Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source

Qin Liao,[1,2,*] Gang Xiao,[1] Chu-Gui Xu,[1] Yang Xu,[1] and Ying Guo[2,†]

[1] *College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*

[2] *Institute of Advanced Photoelectric Detection and Quantum System, Central South University, Changsha 410075, China*

(Received 17 April 2020; revised 22 June 2020; accepted 5 August 2020; published 8 September 2020)

The discretely modulated continuous-variable quantum key distribution (DM CVQKD) has been proven to be secure, and a basic assumption for the current theoretical security proof of the DM CVQKD is that the signal source cannot be compromised. However, this assumption is quite unpractical in real quantum communication systems. In this paper, we investigate the DM CVQKD with a special configuration in which the entanglement source is placed at the untrusted channel. With this configuration, the source is no longer protected by the sender but is exposed to the vulnerable environment. In particular, we consider the configuration for two typical DM CVQKD protocols, which are the four-state protocol and the eight-state protocol. Security analysis based on linear bosonic channel shows that the DM CVQKD with an untrusted entanglement source is able to defend itself against the most powerful quantum collective attack in a certain distance range and it can still generate positive secret key rate when considering finite-size effect and composable security, thereby providing a theoretical proof for applying the DM CVQKD system to a realistic environment.

DOI: 10.1103/PhysRevA.102.032604

I. INTRODUCTION

Continuous-variable quantum key distribution (CVQKD) [1,2] provides an approach to allows two distant legitimate partners, Alice and Bob, to share a random secure key over insecure quantum and classical channels. One of the advantage of the CVQKD protocol is that the most state-of-art telecommunication technologies can be compatible with CVQKD protocols, so that one may apply a CVQKD system to the practical communication network in use.

In general, there are two modulation approaches in the CVQKD protocol, i.e., the Gaussian-modulated CVQKD protocol (GM CVQKD) [3,4] and the discretely modulated CVQKD protocol (DM CVQKD) [5,6]. For the first approach, Alice usually encodes key bits in the quadratures ($\hat{p}$ and $\hat{q}$) of the optical field [7], while Bob can restore the secret key bits through high-speed and high-efficiency coherent detection techniques. This strategy usually has a repetition rate higher than that of single-photon detections so that GM CVQKD could potentially achieve higher secret key rates. After solving the theoretical security issues of GM CVQKD [8,9], its experimental implementation has been widely studied; see, e.g., Refs. [10–13]. However, it still seems unfortunately limited to much shorter distance due to the problem of quite low reconciliation efficiency in long-distance transmission. For the second approach, the DM CVQKD generates several nonorthogonal coherent states and exploits the sign of the measured quadrature of each state to encode information rather than using the quadrature $\hat{p}$ or $\hat{q}$ itself [14]. This discrete modulation strategy is more suitable for long-distance transmission since the sign of the measured quadrature is already discrete, thereby validating most excellent error-correcting codes even at low signal-to-noise ratio (SNR) [15]. Therefore, the DM CVQKD is becoming a hotspot in the long-distance quantum communication field due to its strong compatibility with current telecommunication technologies. However, because the idea of the DM CVQKD was proposed later than that of GM CVQKD, current research regarding the DM CVQKD mainly focuses on its theoretical protocol and proof of security.

DM CVQKD has been proven to be secure in a linear quantum channel against collective attacks [16] and, very recently, its asymptotic security against arbitrary collective attacks has also been proven [17,18]. However, there exists a basic assumption for these theoretical proofs of security; namely, the signal source cannot be compromised. That is to say, the source is perfectly protected by the legitimate sender Alice. Apparently, this assumption is quite unpractical in real quantum communication systems. Legitimate users may also be compromised in a realistic environment, let alone the source. Although this issue can be theoretically fixed by applying plug-and-play measurement-device-independent (PP MDI) configuration in which both measurement device and signal source are integrated with the third untrusted part Charlie [19], the PP MDI-based DM CVQKD actually does not work well in realistic communication system. This is because the most widely used amplitude modulators, e.g., LiNbO$_3$ modulators, are polarization sensitive and feature a polarizer, where the light can hardly be transmitted if its orientation is not perfectly aligned in PP configuration.

To solve this problem, we thoroughly investigate a special configuration for the DM CVQKD in which entanglement

[*] llqqlq@hnu.edu.cn

[†] yingguo@csu.edu.cn

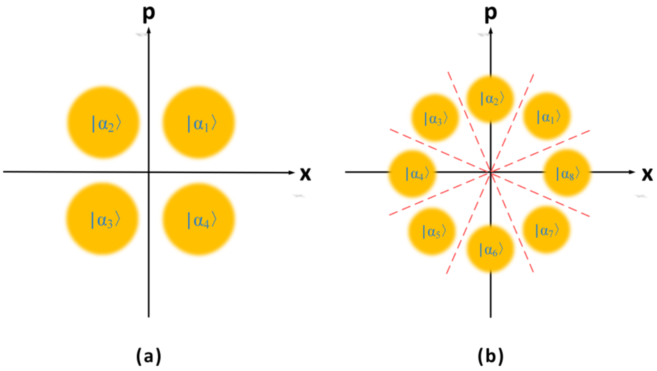

FIG. 1. Phase-space presentation of coherent state in the (a) four-state protocol and (b) eight-state protocol.

source is placed at the untrusted quantum channel. By simply moving the source out of sender's protection, we discover that the DM CVQKD with an untrusted entanglement source is able to defend itself against the most powerful quantum collective attacks in a certain distance range. More specifically, we consider the configuration for two typical DM CVQKD protocols, which are four-state protocol and eight-state protocol, respectively, and compare their performance with different coherent detection technologies, i.e., heterodyne detection and homodyne detection. Numeric simulation based on linear bosonic channels shows that the performance is well acceptable by putting the untrusted entanglement source close to one of the legitimate parties, Alice or Bob. Moreover, by further taking finite-size effects and composable security into account, the DM CVQKD with an untrusted entanglement source can still generate a positive secret key rate. As a result, this work waives the necessity of the assumptions of a secure signal source and an infinite length of the secret key, thereby providing a theoretical proof for applying a DM CVQKD system in a realistic environment.

This paper is structured as follows: In Sec. II, we briefly introduce the two typical DM CVQKD protocols, namely, the four-state protocol and the eight-state protocol. In Sec. III, we detail the proposed configuration of the DM CVQKD with an untrusted entanglement source. Performance analysis and discussion are presented in Sec. IV and final conclusions are drawn in Sec. V.

II. DISCRETELY MODULATED CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION PROTOCOLS

To make the derivation self-contained, in this section, we first introduce two typical discretely modulated CVQKD protocols, i.e., the four-state protocol and the eight-state protocol, both of which can be generalized to the one with N coherent states $|\alpha_k^N\rangle = |\alpha e^{i2k\pi/N}\rangle$, where $k \in \{1, 2, \dots, N\}$ and α is a positive number related to the modulation variance of coherent state as $V_M = 2\alpha^2$ [6]. Figure 1 depicts the phase-space presentation of the coherent state in these two protocols.

