


Trusted-source-noise model of discrete-modulated continuous-variable quantum key distribution

Mingze Wu,¹ Junhui Li^{1,*}, Bingjie Xu,² Song Yu,¹ and Yichen Zhang^{1,†}

¹State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, 100876 Beijing, China

²National Key Laboratory of Security Communication, Institute of Southwestern Communication, Chengdu, 610041 Sichuan, China

 (Received 4 July 2024; revised 4 August 2024; accepted 13 August 2024; published 11 September 2024)

Discrete-modulated continuous-variable quantum key distribution offers a pragmatic solution, greatly simplifying experimental procedures, while retaining robust integration with classical optical communication. Theoretical analyses have progressively validated the comprehensive security of this protocol, paving the way for practical experimentation. However, imperfect sources in practical implementations introduce noise. The traditional approach is to assume that eavesdroppers can control all of the source noise, which overestimates the ability of eavesdroppers and underestimates the secret-key rate. Some parts of source noise are intrinsic and cannot be manipulated by the eavesdropper, so they can be seen as trusted noise. We tailor a trusted-noise model specifically for the discrete-modulated protocol and upgrade the security analysis accordingly. Simulation results demonstrate that this approach successfully mitigates the negative impact of an imperfect source on system performance, while maintaining security of the protocol. Furthermore, our method can be used in conjunction with a trusted-detector-noise model, effectively reducing the influence of both source noise and detector noise in the experimental setup. This is a meaningful contribution to the practical deployment of discrete-modulated-continuous-variable-quantum-key-distribution systems.

DOI: [10.1103/PhysRevApplied.22.034024](https://doi.org/10.1103/PhysRevApplied.22.034024)

I. INTRODUCTION

Quantum key distribution (QKD) [1] is a significant application in the field of quantum information, having strong practicability and commercial value [2–4]. It enables two trusted users to establish secret keys with unconditional security in theory. Continuous-variable quantum key distribution (CVQKD) using coherent states [5–7] exhibits strong compatibility with classical optical communications, and can achieve high secret-key rates over short-to-medium distances, thus having significant advantages in practical deployments within metropolitan areas [8]. In recent years, CVQKD has been considered theoretically [9–11] and experimentally [12–14]. Advancements in chip integration [15–19] and networks [20–23] have significantly increased the practicality of CVQKD.

Distinguished by modulation methods, CVQKD can be categorized into Gaussian-modulated protocols [5–7], discrete-modulated protocols [24–28], etc. Gaussian-modulated protocols were proposed earlier and

have experienced considerable development due to the simplicity of security proofs taking advantage of the extremality of Gaussian states [29–31]. However, Gaussian modulation requires thousands of discrete constellations to approximate continuous modulation in practical experiments [32], which will consume more random numbers and postprocessing resources. In contrast, discrete modulation, a commonly used modulation method in classical optical communication, is straightforward to implement and highly practical, representing one of the promising directions for CVQKD [24]. Because of the non-Gaussian property of the quantum states shared by both communication parties under discrete modulation, security proof of the discrete-modulated protocol is limited by the assumption of a linear channel for a long time [24]. Fortunately, the introduction of the semidefinite-programming (SDP) method has successfully resolved this issue [26,27]. Ghorai *et al.* [26] realized asymptotic security analysis of a quadrature-phase-shift-keying (QPSK) modulation protocol, and used SDP to constrain the covariance term in the covariance matrix. The method was further extended to arbitrary modulation, enabling the analytical bound of SDP [33]. Additionally, experimental verification has been achieved [34–37]. However, this method remains reliant

*Contact author: lijunhui@bupt.edu.cn

†Contact author: zhangyc@bupt.edu.cn

on the optimality theorem of the Gaussian state, resulting in a bound that is not tight enough. Lin *et al.* [27] used quantum relative entropy to express the security key rate, optimizing quantum relative entropy through SDP via a two-step numerical calculation method [38,39] to obtain a more-compact security key rate. This is a highly appealing method that has undergone further enhancements [40–42], and has been thoroughly verified through long-distance experiments [43]. Moreover, on the basis of this method, finite-size security analysis of the discrete-modulated protocol under collective attack [44] and coherent attack [45] has also been proposed.

The basic assumption of QKD protocols is that all devices conform to an ideal model, and eavesdroppers cannot infiltrate the devices of both communication parties. Most security analysis in previous work was solely based on ideal devices, which use ideal light sources, detectors, and other devices that conform to basic assumptions. Unfortunately, in practical systems, few devices can perfectly adhere to the basic assumptions of the protocols, thus necessitating adjustment of security-analysis methods [46,47]. Research into nonidealities in Gaussian-modulated CVQKD is quite extensive [48–50]. However, the trusted-noise model on the source side of discrete-modulated protocols has not been studied. Following the approaches of Gaussian modulation, there have been some developments on nonideal detectors of discrete-modulated protocols, including the trusted-noise model [51] and quantum hacking attacks [52].

Besides detection and channel propagation, state preparation is also important in any QKD protocol. During this step, lasers, digital-to-analog converters (DACs), and modulators all exhibit various nonidealities. These nonidealities result in noise in the prepared quantum states. In previous security analysis, all the source noise was considered as untrusted excess noise that can be fully accessed by the eavesdropper, thus having a huge impact on system performance [32]. Nevertheless, some source noise originates from an intrinsic stochastic mechanism, or always remains within Alice's system, and cannot be manipulated by the eavesdroppers [53,54]. Therefore, previous treatment to see all the source noise untrusted just exaggerates Eve's power and leads to an untight bound on the security key rate [55]. For Gaussian-modulated protocols, there has been much research on the imperfect state preparation, including the trusted-source-noise model [50] and source monitoring [56,57]. Nonidealities also exist in discrete-modulated CVQKD. However, because of the differences in security-analysis methods, these source-noise models cannot be directly applied to discrete-modulated CVQKD.

