Silicon Photonic Chip, Phys. Rev. Lett. **118**, 100503 (2017).

[52] A. Leverrier and P. Grangier, Long distance quantum key distribution with continuous variables, *Conference on Quantum Computation, Communication, and Cryptography* (Springer, Berlin, Heidelberg, 2011).

[53] Z. Li, Y. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052301 (2014).

[54] J. Yang, B. Xu, X. Peng, and H. Guo, Four-state continuous-variable quantum key distribution with long secure distance, Phys. Rev. A **85**, 052302 (2012).

[55] P. Huang, J. Fang, and G. Zeng, State-discrimination attack on discretely modulated continuous-variable quantum key distribution, Phys. Rev. A **89**, 042330 (2014).

[56] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z. Zhang, and G. He, Continuous-variable measurement-device-independent multipartite quantum communication, Phys. Rev. A **93**, 022325 (2016).

[57] H. Ma, P. Huang, T. Wang, D. Bai, S. Wang, W. Bao, and G. Zeng, Security bound of continuous-variable measurement-device-independent quantum key distribution with imperfect phase reference calibration, Phys. Rev. A **100**, 052330 (2019).

[58] H. X. Ma, P. Huang, D. Y. Bai, T. Wang, S. Y. Wang, and W. S. Bao, Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation, Phys. Rev. A **99**, 022322 (2018).

[59] B. Huang, Y. Huang, and Z. Peng, Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack, Opt. Express **27**, 20621 (2019).

[60] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[61] A. Leverrier and P. Grangier, Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, Phys. Rev. Lett. **102**, 180504 (2009).

[62] M. Heid and N. Lütkenhaus, Security of coherent-state quantum cryptography in the presence of Gaussian noise, Phys. Rev. A **76**, 022313 (2007).

[63] D. Sych and G. Leuchs, Coherent state quantum key distribution with multiletter phase-shift keying, New J. Phys. **12**, 053019 (2010).

[64] N. Wiebe, C. Granade, C. Ferrie, and D. G. Cory, Phys. Rev. Lett. **112**, 190501 (2014).