Let us first consider the prepare-and-measurement (PM) version of the discretely modulated CVQKD protocol. Alice randomly chooses one of the coherent states $|\alpha_k^N\rangle$ and sends it to the remote Bob through a lossy and noisy quantum channel, which is characterized by a transmission efficiency T and an excess noise ε. When Bob receives the modulated coherent states, he can apply either homodyne or heterodyne detector with detection efficiency μ and electronics noise v_{el} to measure arbitrary one of the two quadratures $\hat{x}$ or $\hat{p}$ (or both quadratures). The mixture state that Bob received can be expressed with the following form

$$\rho_N = \frac{1}{N}\sum_{k=1}^{N} |\alpha_k^N\rangle\langle\alpha_k^N|. \tag{1}$$

After the measurement, Bob reveals some values publicly through a classical authenticated channel (see Ref. [18] for further details about these values). This information allows Alice and Bob to turn the information-reconciliation problem into a well-studied channel-coding problem for the binary-input additive white-noise Gaussian channel. The rest steps of the protocol are standard, namely, parameter estimation, reconciliation, and privacy amplification. Finally, Alice and Bob can establish a correlated sequence of random secure key.

The PM version of the DM CVQKD protocol is equivalent to the entanglement-based (EB) version, which is more convenient for security analysis [17,20,21]. In what follows, we present the specific four-state protocol and eight-state protocol with the respective EB version.

A. Four-state protocol

Alice prepares a pure state $|\Psi_4\rangle$ which is defined as

$$\begin{aligned}|\Psi_4\rangle &= \sum_{k=0}^{3}\sqrt{\lambda_k}|\phi_k^4\rangle|\phi_k^4\rangle\\ &= \frac{1}{2}\sum_{k=0}^{3}|\psi_k^4\rangle|\alpha_k^4\rangle,\end{aligned} \tag{2}$$

where the states

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

are the non-Gaussian states, and the state $|\phi_m^4\rangle$ is given by

$$|\phi_k^4\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}|4n+k\rangle, \tag{4}$$

with

$$\lambda_{0,2} = \tfrac{1}{2}e^{-\alpha^2}[\cosh(\alpha^2) \pm \cos(\alpha^2)], \tag{5}$$

$$\lambda_{1,3} = \tfrac{1}{2}e^{-\alpha^2}[\sinh(\alpha^2) \pm \sin(\alpha^2)], \tag{6}$$

Consequently, the mixture state ρ_4 can be expressed by

$$\begin{aligned}\rho_4 &= \mathrm{Tr}(|\Psi_4\rangle\langle\Psi_4|)\\ &= \sum_{k=0}^{3}\lambda_k|\phi_k^4\rangle\langle\phi_k^4|.\end{aligned} \tag{7}$$

Let A and B respectively denote the two output modes of the bipartite state $|\Psi_4\rangle$, $\hat{a}$ and $\hat{b}$ denote the annihilation operators applying to mode A and B respectively. We have the covariance matrix Γ_{AB}^4 of the bipartite state $|\Psi_4\rangle$ with the following form

$$\Gamma_{AB}^{4} = \begin{pmatrix} X\mathbb{I} & Z_4\sigma_z \\ Z_4\sigma_z & Y\mathbb{I} \end{pmatrix}, \tag{8}$$

where $\mathbb{I}$ and σ_z represent diag(1, 1) and diag(1, −1) respectively, and

$$\begin{aligned} X &= \langle\Psi_4|1+2a^\dagger a|\Psi_4\rangle = 1+2\alpha^2, \\ Y &= \langle\Psi_4|1+2b^\dagger b|\Psi_4\rangle = 1+2\alpha^2, \\ Z_4 &= \langle\Psi_4|ab+a^\dagger b^\dagger|\Psi_4\rangle = 2\alpha^2\sum_{k=0}^{3}\lambda_{k-1}^{3/2}\lambda_k^{-1/2}. \end{aligned} \tag{9}$$

Note that the addition arithmetic should be operated with modulo four.

After preparing the bipartite state $|\Psi_4\rangle$ with variance $V = 1+V_M$, Alice performs projective measurements $|\psi_k\rangle\langle\psi_k|$ $(k = 0, 1, 2, 3)$ on mode A, which projects another mode B onto a coherent state $|\alpha_k^4\rangle$. Alice subsequently sends mode B to Bob through the quantum channel. Bob then applies homodyne (or heterodyne) detection to measure the incoming mode B. Finally, the two trusted parties Alice and Bob extract a string of secret keys by using error correction and privacy amplification.

B. Eight-state protocol

Similarly, Alice prepares a pure state $|\Psi_8\rangle$ which is defined as

$$|\Psi_8\rangle = \frac{1}{4}\sum_{k=0}^{7}|\psi_k^8\rangle|\alpha_k^8\rangle, \tag{10}$$

where the states

$$|\psi_k^8\rangle = \frac{1}{2}\sum_{m=0}^{7}e^{i(1+4k)m\pi/4}|\phi_m^8\rangle \tag{11}$$

are orthogonal non-Gaussian states. The state $|\phi_m^8\rangle$ could be described as follows:

$$|\phi_k^8\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}e^{\frac{\alpha^{(8n+k)}}{\sqrt{(8n+k)!}}}|8n+k\rangle, \tag{12}$$

with

$$\lambda_{0,4} = \frac{1}{4}e^{-\alpha^2}\left[\cosh(\alpha^2)+\cos(\alpha^2)\pm 2\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right], \tag{13}$$

$$\lambda_{1,5} = \frac{1}{4}e^{-\alpha^2}\left[\sinh(\alpha^2)+\sin(\alpha^2)\pm\sqrt{2}\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right]\pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\Bigg], \tag{14}$$

$$\lambda_{2,6} = \frac{1}{4}e^{-\alpha^2}\left[\cosh(\alpha^2)-\cos(\alpha^2)\pm 2\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right], \tag{15}$$

$$\lambda_{3,7} = \frac{1}{4}e^{-\alpha^2}\left[\sinh(\alpha^2)-\sin(\alpha^2)\mp\sqrt{2}\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right]\pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\Bigg]. \tag{16}$$

The covariance matrix Γ_{AB}^{8} has the form

$$\Gamma_{AB}^{8} = \begin{pmatrix} X\mathbb{I} & Z_8\sigma_z \\ Z_8\sigma_z & Y\mathbb{I} \end{pmatrix}, \tag{17}$$

where

$$\begin{aligned} X &= \langle\Psi_8|1+2a^\dagger a|\Psi_8\rangle = 1+2\alpha^2, \\ Y &= \langle\Psi_8|1+2b^\dagger b|\Psi_8\rangle = 1+2\alpha^2, \\ Z_8 &= \langle\Psi_8|ab+a^\dagger b^\dagger|\Psi_8\rangle = 2\alpha^2\sum_{k=0}^{7}\lambda_{k-1}{}^{3/2}\lambda_k{}^{-1/2}. \end{aligned} \tag{18}$$

Here the addition arithmetic should be operated with modulo eight, and the remaining steps are the same as for the four-state protocol.