In this contribution, we provide a trusted-source-noise model of a discrete-modulated-CVQKD protocol based on a foregoing security-analysis method with SDP. We analyze the nonideality in the state-preparation process of the discrete-modulated protocol, and show that some

parts of noise cannot be manipulated by eavesdroppers, so can be trusted. For trusted source noise, the thermal state is used for modeling, and the trusted-source-noise model is established. According to this model, the secret-key rate of discrete-modulated CVQKD is calculated, which shows that previous untrusted-source-noise treatment significantly underestimates the secret-key rate. Numerical results also show that the secret-key rate obtained by adjustment of the security analysis based on the trusted-noise model can approach the key rate with ideal noiseless devices, indicating that the trusted-source-noise model can almost eliminate the influence of trusted source noise on system performance.

This paper is organized as follows. In Sec. II, we delve into underlying causes and the influence of source noise during the state-preparation process in a practical discrete-modulated-CVQKD system. In Sec. III, we describe the discrete-modulated-CVQKD protocol with noisy coherent states, and then give security analysis of the protocol in detail. In Sec. IV, we present simulation results. Finally, we discuss the work presented in this paper in Sec. V.

II. IMPERFECTION IN PREPARING QUANTUM STATES

In practical experiments, various imperfections introduce noise that can significantly compromise the system's performance. Such unwanted noise, known as excess noise, can be quantified by extra fluctuations in the quadrature measurements. Assuming it is decomposable, in a practical discrete-modulated-CVQKD system, the excess noise can be attributed to various sources, as shown in Fig. 1, including laser relative intensity noise ξ_{RIN} , modulator noise ξ_{mod} , DAC noise ξ_{DAC} , quantum channel noise ξ_{ch} , and detector noise ξ_{det} [47]:

$$\xi = \xi_{\text{RIN}} + \xi_{\text{mod}} + \xi_{\text{DAC}} + \xi_{\text{ch}} + \xi_{\text{det}} + \dots, \quad (1)$$

where ξ represents the equivalent excess noise at the source side. Since signal laser, modulator, and DAC noise exist in the transmitter of the CVQKD system, this part of

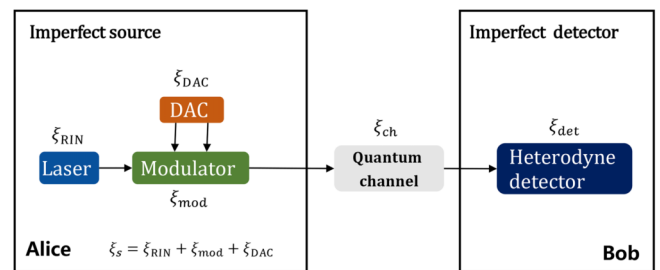


FIG. 1. Practical discrete-modulated-CVQKD system with source noise introduced in Sec. II.

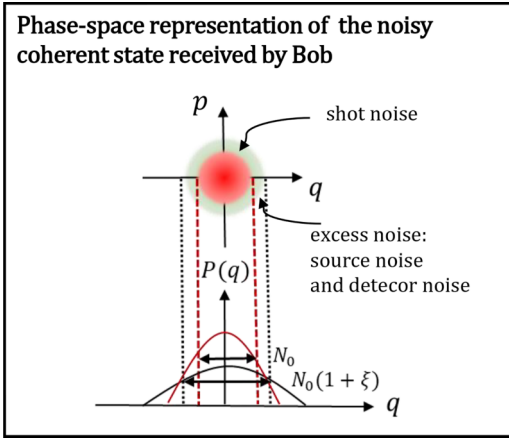


FIG. 2. Phase-space representation of the coherent state received by Bob. The red circle represents shot noise with variance of N_0 , the outer green ring represents excess noise, both source noise and detector noise, and the total variance of the noisy coherent state is $N_0(1 + \xi)$.

noise can be summed as source noise ξ_s :

$$\xi_s = \xi_{\text{RIN}} + \xi_{\text{mod}} + \xi_{\text{DAC}}. \quad (2)$$

The phase-space representation of the coherent state received by Bob with excess noise is shown in Fig. 2. The effect of source noise on coherent states is to expand the fluctuation range—that is, to increase the variance from N_0 to $N_0(1 + \xi_s)$, where N_0 is shot-noise variance. In the following, noise is represented in the natural unit by default. The three types of source noise are described below. The excess noise caused by relative intensity noise comes from the power fluctuations of the laser:

$$\xi_{\text{RIN}} = V_M \sqrt{R \Delta \nu}, \quad (3)$$

where V_M is the modulation variance of Alice's data, R is the relative intensity noise, and $\Delta \nu$ is the laser linewidth. The excess noise of the modulator mainly comes from modulated light extinction:

$$\xi_{\text{mod}} = V_M 10^{-d_{\text{dB}}/10}, \quad (4)$$

where d_{dB} is the extinction ratio of the modulator. The excess noise introduced by the DAC arises from errors in converting signal digits into voltage, which can be bounded by

$$\xi_{\text{DAC}} \leq V_M \left[\pi \frac{\delta U_{\text{DAC}}}{U_{\text{DAC}}} + \frac{1}{2} \left(\pi \frac{\delta U_{\text{DAC}}}{U_{\text{DAC}}} \right)^2 \right]^2, \quad (5)$$

where U_{DAC} is the signal voltage and δU_{DAC} is a specific deviation.

It is worth mentioning that not all of the excess noise in Eq. (1) can be used by eavesdroppers, such as source noise ξ_s and detector noise ξ_{det} , as they are within the system and no quantum hacking attack has been proposed to manipulate source noise, up to now. If they are treated as untrusted, they can lead to overestimation of the eavesdropper's capabilities, significantly reducing system performance. Therefore, if this part of the noise can be trusted, system performance will improve. If the corresponding quantum hacking attack appears in the future, then the corresponding noise can be removed from the trusted part. The trusted-noise model in our work can adapt to this change. Since trusted detector noise for discrete-modulated CVQKD has been studied in Ref. [51], next we consider mainly the trusted-noise model of an imperfect source and combine it with trusted detector noise.

III. DISCRETE-MODULATED CVQKD WITH AN IMPERFECT SOURCE

In this section, we focus on a practical discrete-modulated-CVQKD system with source noise as in Fig. 1, taking QPSK-modulated CVQKD as an example. The protocol description is shown in Appendix A, based on previous work [27,51]. We present the model of trusted source noise, together with comprehensive security analysis of the protocol. It is worth noting that our scheme modeling an imperfect source can be scaled up to a higher number of modulation constellations, enhancing protocol performance at the cost of increased computational complexity. For a protocol using homodyne detection, our model is also applicable.

Because the trusted part of source noise is inside Alice's system, it cannot be exploited by eavesdroppers and can be renamed as ν_s to distinguish it from excess noise. In the Gaussian-modulated protocol, source noise is modeled as a mode of an Einstein-Podolsky-Rosen state, and the covariance matrix and optimality of Gaussian attacks are used in the security analysis [53]. However, this approach is not applicable to the discrete-modulated protocol. In our model, a beam splitter with transmittance $\eta_s \rightarrow 1$ (we set $\eta_s = 0.9999$) and a thermal state can be used to model the trusted part of source noise. The signal state $\rho_{AA'}$ and the thermal state $\rho_{\text{th}}(\bar{n}_s)$ are coupled by a beam splitter, and the output state is transmitted to Bob through the quantum channel, as shown in Fig. 3. When the source noise is ν_s , the average photon number \bar{n}_s of the input equivalent thermal state $\rho_{\text{th}}(\bar{n}_s)$ is given by $\bar{n}_s = \nu_s / (1 - \eta_s) N_0$, where N_0 is the variance of shot noise in the unit of vacuum fluctuation. The variance of each quadrature of the thermal state is $[1 + \nu_s / (1 - \eta_s)] N_0$.

In the ideal protocol, based on the source-replacement scheme, when Alice sends coherent states $|\varphi_k\rangle$ with probability p_k in the prepare-and-measure scheme, she equivalently prepares a bipartite state $|\Psi\rangle_{AA'}$ in the

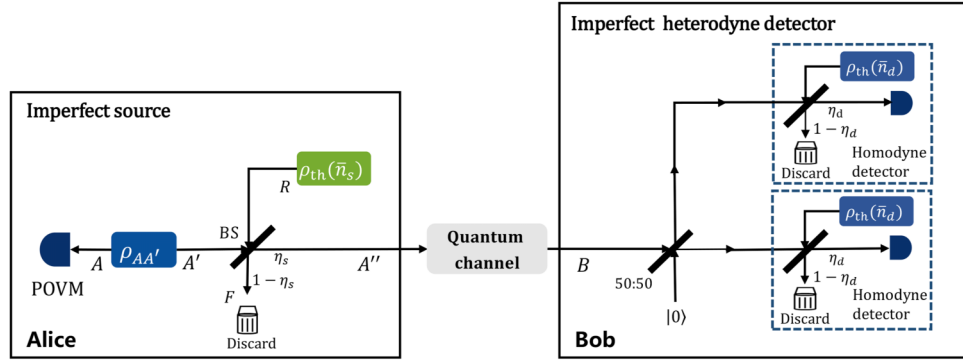


FIG. 3. Entanglement-based discrete-modulated-CVQKD protocol with imperfect source, where $\rho_{\text{th}}(\bar{n}_s)$ is a thermal state with average photon number \bar{n}_s , the beam splitter (BS) has transmittance $\eta_s = 0.9999$, and M^A is the POVM. Mode F is discarded. Bob performs heterodyne detection with trusted detector noise [51].

entanglement-based scheme

$$|\Psi\rangle_{AA'} = \sum_{x=0}^3 \sqrt{p_x} |x\rangle_A |\varphi_x\rangle_{A'}, \quad (6)$$

where $\{|x\rangle\}$ serves as an orthonormal basis set in register A . The density matrix of the bipartite state can be expressed as $\rho_{AA'} = |\Psi\rangle_{AA'} \langle\Psi|$. Alice reserves register A and performs positive-operator-valued measurement (POVM) $M^A = \{M_x^A = |x\rangle \langle x| : x \in \{0, 1, 2, 3\}\}$ to obtain outcome x . Register A' is coupled with the thermal state $\rho_{\text{th}}(\bar{n}_s)$ through the beam splitter of transmittance η_s to model the trusted source noise. The density operator of the thermal state with the average photon number \bar{n}_s is given by

$$\rho_{\text{th}}(\bar{n}_s) = \sum_{n=0}^{\infty} \frac{\hat{n}^n}{(1 + \hat{n})^{n+1}} |n\rangle \langle n|. \quad (7)$$

In the coherent-state representation, the thermal state can be rewritten as

$$\rho_{\text{th}}(\bar{n}_s) = \frac{1}{\pi \bar{n}_s} \int_{\mathbb{C}} \exp\left(-\frac{|\beta|^2}{\bar{n}_s}\right) |\beta\rangle \langle \beta| d^2\beta, \quad (8)$$

where β is the complex amplitude of a coherent state and \mathbb{C} is the set of complex numbers. After being coupled through the beam splitter, the quantum state of Alice's system, which includes the source noise, is given by

$$\rho_{AA''} = \text{Tr}_R[\hat{S}(\theta) \rho_{AA'} \otimes \rho_{\text{th}_R}(\bar{n}_s) \hat{S}^\dagger(\theta)], \quad (9)$$

where $\hat{S}(\theta) = \exp[\theta(\hat{a}'_A \hat{a}_R - \hat{a}'_A \hat{a}_R^\dagger)]$ is the beam-splitter operator, \hat{a}'_A (or \hat{a}_R) and \hat{a}'_A (or \hat{a}_R^\dagger) are, respectively, the annihilation and creation operators of system A' (R), and θ is related to transmittance η_s by $\eta_s = 1/(1 + \tan^2 \theta)$. According to Appendix B, if coherent states $|\alpha_{A'}\rangle$ and $|\alpha_R\rangle$

are coupled through a beam splitter of transmittance η , the output coherent state is given by

$$|\alpha_{A''}\rangle = |\sqrt{\eta}\alpha_{A'} + \sqrt{1-\eta}\alpha_R\rangle_{A''}. \quad (10)$$