The detailed derivation of the four-state protocol and eight-state protocol can be found in Ref. [22].

III. DISCRETELY MODULATED CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION WITH UNTRUSTED ENTANGLEMENT SOURCE

In this section, we first detail the DM CVQKD scheme in which the entanglement source is placed at the untrusted quantum channel, and then derive the calculation of its asymptotic secret key rate.

A. Scheme

Figure 2 (top) shows the EB version of the original DM CVQKD protocol in which bipartite state $|\Psi\rangle$ is perfectly protected by Alice, whose security is trusty. However, from an

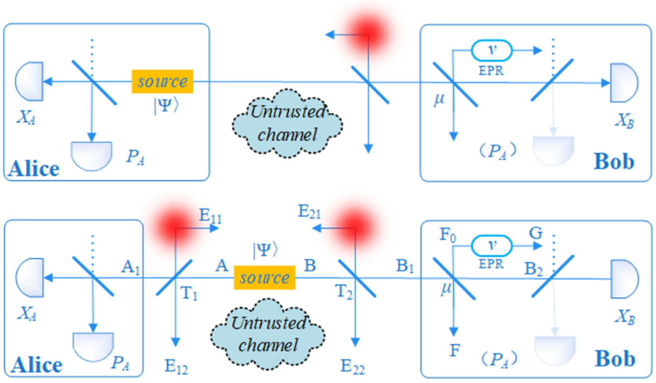

FIG. 2. (top) Original DM CVQKD protocol. (bottom) DM CVQKD with entanglement source in the untrusted channel.

eavesdropping point of view, it is necessary to assume that Eve could have controlled the entangled source. As shown in Fig. 2 (bottom), the source is moved out of the sender's protection, so that Eve may replace the quantum channel between Alice and Bob with her own quantum channel. Two separate beam splitters with transmittances T_1 and T_2 are used for simulating the losses caused by the replaced channels. Note that the scheme will return to the original DM CVQKD with a trusted source when $T_1 = 1$. Bob's detector inefficiency is modeled by a beam splitter with transmission μ, while its electronic noise υ_{el} is modeled by an EPR state of variance υ, one half of which is entering the second input port of the beam splitter.

Assuming Eve launches quantum collective attack strategy, which has been proven to be the most powerful attack under both direct and reverse reconciliation [7]. Eve prepares her ancillary system in a product state for both quantum links, and the ancilla mode of each link interacts individually with a single pulse sent to Alice and Bob, respectively. The combined state reads

$$\rho_{AE_1BE_2} = \sum_{a,b} \left[P(a)|a\rangle\langle a| \otimes \psi^{a}_{AE_1} \oplus P(b)|b\rangle\langle b| \otimes \psi^{b}_{BE_2}\right]^{\otimes n}. \tag{19}$$

Then Eve exploits the so-called *entangling cloner* [7,23] to perform a collective attack. In particular, Eve replaces the channels with transmittance T_i $(i = 1, 2)$ and excess noise referred to the input χ_{line_i} by preparing the ancilla $|E_i\rangle$ of variance W_i and a beam splitter of transmittance T_i. The value W_i can be tuned to match the noise of the real channel $\chi_{\text{line}_i} = 1/T_i - 1 + \varepsilon$. Note that for a special case which entangled source is located in the middle of channel, the two related beam-splitter attacks are symmetric, i.e., $T_1 = T_2$, and the total transmittance $T = T_1T_2$. After that, Eve keeps one mode E_{i1} of $|E_i\rangle$ and injects the other mode into the unused port of each beam splitter respectively and thus acquires the output mode E_{i2}. After repeating this process for each pulse, Eve stores her ancilla modes, E_{i1} and E_{i2}, in quantum memories. Finally, Eve measures the exact quadrature on E_{i1} and E_{i2} after Alice and Bob reveal the classical communication information. The measurement of E_{i1} will allow her to decrease the noise added by E_{i2}.

B. Calculation

In what follows, we derive the expressions of asymptotic secret key rate for the DM CVQKD with an untrusted entanglement source. Without loss of generality, we here mainly consider the situation where reverse reconciliation in use.

In general, the asymptotic secret key rate of the DM CVQKD under collective attack can be given by

$$K = \beta I(A_1 : B_2) - S(B_2 : E), \tag{20}$$

where β is reverse reconciliation efficiency, and $I(A_1 : B_2)$ is the Shannon mutual information between Alice and Bob, which can be straightforwardly derived as [24]

$$I(A_1 : B_2) = \begin{cases} \log_2 \frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}, & \text{for heterodyne detection} \\ \frac{1}{2}\log_2 \frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}, & \text{for homodyne detection,} \end{cases} \tag{21}$$

where $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_h/T$ is the total noise referred to the channel input $\chi_{\text{line}} = 1/T - 1 + \varepsilon$ and detection input $\chi_h := \chi_{\text{het}} = (2 - \mu + 2\upsilon_{el})/\mu$ for heterodyne detection or $\chi_h := \chi_{\text{hom}} = (1 - \mu + \upsilon_{el})/\mu$ for homodyne detection. Term $S(B_2 : E)$ denotes the maximum information available to Eve on Bob's measurement, it is bounded by Holevo quantity [25]

$$S(B_2 : E) = S(\rho_E) - \int \mathrm{d}m_B P(m_B) S\left(\rho_E^{m_B}\right), \tag{22}$$

where m_B denotes Bob's measurement result, it can be expressed as $m_B = x_B, p_B$ for heterodyne detection or $m_B = x_B$ for homodyne detection. $P(m_B)$ is the probability density of the measurement, $\rho_E^{m_B}$ is the eavesdropper's state conditional on Bob's measurement result, and S is the von Neumann entropy of the quantum state ρ.

Due to the fact that Eve's system purifies the system A_1B_1 and Bob's measurement purifies the system A_1EFG, Eq. (22) can be further expressed as

$$\begin{aligned} S(B_2 : E) &= S(\rho_{A_1B_1}) - S\left(\rho^{m_B}_{A_1FG}\right) \\ &= \sum_{j=1}^{2} G\left(\frac{\lambda_j - 1}{2}\right) - \sum_{j=3}^{5} G\left(\frac{\lambda_j - 1}{2}\right), \end{aligned} \tag{23}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ is the von Neumann entropy and λ_1, λ_2 are symplectic eigenvalues of the covariance matrix $\Gamma_{A_1B_1}$ characterizing the state $\rho_{A_1B_1}$, and λ_3, λ_4, λ_5 are symplectic eigenvalues of the covariance matrix $\Gamma^{m_B}_{A_1FG}$ characterizing the state $\rho^{m_B}_{A_1FG}$ after Bob's coherent measurement.