Thus, the quantum state of Alice's system is given by

$$\begin{aligned} \rho_{AA''} &= \frac{1}{\pi \bar{n}_s} \sum_{i,j=0}^3 \sqrt{p_i p_j} |i\rangle_A \langle j| \int_{\mathbb{C}} \exp\left(-\frac{|\beta|^2}{\bar{n}_s}\right) \\ &\times \left| \sqrt{\eta}\alpha_i + \sqrt{1-\eta}\beta \right\rangle_{A''} \left\langle \sqrt{\eta}\alpha_j + \sqrt{1-\eta}\beta \right| d^2\beta. \end{aligned} \quad (11)$$

Then, register A'' is sent to Bob through the quantum channel. The quantum channel can be regarded as a completely-positive-and-trace-preserving (CPTP) map $\mathcal{E}_{A'' \rightarrow B}$, which maps Alice's register A'' to Bob's register B , and is controlled by Eve. Therefore, the quantum state shared by Alice and Bob is given by

$$\rho_{AB} = (I_A \otimes \mathcal{E}_{A'' \rightarrow B}) \rho_{AA''}, \quad (12)$$

where I_A refers to the identity channel within Alice's system A .

After Alice uses POVM $\{M_x^A\}$ to perform local measurement on register A and gets the result x , the coherent state $|\varphi_x\rangle$ will be sent to Bob. Bob's received state conditioned on the choice of x is given by

$$\rho_B^x = \frac{1}{p_x} \text{Tr}_A[\rho_{AB}(|x\rangle \langle x|_A \otimes I_B)]. \quad (13)$$

Bob uses POVM $M^B = \{M_y^B\}$ to get his measurement results. For trusted detector noise, the POVM of heterodyne detection $M_y^B = G_y$ can be expressed as [51]

$$G_y = \frac{1}{\eta_d \pi} \hat{D}\left(\frac{y}{\sqrt{\eta_d}}\right) \rho_{\text{th}}\left(\frac{1-\eta_d + \nu_{\text{el}}}{\eta_d}\right) \hat{D}^\dagger\left(\frac{y}{\sqrt{\eta_d}}\right), \quad (14)$$

where $y \in \mathbb{C}$ is the complex amplitude of the coherent state, η_d is the detector efficiency, v_{el} is detector electrical noise, $\hat{D}(y/\sqrt{\eta_d})$ is the displacement operator, and $\rho_{\text{th}}[(1 - \eta_d + v_{\text{el}})/\eta_d]$ is the thermal state with mean photon number $(1 - \eta_d + v_{\text{el}})/\eta_d$.

The secret-key-rate optimization based on the method in Ref. [51] is shown in Appendix C. Differently from Ref. [51], the state of register A with the trusted-source-noise model is given by

$$\begin{aligned} \rho_A = \text{Tr}_B(\rho_{AB}) &= \frac{1}{\pi \bar{n}_s} \sum_{i,j=0}^3 \sqrt{p_i p_j} |i\rangle \langle j|_A \\ &\times \int_{\mathbb{C}} \exp\left(-\frac{|\beta|^2}{\bar{n}_s}\right) \left(\sqrt{\eta} \alpha_j + \sqrt{1-\eta} \beta \right) \left(\sqrt{\eta} \alpha_i \right. \\ &\left. + \sqrt{1-\eta} \beta \right) d^2 \beta, \end{aligned} \quad (15)$$

which forms a different constraint for the key-rate-optimization problem in Eq. (C3).

In experiments, the parameters of the experimental equipment, such as the relative intensity noise of the laser, the extinction ratio of the modulator, the signal voltage, and specific deviation of the DAC can be used to calculate the source excess noise by Eqs. (2)–(5). The trusted source noise can be separated from excess noise, and then our theoretical model can be used to calculate the secret-key rate.

IV. SIMULATIONS

In this section, we initially present the channel model within the simulation framework and compute the simulated statistics. Subsequently, we simulate the QPSK-modulated-CVQKD protocol, comparing three types of source noise, i.e., ideal noiseless source, untrusted source noise, and trusted source noise, respectively.

A. Simulation method

To demonstrate the protocol's performance, we simulate the quantum channel as a phase-invariant Gaussian channel with transmissivity η_t and excess noise ξ , where $\eta_t = 10^{-\alpha L/10}$ for transmission distance L in kilometers, $\alpha = 0.2$ dB/km is the attenuation coefficient, and the excess noise is defined as

$$\xi = \frac{(\Delta q_{\text{obs}})^2}{(\Delta q_{\text{vac}})^2} - 1, \quad (16)$$

where $(\Delta q_{\text{vac}})^2 = N_0 = 1/2$ is the variance of shot noise for quadrature q , and $(\Delta q_{\text{obs}})^2$ is q quadrature's variance of the signal state measured by Alice.

In this situation, simulated statistics $\langle \hat{F}_Q \rangle_x$, $\langle \hat{F}_P \rangle_x$, $\langle \hat{S}_Q \rangle_x$, $\langle \hat{S}_P \rangle_x$ and estimation of error-correction cost δ_{EC} which

are described in detail in Appendix C can be calculated. The simulated state σ_B^x conditioned on selection of x is a displaced thermal state, and its Wigner function is given by

$$W_{\sigma_B^x}(\gamma) = \frac{1}{\pi} \frac{1}{\frac{1}{2}(1 + \eta_t \eta_s \xi)} \exp\left[-\frac{|\gamma - \sqrt{\eta_t \eta_s} \alpha'_x|^2}{\frac{1}{2}(1 + \eta_t \eta_s \xi)}\right], \quad (17)$$

where

$$\alpha'_x = \frac{1}{\pi \bar{n}_s} \int_{\mathbb{C}} \exp(-|\beta|^2/\bar{n}_s) (\sqrt{\eta} \alpha_x + \sqrt{1-\eta} \beta) d^2 \beta, \quad (18)$$

which can be quickly calculated numerically. Bob uses heterodyne measurement with trusted detector noise that is expressed by POVM G_y and probability density function $P(y|x)$ of measurement result y , conditioned on Alice's selection x :

$$\begin{aligned} P(y|x) &= \frac{1}{\pi \left(1 + \frac{1}{2} \eta_d \eta_t \eta_s \xi + v_{\text{el}}\right)} \\ &\times \exp\left[-\frac{|y - \sqrt{\eta_d \eta_t \eta_s} \alpha'_x|^2}{1 + \frac{1}{2} \eta_d \eta_t \eta_s \xi + v_{\text{el}}}\right]. \end{aligned} \quad (19)$$

Expectation values of the observables in Eq. (C4) can be written as

$$\begin{aligned} \langle \hat{F}_Q \rangle_x &= \sqrt{2 \eta_d \eta_t \eta_s} \text{Re}(\alpha'_x), \\ \langle \hat{F}_P \rangle_x &= \sqrt{2 \eta_d \eta_t \eta_s} \text{Im}(\alpha'_x), \\ \langle \hat{S}_Q \rangle_x &= 2 \eta_d \eta_t \eta_s \text{Re}(\alpha'_x)^2 + 1 + \frac{1}{2} \eta_d \eta_t \eta_s \xi + v_{\text{el}}, \\ \langle \hat{S}_P \rangle_x &= 2 \eta_d \eta_t \eta_s \text{Im}(\alpha'_x)^2 + 1 + \frac{1}{2} \eta_d \eta_t \eta_s \xi + v_{\text{el}}, \end{aligned} \quad (20)$$

which are used as input for the SDP problem. To solve the SDP problem, we use the numerical framework in Refs. [38,39].

B. Simulation results

In this subsection, we first simulate the discrete-modulated CVQKD with an imperfect source in the case of an ideal detector ($v_{\text{el}} = 0, \eta_d = 1$). Then we introduce an imperfect detector with trusted noise ($v_{\text{el}} > 0, \eta_d < 1$), and show the secret-key rates. Furthermore, we optimize the coherent-state amplitude; the optimal amplitude can serve as a valuable guideline for practical experimental implementations. Finally, the effect of postselection on the secret-key rate is studied.

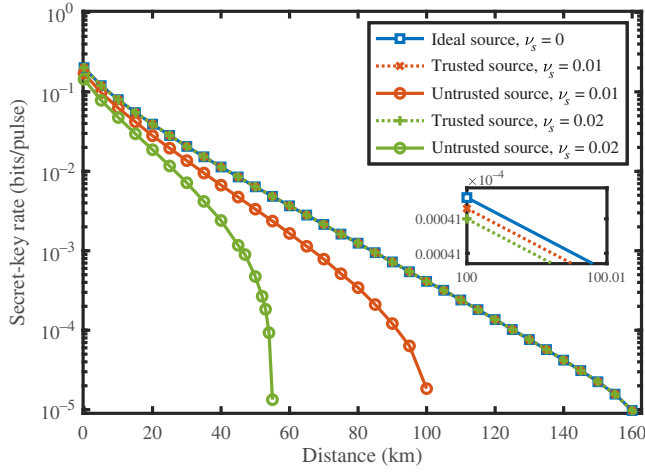


FIG. 4. Secret-key rate versus distance for QPSK-modulated CVQKD with source noise $\nu_s = 0.01$ and $\nu_s = 0.02$ for an ideal source ($\nu_s = 0$) under both trusted and untrusted models. Excess noise $\xi = 0.02$, reconciliation efficiency $\beta = 0.956$, coherent-state amplitude $\alpha = 0.6$, and postselection parameter $\Delta_a = 0$.

1. Comparison of source-noise models

To evaluate source noise's effect, we compare the performance of the QPSK-modulated-CVQKD protocol with an ideal noiseless source, trusted source noise, and untrusted source noise, respectively, as illustrated in Figs. 4 and 5.

In Fig. 4, the secret-key rate with omission of detector noise is shown versus the transmission distance. We take the excess noise ξ to be 0.02, and error-correction efficiency $\beta = 0.956$ [58], without considering the postselection process. We set the source noise ν_s as 0.01 and

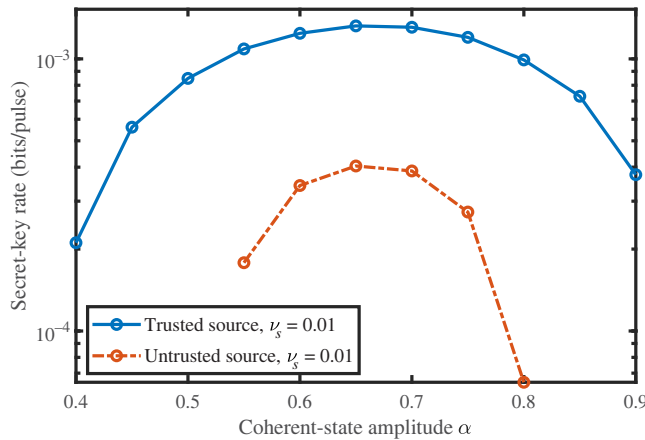


FIG. 5. Secret-key rate versus coherent-state amplitude α for QPSK-modulated CVQKD with imperfect source noise $\nu_s = 0.01$, trusted and untrusted, respectively. Excess noise $\xi = 0.02$, reconciliation efficiency $\beta = 0.956$, transmission distance $L = 80$ km, and postselection parameter $\Delta_a = 0$.

0.02, respectively. Simulation results indicate that, even with source noise of 0.02, the performance of the protocol with trusted source noise is almost equivalent to that with an ideal source. In contrast, when source noise cannot be trusted, the maximum transmission distance of the protocol is less than 60 km under source noise $\nu_s = 0.02$. However, when it can be trusted, it can be transmitted to more than 160 km. The result shows that the proposed trusted-noise model almost eliminates the impact of an imperfect source on the performance of discrete-modulated CVQKD. Compared with the performance with an untrusted source, the performance is greatly improved, both for transmission distance and for secret-key rate. Moreover, the performance improvement becomes more significant as the source noise increases.