The first covariance matrix $\Gamma_{A_1B_1}$ depends on the system after mode A and B passed respective quantum channel, so that the first part of Eq. (23) can be given by

$$\Gamma_{A_1B_1} = \begin{pmatrix} a\mathbb{I} & c\sigma_z \\ c\sigma_z & b\mathbb{I} \end{pmatrix}, \tag{24}$$

where $a = T_1V + (1 - T_1)W_1$, $b = T_2V + (1 - T_2)W_2$, and $c = [T_1T_2(V^2 - 1)]^{1/2}$. Therefore, the symplectic eigenvalues λ_1, λ_2 of the above matrix can be calculated by

$$\lambda^2_{1,2} = \tfrac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4C}], \tag{25}$$

with

$$\Delta = a^2 + b^2 - 2c^2 \tag{26}$$

and

$$C = (ab - c^2)^2. \tag{27}$$

The second covariance matrix $\Gamma^{m_B}_{A_1FG}$ can be written as

$$\Gamma^{m_B}_{A_1FG} = \Gamma_{A_1FG} - \sigma^{\mathrm{T}}_{A_1FGB_2}\Pi\sigma_{A_1FGB_2}, \tag{28}$$

where $\Pi = (\Gamma_{B_2} + \mathbb{I})^{-1}$ for heterodyne detection and $\Pi = (X\Gamma_{B_2}X)^{\text{MP}}$ for homodyne detection, with

$$X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

and MP presents the Moore-Penrose pseudoinverse of a matrix. The matrices Γ_{A_1FG}, Γ_{B_2}, and $\sigma_{A_1FGB_2}$ can all be derived from the decomposition of the covariance matrix $\Gamma_{A_1FGB_2}$, which can be derived with appropriate rearrangement of lines and columns from the matrix describing the quantum system $\rho_{A_1B_2FG}$, we have

$$\Gamma_{A_1B_2FG} = (Y^{BS})^{\mathrm{T}}[\Gamma_{A_1B_1} \oplus \Gamma_{F_0G}]Y^{BS}, \tag{29}$$

where Γ_{F_0G} is the matrix that describes the EPR state with variance v used to model the detector's electronic noise. It can be written as

$$\Gamma_{F_0G} = \begin{pmatrix} v\mathbb{I} & \sqrt{v^2-1}\sigma_z \\ \sqrt{v^2-1}\sigma_z & v\mathbb{I} \end{pmatrix}, \tag{30}$$

where v takes the proper value for coherent detection. The matrix Y^{BS} describes the beam splitter transformation that models the inefficiency of the detector and acts on modes B_1 and F_0. It can be expressed by

$$Y^{BS} = \mathbb{I}_{A_1} \oplus \begin{pmatrix} \sqrt{\mu}\mathbb{I} & \sqrt{1-\mu}\mathbb{I} \\ -\sqrt{1-\mu}\mathbb{I} & \sqrt{\mu}\mathbb{I} \end{pmatrix} \oplus \mathbb{I}_G. \tag{31}$$

Now, we have all the elements required to proceed to the calculation of the symplectic eigenvalues $\lambda_3, \lambda_4, \lambda_5$ which are given by the following form:

$$\lambda_{3,4}^2 = \tfrac{1}{2}[O \pm \sqrt{O^2 - 4D}],$$
$$\lambda_5 = 1, \tag{32}$$

where for heterodyne detection,

$$O_{\mathrm{het}} = \frac{1}{T^2(V+\chi_{\mathrm{tot}})^2}\big[\Delta\chi_{\mathrm{het}}^2 + C + 1 + 2\chi_{\mathrm{het}}(V\sqrt{C} + T(V+\chi_{\mathrm{line}}) + 2TZ^2)\big], \tag{33}$$

$$D_{\mathrm{het}} = \left(\frac{V + \sqrt{C}\chi_{\mathrm{het}}}{T(V+\chi_{\mathrm{tot}})}\right)^2, \tag{34}$$

and for homodyne detection,

$$O_{\mathrm{hom}} = \frac{\Delta\chi_{\mathrm{hom}} + V\sqrt{C} + T(V+\chi_{\mathrm{line}})}{T(V+\chi_{\mathrm{tot}})}, \tag{35}$$

$$D_{\mathrm{hom}} = \sqrt{C}\frac{V + \sqrt{C}\chi_{\mathrm{hom}}}{T(V+\chi_{\mathrm{tot}})}. \tag{36}$$

Finally, we can calculate the Holevo information bound $S(B_2 : E)$ and thereby derive the asymptotic secret key rate K of the DM CVQKD with an untrusted entanglement source.

IV. PERFORMANCE ANALYSIS AND DISCUSSION

For comparison, we first present the performance of the original DM CVQKD protocols depicted in Fig. 2 (top), whose calculation can be found in Ref. [15]. Figure 3 shows the asymptotic secret key rates of four-state protocol and eight-state protocol as functions of transmission distance. Although the eight-state protocol outperforms the four-state protocol in terms of maximal transmission distance, both protocols achieve more than 150 km. In particular, the performance of the protocols with fixed V_m ($V_m = 0.3$ for the four-state protocol and $V_m = 0.35$ for the eight-state protocol) is very similar to the performance of the protocols with optimized V_m, which is quite different from the Gaussian-modulated CVQKD protocol [26]. Therefore, we can use these fixed values to perform the following numeric experiments:

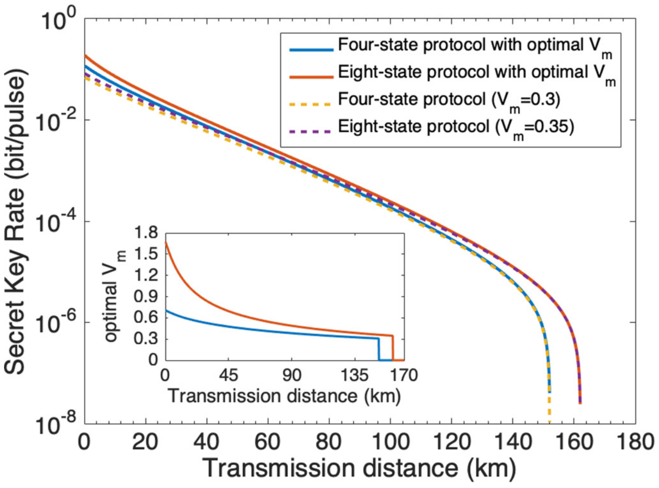

FIG. 3. Performance of original DM CVQKD protocols. The upper solid line (red) denotes the four-state protocol with optimal modulation variance and the lower solid line (blue) denotes the eight-state protocol with optimal modulation variance. The upper dashed line (purple) denotes the four-state protocol with fixed $V_m = 0.3$ and the lower dashed line (yellow) denotes the eight-state protocol with fixed $V_m = 0.35$. Inset shows the optimal modulation variance as a function of transmission distance. The parameters of this paper are set to $\mu = 0.6$, $v_{el} = 0.05$, reconciliation efficiency $\beta = 0.98$, and excess noise $\varepsilon = 0.01$.