In Fig. 5, the coherent-state amplitude is optimized for the QPSK-modulated-CVQKD protocol in 80 km with trusted source and untrusted source noise, respectively, where source noise $\nu_s = 0.01$ and other parameters are the same as in Fig. 4. Simulation results show that in this condition, the optimal coherent-state modulation amplitude is about 0.65, no matter whether the source noise is trusted or not. However, when the source noise can be trusted, the secret-key rate of the protocol is more than 10^{-3} bits per pulse, nearly an order of magnitude larger than for its untrusted-source-noise counterpart.

2. Inclusion of detector noise

Next, we consider an actual situation in the experiments, an imperfect detector, and use real parameters to simulate the QPSK-modulated-CVQKD protocol with the trusted-detector-noise model [51].

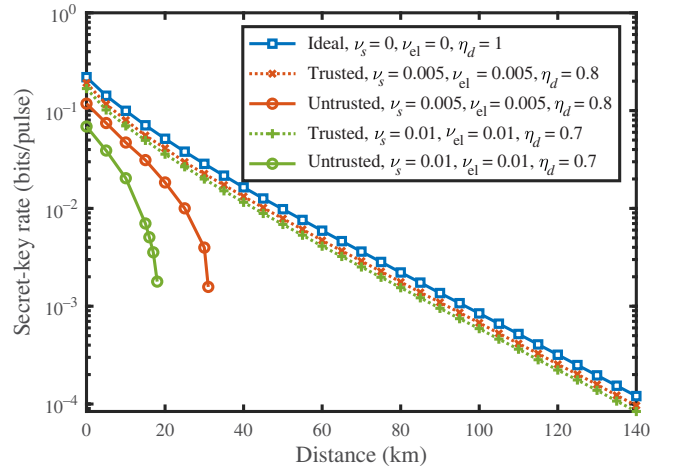


FIG. 6. Secret-key rate versus distance for QPSK-modulated CVQKD with ideal, trusted, and untrusted noise. Trusted detector noise is included. Excess noise $\xi = 0.01$, reconciliation efficiency $\beta = 0.956$, coherent-state amplitude $\alpha = 0.6$, and postselection parameter $\Delta_a = 0$.

In Fig. 6, we compare the secret-key rates of the protocol with ideal, trusted, and untrusted noise (trusted noise means that both the source noise and the detector noise are trusted, and untrusted noise means that both the source noise and the detector noise are untrusted). For noise amplitude, two situations—with $\nu_s = 0.005$, $\nu_{el} = 0.005$, and $\eta_d = 0.8$, and with $\nu_s = 0.01$, $\nu_{el} = 0.01$, and $\eta_d = 0.7$ —are considered to represent high and low noise status. Compared with ideal sources and detectors, the key rate under trusted noise is slightly lower, mainly due to imperfect detection efficiency. However, when the noise from the source and the noise from the detector become untrusted, the protocol performance rapidly declines, primarily since the noise is factored into the excess noise, and the equivalent excess noise on the source side $\xi = \nu_s + \nu_{el}/\eta_t$. When the transmission distance increases, excess noise significantly rises, leading to a rapid decrease of the secret-key rate. The trusted models effectively address this issue, and enable the protocols to maintain high performance.

In Fig. 7, we show the secret-key rate versus the distance with different excess noise, where source noise $\nu_s = 0.001$, detector noise $\nu_{el} = 0.297$, and detection efficiency $\eta_d = 0.45$ [34]. When they cannot be trusted, the protocol cannot generate secret keys. When source noise and detector noise can be trusted, the simulation outcomes indicate that, under the given parameters, the protocol can transmit over 200 km when excess noise is 0.01. However, as excess noise increases to 0.02, the secret-key rate experiences a notable decline once the transmission distance surpasses 180 km. Furthermore, with excess noise of 0.03, the protocol's transmission limit is reduced to approximately 120 km.

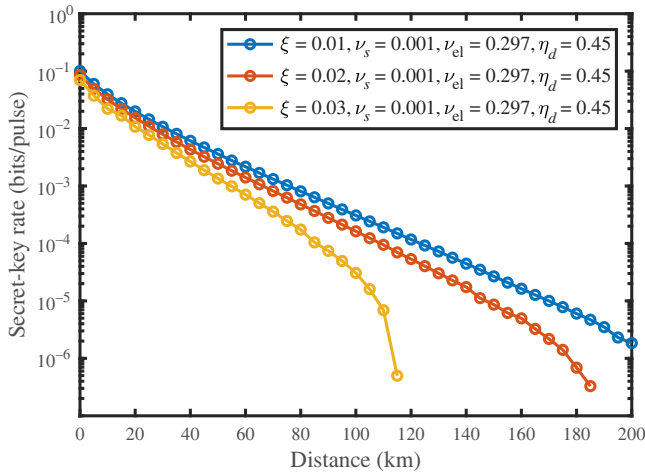


FIG. 7. Secret-key rate versus distance for QPSK-modulated CVQKD with different excess noise. Source noise $\nu_s = 0.001$, detector noise $\nu_{el} = 0.297$, detection efficiency $\eta_d = 0.45$, reconciliation efficiency $\beta = 0.956$, coherent-state amplitude $\alpha = 0.65$, and postselection parameter $\Delta_a = 0$.

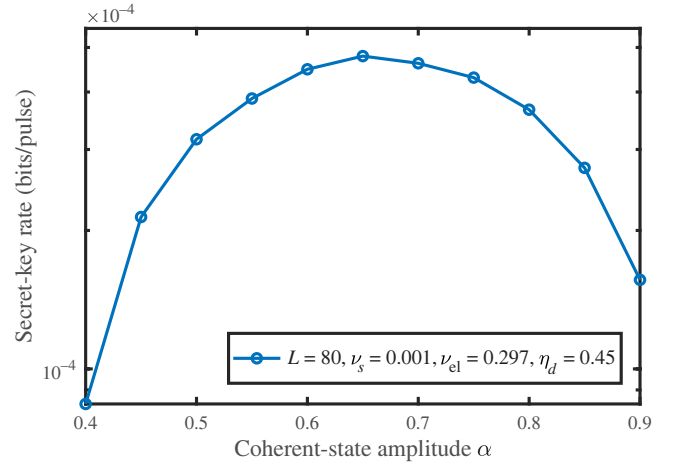


FIG. 8. Optimization of coherent-state amplitude α of QPSK-modulated CVQKD with excess noise $\xi = 0.02$, source noise $\nu_s = 0.001$, detector noise $\nu_{el} = 0.297$, detection efficiency $\eta_d = 0.45$, reconciliation efficiency $\beta = 0.956$, and postselection parameter $\Delta_a = 0$. When the source noise and detector noise are untrusted, the secret-key rate is 0.

In Fig. 8, the coherent-state amplitude is optimized for the QPSK-modulated-CVQKD protocol in 80 km with trusted source noise and detector noise, excess noise $\xi = 0.02$, and other parameters the same as in Fig. 7. Simulation results show that the optimal coherent-state amplitude is about 0.65 in this condition, which is almost equal to the value in the situation without the trusted-noise model in Fig. 5. The secret-key rate with optimal coherent-state amplitude is about 4×10^{-4} bits per pulse.

3. Inclusion of postselection

Next we consider the influence of trusted-source-noise and trusted-detector-noise models on the postselection parameter, and demonstrate the increase of the secret-key

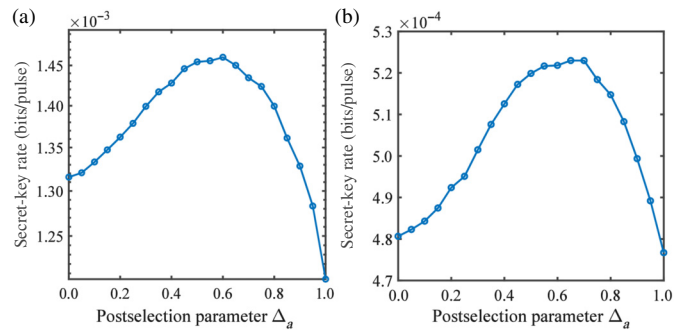


FIG. 9. Optimization of postselection parameter Δ_a of QPSK-modulated CVQKD. (a) Ideal source and detector. (b) Trusted source and detector. Both with distance $L = 80$ km, excess noise $\xi = 0.02$, source noise $\nu_s = 0.001$, detector noise $\nu_{el} = 0.297$, detection efficiency $\eta_d = 0.45$, and reconciliation efficiency $\beta = 0.956$.

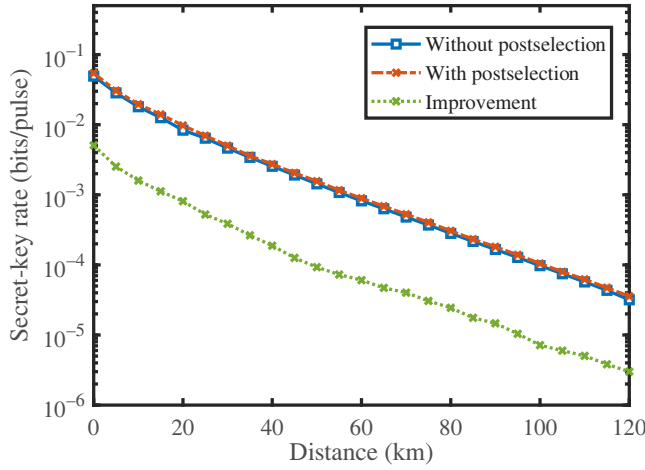


FIG. 10. Secret-key rate versus distance for QPSK-modulated CVQKD with and without postselection. Source noise $\nu_s = 0.001$, detector noise $\nu_{el} = 0.297$, detection efficiency $\eta_d = 0.45$, reconciliation efficiency $\beta = 0.956$, coherent-state amplitude $\alpha = 0.65$, and optimized postselection parameter.

rate in QPSK-modulated CVQKD with trusted source and detector noise through postselection.

In Fig. 9, the postselection parameter of QPSK-modulated CVQKD in 80 km with trusted source and detector noise is optimized, in parallel with the ideal noiseless case, where the coherent-state amplitude is $\alpha = 0.65$ and other parameters are the same as in Fig. 8. Simulation results show that for ideal case as shown in Fig. 9(a), the optimal postselection parameter is about 0.65, and the secret-key rate can increase by up to approximately 7% compared with the rate without postselection ($\Delta_a = 0$). In Fig. 9(b), with the trusted-noise model, the optimal postselection parameter is about 0.7, and the secret-key rate can be increased from 4.8×10^{-4} bits per pulse ($\Delta_a = 0$) to 5.2×10^{-4} bits per pulse, which is about 8% higher. Overall, the trusted-noise model would not change much the optimal postselection parameter, nor would it improve the performance of postselection.

In Fig. 10, we demonstrate the performance improvement of optimal postselection at different distances for noise parameters the same as those in Fig. 7. Simulation results show that postselection can increase the secret-key rate by about 7% at various distances.

In summary, the simulation results exhibit significant enhanced performance of the QPSK-modulated-CVQKD protocol when source and detector noise can be trusted, compared with the untrusted counterpart. In addition, application of trusted-noise models has little impact on postselection, and reasonable postselection can further improve the performance of a discrete-modulated-CVQKD system.

V. DISCUSSION AND CONCLUSION

Over the past 5 years, theoretical security of discrete-modulated CVQKD has been progressively refined. The modeling of trusted noise in practical systems is an important part of the practical security of CVQKD, which can avoid the loss of secret-key rate caused by one mistakenly listing trusted noise as untrusted. The trusted-noise model makes sense since the devices are inside the system and cannot be manipulated. It is worth noting that there may be some quantum hacking attacks in the future that can break this assumption. For example, the modulation noise of an in-phase-and-quadrature modulator can be trusted in many cases, but if Eve could control the driver electrical signal of an in-phase-and-quadrature modulator, the trusted-source-noise assumption is compromised. Once such attacks are proposed, these parts of noise cannot be regarded as trusted noise. If communication parties still consider them as trusted noise, the overestimation of the secret-key rate will have a serious impact on system security. In this case, these parts of noise need to be regarded as untrusted, and our trusted modeling is still applicable to other source noise. Meanwhile, some countermeasures are also feasible, such as electromagnetic shielding, to keep the source noise trusted.