Heterodyne-detection case. Figure 4 shows the performance of the DM CVQKD with an untrusted entanglement source using heterodyne detection. We find that both four-state protocol and eight-state protocol can still generate positive secret key rate in certain distance range between Alice and the untrusted source. However, their performance is remarkably reduced when compared with the original DM CVQKD protocol. In particular, the maximal transmission distance is immediately decreased to approximately 20 km for the four-state protocol and 25 km for the eight-state protocol, once the source is just moved out of the sender's protection (but very close to the sender, $L_{\mathrm{Alice}} \to 0$ km). As shown in Fig. 5, the definition of the notation $L_{\mathrm{Alice}} \to 0$ km is not equivalent to that of $L_{\mathrm{Alice}} = 0$ km. The former denotes that the source is placed at the port of Alice's side without protection so that we have $V_{A_1} = \lim a = V + \varepsilon$, while the latter denotes that the source is placed inside the sender, which returns to the original DM CVQKD protocol, so we have $V_{A_1} = V$. Since the security of the DM CVQKD under quantum collective attack can only be guaranteed by the small modulation variance shown in the inset of Fig. 3, the negative impact of excess noise on the DM CVQKD system is larger than that on the GM CVQKD system for short-distance transmission. On the other hand, as shown in Fig. 6, the Holevo information of the protocols with $L_{\mathrm{Alice}} \to 0$ km is more than that of the protocols with $L_{\mathrm{Alice}} = 0$ km (original DM CVQKD protocol), while their Shannon mutual information does not change regardless of $L_{\mathrm{Alice}} \to$

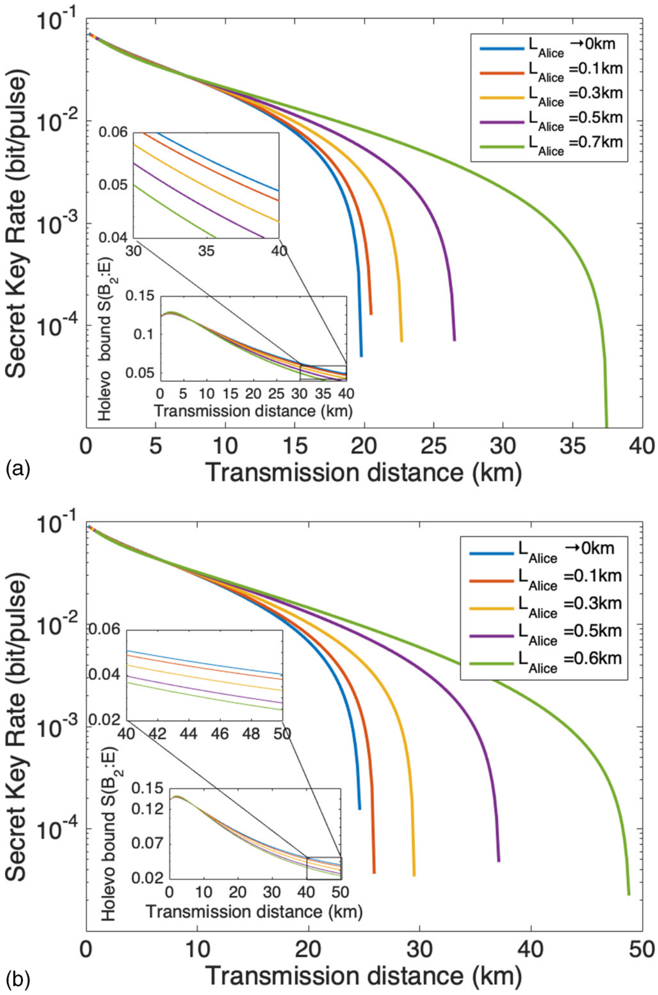

FIG. 4. Performance of (a) four-state protocol with untrusted entanglement source and (b) eight-state protocol with untrusted entanglement source using heterodyne detection. L_{Alice} is the distance between Alice and the signal source. From left to right (main figure) and from top to bottom (inset), the solid lines denote $L_{\text{Alice}} \to 0$ km, $L_{\text{Alice}} = 0.1$ km, $L_{\text{Alice}} = 0.3$ km, $L_{\text{Alice}} = 0.5$ km and (a) $L_{\text{Alice}} = 0.7$ km or (b) $L_{\text{Alice}} = 0.6$ km.

0 km or $L_{\text{Alice}} = 0$ km. This illustrates that the untrusted source can enhance the power of Eve's quantum collective attack. As a result, the performance is fast reduced when the untrusted source is very close to the sender. However, the maximal transmission distance can be increased as the source slowly moves far away from the sender. The reason is that the Holevo information $S(B_2 : E)$ decreases rapidly as the risen distance L_{Alice}, which is shown in the insets of Fig. 4.

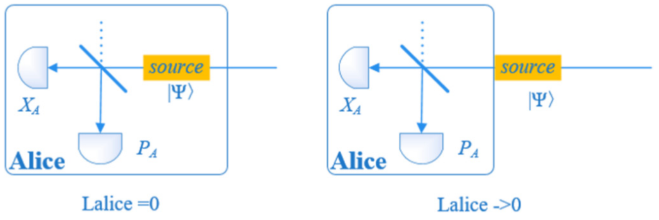

FIG. 5. Different definition of the notations $L_{\text{Alice}} = 0$ and $L_{\text{Alice}} \to 0$. (left) $L_{\text{Alice}} = 0$ denotes that the signal source is placed in the Alice side and cannot be compromised, so that the source is trusted. (right) $L_{\text{Alice}} \to 0$ denotes that the signal source is very close to Alice but not protected by the sender, so that the source is untrusted.

Homodyne-detection case. Figure 7 shows the performance of the DM CVQKD with an untrusted entanglement source using homodyne detection. Both the four-state protocol and the eight-state protocol can also generate a positive secret key rate, and their maximal transmission distances are even longer than those in heterodyne-detection case. For instance, the maximal transmission distance of the eight-state protocol with $L_{\text{Alice}} = 0.6$ km in the homodyne-detection case is nearly 70 km, while it is close to 50 km with heterodyne detection. The probable reason is that heterodyne detection is more noisy than homodyne detection in a realistic scenario ($\mu = 0.6$ and $v_{el} = 0.05$), this part of the noise can be counted on as a part of Eve's intercepted information, thereby resulting the obvious increase of Holevo bound, which is shown in Fig. 8. However, the change of Shannon mutual information between Alice and Bob is quite slight (shown in the inset of Fig. 8), therefore, the overall performance of the DM CVQKD with an untrusted entanglement source in the heterodyne-detection case is worse than that in the homodyne-detection case.

In addition, we also investigate another situation where the untrusted source is close to Bob's side. We find that the result has symmetrical characteristics. That is to say, the performance can be obtained in both the heterodyne-detection case and the homodyne-detection case by simply replacing the notation L_{Alice} with L_{Bob}.

It is worth noting that the above asymptotic performance of the DM CVQKD with an untrusted source is based on the technique developed in Ref. [16], which proved the asymptotic security of the DM CVQKD against collective attacks under a linear quantum channel. Very recently, the

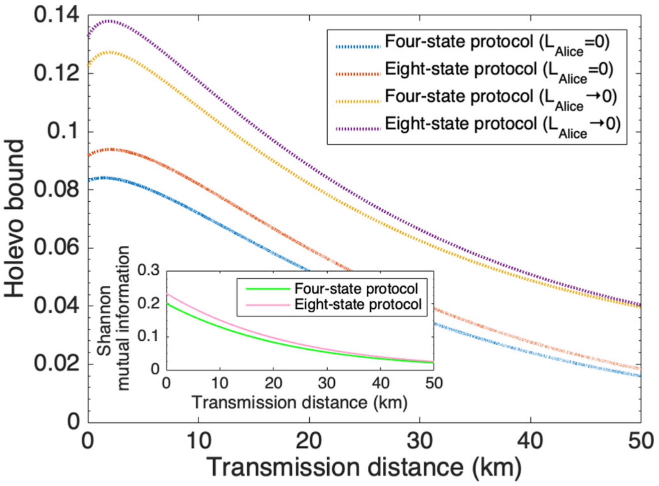

FIG. 6. Holevo bounds of DM CVQKD protocols as a function of transmission distance in different L_{Alice} (heterodyne detection). From top to bottom (main figure), the dotted lines denote the four-state protocol with $L_{\text{Alice}} = 0$, the eight-state protocol with $L_{\text{Alice}} = 0$, the four-state protocol with $L_{\text{Alice}} \to 0$, and the eight-state protocol with $L_{\text{Alice}} \to 0$, respectively. From top to bottom (inset), the solid lines denote the four-state protocol and the eight-state protocol.

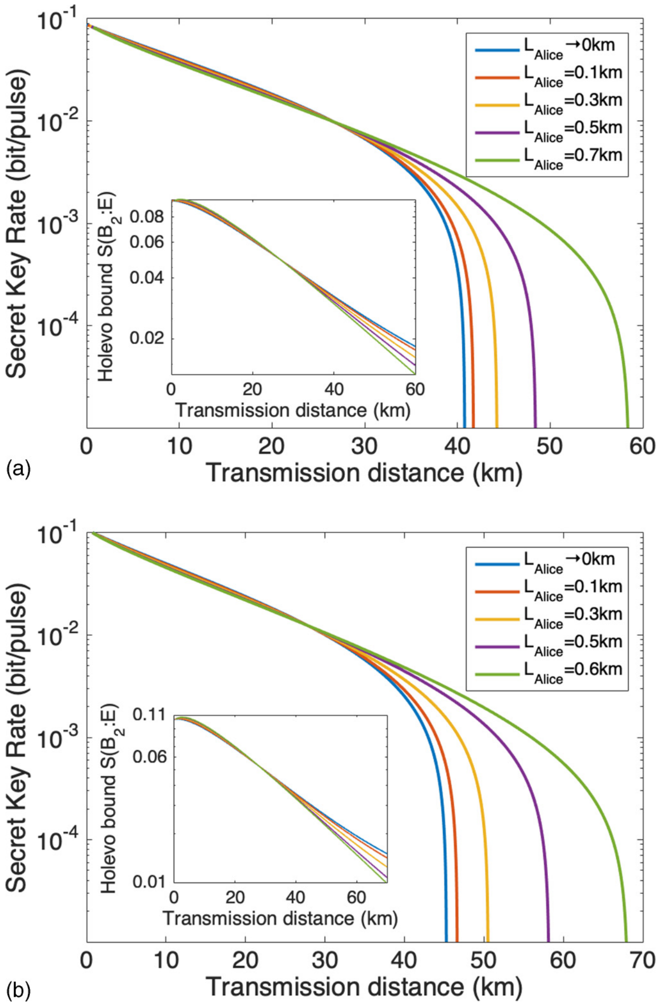

FIG. 7. Performance of (a) four-state protocol with untrusted entanglement source and (b) eight-state protocol with untrusted entanglement source using homodyne detection. From left to right (main figure) and from top to bottom (right side of the inset), the solid lines denote $L_{\text{Alice}} \to 0$ km, $L_{\text{Alice}} = 0.1$ km, $L_{\text{Alice}} = 0.3$ km, $L_{\text{Alice}} = 0.5$ km and (a) $L_{\text{Alice}} = 0.7$ km or (b) $L_{\text{Alice}} = 0.6$ km.

asymptotic security of the original DM CVQKD against arbitrary collective attacks has been proven [17,18], so that one can obtain a tighter asymptotic bound of the DM CVQKD with an untrusted source by removing the hidden linear-channel assumption.

Moreover, the above analysis considers the security of a protocol in the asymptotic regime of infinity many signals exchanged by Alice and Bob. However, the realistic security of all QKD implementations realized until now is in fact jeopardized due to the finite length of the data blocks exchanged by the legitimate users [8]. Therefore, it is necessary to consider the impact of finite-size effects on the DM CVQKD with an untrusted entanglement source. In the finite-size scenario, the secret key rate of Eq. (20) is modified as

$$K_{\text{fini}} = \frac{n}{N}[\beta I(A_1 : B_2) - S_{\epsilon_{PE}}(B_2 : E) - \Delta(n)], \qquad (37)$$

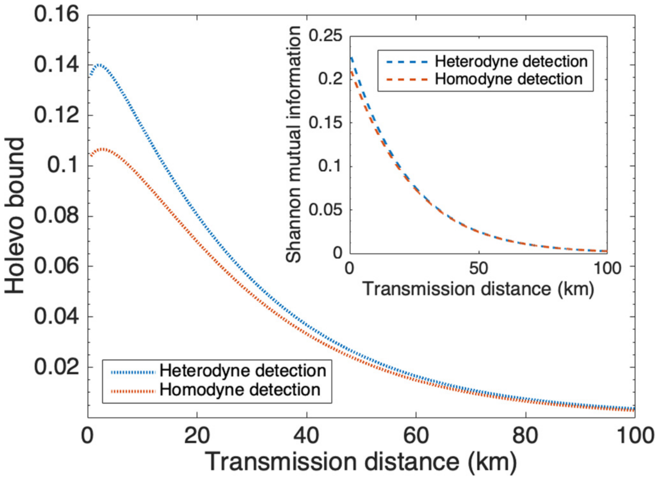

FIG. 8. Holevo bounds of eight-state protocol with $L_{\text{Alice}} = 0.6$ km as a function of transmission distance in different detection technologies. From top to bottom in both the main figure and the inset, the lines denote heterodyne detection and homodyne detection, respectively.

where N denotes the total number of the exchanged signals and n denotes the number of signals used for sharing the key between Alice and Bob. The remaining $N - n$ signals is used for parameter estimation with the failure probability ϵ_{PE}. The parameter $\Delta(n)$ is related to the security of the privacy amplification, which is given by

$$\Delta(n) = (2\dim\mathcal{H}_B + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{PA}), \qquad (38)$$

where $\bar{\epsilon}$ is a smoothing parameter, ϵ_{PA} is the failure probability of privacy amplification, and $\mathcal{H}_B$ is the Hilbert space corresponding to Bob's raw key. Since the raw key is usually encoded on binary bits, we have $\dim\mathcal{H}_B = 2$. We do not proceed a detailed derivation for the finite-size calculation here, since it can be found in our previous work [15]. As an example, Fig. 9 shows the performance of the eight-state protocol with $L_{\text{Alice}} = 0.6$ km using homodyne detection in the finite-size regime. Although the maximal transmission distance decreases as the reduction of the data-block length, it can still generate a positive secret key rate when the block length $N = 10^7$. A similar trend also occurred in other situations. Therefore, the DM CVQKD with an untrusted entanglement source is available for practical transmission with a finite secret key.

Finally, let us consider the performance of the DM CVQKD with an untrusted source in composable security framework. The composable security, which takes every step's failure probability of the CVQKD system into account, is the strictest theoretical security analysis of the CVQKD system so that one can obtain a more practical secure bound. Figure 10 depicts the composable secret key rate of the eight-state protocol with $L_{\text{Alice}} = 0.6$ km using homodyne detection as a function of total exchanged signals N (other situations have a similar trend); its calculation is presented in the Appendix. We find that the performance is more pessimistic than that

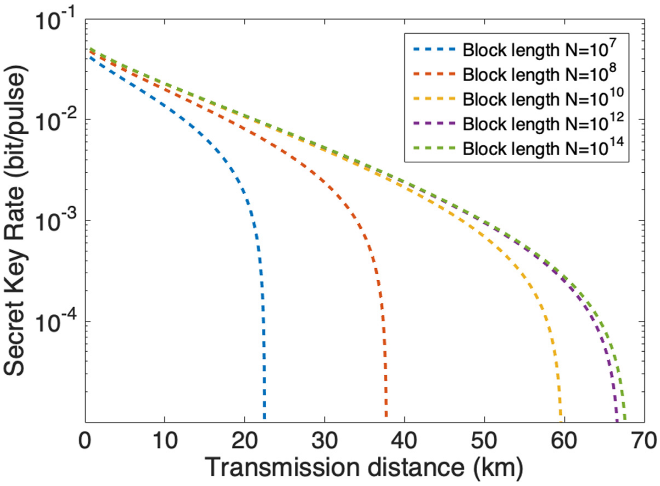

FIG. 9. Finite-size secret key rate of eight-state protocol with $L_{\rm Alice} = 0.6$ km using homodyne detection as a function of transmission distance. From left to right, dashed lines correspond to block lengths of $N = 10^7$, $N = 10^8$, $N = 10^{10}$, $N = 10^{12}$, and $N = 10^{14}$. Parameters are set to $n = N/2$, $\bar{\epsilon} = \epsilon_{PE} = \epsilon_{PA} = 10^{-10}$.

obtained in the finite-size regime. For example, the positive secret key rate exists in finite-size regime but vanishes in a composable security framework when the block length $N = 10^{12}$ and the transmission distance is 60 km. It is worth mentioning that the technique we used for analyzing composable security is developed in Ref. [9], which mainly focuses on the composable analysis of the GM CVQKD. Fortunately, it can also be used for the composable analysis of the DM CVQKD with the linear quantum channel [15]. Most recently, a latest study on the composable security of the DM CVQKD against collective Gaussian attacks has been proposed (but has not been officially published yet) [27], so that one may obtain a more precise composable security bound of the DM CVQKD with an untrusted source by taking advantage of their techniques in the future.

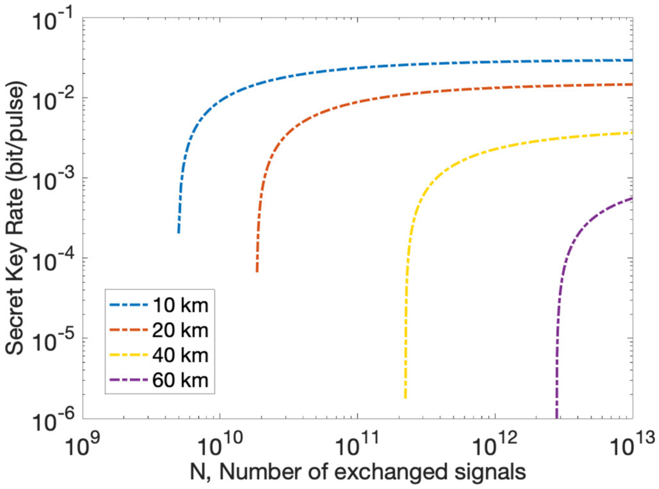

FIG. 10. Composable secret key rate of eight-state protocol with $L_{\rm Alice} = 0.6$ km using homodyne detection as a function of number of exchanged signals. From left to right, lines correspond to transmission distances of 10, 20, 40, and 60 km. See the Appendix for the settings of parameters.

V. CONCLUSION

In this paper, we have thoroughly investigated the DM CVQKD with a special configuration in which the signal source is placed at the untrusted quantum channel. By moving the entanglement source out of Alice's side, the source is no longer protected by the trusted sender but is exposed to the vulnerable environment. Specifically, we have considered two typical DM CVQKD protocols, which are the four-state protocol and the eight-state protocol, and two classic coherent detection technologies, i.e., heterodyne detection and homodyne detection. A security analysis based on the linear bosonic channel shows that the DM CVQKD with an untrusted entanglement source is able to defend itself against the most powerful quantum collective attack when the source is close to one of the legitimate users, thereby discarding the necessity of the security assumption that signal source cannot be compromised. Moreover, by taking account of the finite-size effect and composable security, the DM CVQKD with an untrusted entanglement source can still generate a positive secret key rate. Although its performance is degenerated without the assumptions of the security source and the infinite length of secret key, this work evaluates the performance of the DM CVQKD in realistic conditions, thereby providing a theoretical ground for applying the DM CVQKD system to a real environment.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grants No. 61871407 and No. 61772191), National Key R&D Project (Grant No. 2018YFB0704000), Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ5088), and the Fundamental Research Funds for the Central Universities (Grant No. 531118010371).

APPENDIX: COMPOSABLE SECRET KEY RATE OF DISCRETELY MODULATED CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION WITH UNTRUSTED SOURCE

Before we detail the calculation of the composable secret key rate for the DM CVQKD with an untrusted source, several parameters need to be defined at first.

Let d be the number of bits on which each coherent state is encoded, so we have $d = 2$ for the four-state protocol and $d = 3$ for the eight-state protocol. Let l_{EC} be the size of Bob's communication to Alice during the error-correction step, ϵ_{PE} be the maximum failure probability of parameter estimation step, $\epsilon_{\rm cor}$ be the small probability of the failure that the keys of Alice and Bob are not identical and the protocol did not abort, n_{PE} be the number of bits that Bob sends to Alice during the parameter-estimation step, and $\Omega_a^{\max}$, $\Omega_b^{\max}$, $\Omega_c^{\min}$ be the bounds on covariance matrix elements, which must be apt in the realization of the protocol.

Assuming $\epsilon = 2\epsilon_{sm} + \bar{\epsilon} + \epsilon_{PE}/\epsilon + \epsilon_{\rm cor}/\epsilon + \epsilon_{\rm ent}/\epsilon$, a CVQKD protocol is ϵ secure against collective attacks when the final key length n is selected such that

$$\begin{aligned} n \leqslant 2N\hat{H}_{MLE}(U) - NF\left(\Omega_a^{\max},\ \Omega_b^{\max},\ \Omega_c^{\min}\right) \\ - l_{EC} - \Delta_{AEP} - \Delta_{\text{ent}} - 2\log_2\frac{1}{2\bar{\epsilon}}, \end{aligned} \tag{A1}$$

where $\hat{H}_{MLE}(U)$ is the empiric entropy of U, and F is the function computing the Holevo information between Eve and Bob, and

$$\begin{aligned} \Delta_{AEP} &= \sqrt{N}(d+1)^2 + \sqrt{16N}(d+1)\log_2\frac{2}{\epsilon_{sm}^2} \\ &\quad + \sqrt{4N}\log_2\frac{2}{\epsilon^2\epsilon_{sm}} - 4\frac{\epsilon_{sm}d}{\epsilon}, \end{aligned} \tag{A2}$$

$$\Delta_{\text{ent}} = \log_2\frac{1}{\epsilon} - \sqrt{4N\log^2(2N)\log_2(2/\epsilon_{sm})}. \tag{A3}$$

Since the calculation is based on a linear quantum channel with transmissivity $T = T_1T_2$ and excess noise ε, we have the following model to describe the error correction:

$$\beta I(A:B) = 2\hat{H}_{MLE(U)} - \frac{1}{2n}l_{EC}. \tag{A4}$$

For simplicity, we only consider homodyne detection, so that $I(A:B)$ can be further expressed as

$$\begin{aligned} I(A:B) &= \frac{1}{2}\log_2(1+SNR) \\ &= \frac{1}{2}\log_2\left(1+\frac{TV_M}{2+T\varepsilon}\right). \end{aligned} \tag{A5}$$

In addition, we assume that the robustness of the protocol is $\epsilon_{rob} \leqslant 10^{-2}$, rendering the probability of passing the parameter estimation to no less than 0.99. This can be achieved by taking values for $\Omega_a^{\max}$, $\Omega_b^{\max}$, $\Omega_c^{\min}$ differing by three standard deviations from the expected values. After doing that, the values of random variables $||X||^2$, $||Y||^2$, and $\langle X, Y\rangle$ satisfy the following restraints:

$$||X||^2 \leqslant T_1(N+3\sqrt{N})(X+\chi_{\text{line}_1}), \tag{A6}$$

$$||Y||^2 \leqslant T_2(N+3\sqrt{N})(Y+\chi_{\text{line}_2}), \tag{A7}$$

$$\langle X, Y\rangle \geqslant (N-3\sqrt{N})\sqrt{T}Z. \tag{A8}$$

Note that the above restraints can be acquired from the covariance matrix $\Gamma_{A_1B_2}$ of the DM CVQKD with an untrusted entanglement source. According to these bounds, we can derive

$$\Omega_a^{\max} = \frac{||X||^2}{N}\left[1+2\sqrt{\frac{\log_2(36/\epsilon_{PE})}{N/2}}\right] - 1, \tag{A9}$$

$$\Omega_b^{\max} = \frac{||Y||^2}{N}\left[1+2\sqrt{\frac{\log_2(36/\epsilon_{PE})}{N/2}}\right] - 1, \tag{A10}$$

$$\Omega_c^{\min} = \frac{\langle X, Y\rangle}{N} - 5\left(||X||^2+||Y||^2\right)\sqrt{\frac{\log_2(8/\epsilon_{PE})}{(N/2)^3}}. \tag{A11}$$

With all the equations, the composable secret key rate of the DM CVQKD with an untrusted entanglement source can be calculated by

$$\begin{aligned} K_{\text{composable}} = (1-\epsilon_{rob})\Bigg\{&\beta I(A:B) \\ &-F\left(\Omega_a^{\max}, \Omega_b^{\max}, \Omega_c^{\min}\right) \\ &-\frac{1}{N}\left(\Delta_{AEP}+\Delta_{\text{ent}}+2\log_2\frac{1}{2\bar{\varepsilon}}\right)\Bigg\}. \end{aligned} \tag{A12}$$

It is worth noting that the parameters have to be optimized to satisfy $\epsilon = 10^{-20}$, but to simplify the data process, we make the following suboptimized choices:

$$\begin{aligned} \epsilon_{sm} &= \bar{\epsilon} = 10^{-21}, \\ \epsilon_{PE} &= \epsilon_{\text{cor}} = \epsilon_{\text{ent}} = 10^{-41}. \end{aligned} \tag{A13}$$

[1] C. H. Bennett and G. Brassard, Quantum cryptography : Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, arXiv:1906.01645.

[3] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, No-Switching Quantum Key Distribution using Broadband Modulated Coherent Light, Phys. Rev. Lett. **95**, 180503 (2005).

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

[5] Q. Liao, G. Xiao, H. Zhong, and Y. Guo, Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution, New J. Phys. **22**, 083086 (2020).

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

[7] R. García-Patrón and N. J. Cerf, Unconditional Optimality of Gaussian Attacks Against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

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

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

[10] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, Blockchain empowered arbitrable data auditing scheme for network storage as a Service, IEEE Trans. Serv. Comput. **13**, 289 (2020).

[11] N. Wang, S. Du, W. Liu, X. Wang, Y. Li, and K. Peng, Long-Distance Continuous-Variable Quantum Key Distribution with Entangled States, Phys. Rev. Appl. **10**, 064028 (2018).

[12] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[13] 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. Photonics **13**, 839 (2019).

[14] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks, Phys. Rev. A **79**, 012307 (2009).

[15] Q. Liao, Y. Guo, D. Huang, P. Huang, and G. Zeng, Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection, New J. Phys. **20**, 023015 (2018).

[16] 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).

[17] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution, Phys. Rev. X **9**, 041064 (2019).

[18] 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).

[19] Q. Liao, Y. Guo, Y. Wang, and D. Huang, Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution, Opt. Express **26**, 19907 (2018).

[20] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, Phys. Rev. A **85**, 052310 (2012).

[21] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, Phys. Rev. Lett. **92**, 217903 (2004).

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

[23] S. Pirandola, S. L. Braunstein, and S. Lloyd, Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography, Phys. Rev. Lett. **101**, 200504 (2008).

[24] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, J. Phys. B: At., Mol. Opt. Phys. **42**, 114014 (2009).

[25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[26] Q. Liao, Y. Guo, C. Xie, D. Huang, P. Huang, and G. Zeng, Composable security of unidimensional continuous-variable quantum key distribution, Quantum Inf. Process. **17**, 1 (2018).

[27] P. Papanastasiou and S. Pirandola, Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks, arXiv:1912.11418.