In this contribution, we examined the challenges posed by an imperfect source in a discrete-modulated-CVQKD system and proposed a trusted-source-noise model. Our work can readily be applied to the finite-size regime that ensures composable security, and protocols using higher-order modulation. The results show that, compared with previous treatment, which classifies all source noise into the excess noise controllable by eavesdroppers, this model more accurately evaluates the ability of eavesdroppers and increases the secret-key rate of discrete-modulated-CVQKD systems, which takes an important step towards practical application of discrete-modulated CVQKD.

ACKNOWLEDGMENTS

This research was supported by the National Natural Science Foundation of China (Grant No. 62001044), the Basic Research Program of China (Grant No. JCKY2021210B059), the Equipment Advance Research Field Foundation (Grant No. 315067206), the Fund of State Key Laboratory of Information Photonics and Optical Communications, and the Fundamental Research Funds for Central Universities, China (Grant No. 2023RC28).

APPENDIX A: PROTOCOL DESCRIPTION OF QPSK-MODULATED CVQKD WITH AN IMPERFECT SOURCE

The prepare-and-measure version of the practical QPSK-modulated protocol is as follows:

(1) State preparation. For each round, Alice uses a laser, which is then integrated into the modulator, facilitating the emission of a coherent state $|\varphi_k\rangle$ chosen from the set $\{|\alpha\rangle, |-\alpha\rangle, |i\alpha\rangle, |-i\alpha\rangle\}$ according to probability $p_k = 1/4$, where $\alpha \in \mathbb{R}$ is the amplitude of the coherent states. The modulator is driven by a DAC. It should be noted that these devices are imperfect and contain nonideal factors as shown in Sec. II. The coherent state is sent to Bob through the quantum channel that is controlled by Eve.

(2) Measurement. After receiving the state sent from Alice, Bob uses a heterodyne detector with trusted noise and obtains the measurement result $y \in \mathbb{C}$.

The physical process of the prepare-and-measure version of the practical QPSK-modulated protocol is shown in Fig. 1(a), and the excess noise introduced in Sec. II is considered. The excess noise makes the variance of the quadrature increase from N_0 to $N_0(1 + \xi)$, and its phase-space representation is shown in Fig. 1(b). After the physical process of the protocol, Alice and Bob perform postprocessing through the classic channel, including announcement and sifting, parameter estimation, reverse-reconciliation key map, error correction, and privacy amplification. These processes are similar to those in the literature [27,51]. For the sake of integrity, we briefly introduce these steps:

(a) Announcement and sifting. After N rounds of communication, Alice and Bob identify a small subset of test rounds τ_{test} used for parameter estimation, and use the remaining rounds τ_{key} to generate keys. Following the sifting process, Alice obtains her string $\mathbf{X} = (x_1, \dots, x_m)$ according to the following rule:

$$\forall j \in [m], \quad x_j = \begin{cases} 0 & \text{if } |\psi_{f(j)}\rangle = |\alpha\rangle, \\ 1 & \text{if } |\psi_{f(j)}\rangle = |i\alpha\rangle, \\ 2 & \text{if } |\psi_{f(j)}\rangle = |-\alpha\rangle, \\ 3 & \text{if } |\psi_{f(j)}\rangle = |-i\alpha\rangle, \end{cases} \quad (\text{A1})$$

where m is the size of the set τ_{key} and f is a function from $[m]$ to τ_{key} .

(b) Parameter estimation. Alice and Bob perform parameter estimation by revealing all information from the rounds designated by the test set τ_{test} . To conduct this analysis, they process the data by calculating the observable measurement, conditioned on each of the four states sent by Alice. These metrics enable them to place limitations on their joint state ρ_{AB} . Subsequently, they compute the secret-key rate in accordance with the optimization problem. If their analysis indicates that secret keys cannot be produced, they terminate the protocol. Otherwise, they move forward.

(c) Reverse-reconciliation key map. Bob uses a key-map process to derive his raw key string. This map process transforms his measurement result y_k into an element within a specific set $\{0, 1, 2, 3, \perp\}$. Bob obtains his key

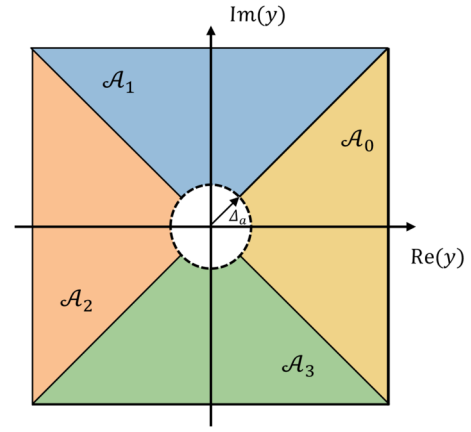


FIG. 11. Bob's key-map process for the measurement results y . Each region \mathcal{A}_z represents a key-map value j . During the postselection of data, the measurement result obtained from the central disk with a radius of Δ_a is disregarded and instead assigned the symbol \perp .

string $\mathbf{Z} = (z_1, \dots, z_m)$ according to the rule as shown in Fig. 11;

$$z_j = \begin{cases} j & \text{if } \theta \in \left[\frac{(2j-1)\pi}{4}, \frac{(2j+1)\pi}{4} \right) \text{ and } |y| \geq \Delta_a, \\ \perp & \text{otherwise,} \end{cases} \quad (\text{A2})$$

where Δ_a is a postselection parameter and $j \in \{0, 1, 2, 3\}$.

(d) Error correction and privacy amplification. Alice and Bob use privacy amplification to diminish Eve's knowledge of their shared information by eliminating certain portions of their jointly held key.

APPENDIX B: COUPLING OF TWO COHERENT STATES THROUGH A BEAM SPLITTER

Considering that coherent states $|\alpha_{A'}\rangle$ and $|\alpha_R\rangle$ are coupled through a beam splitter with transmittance η , the output coherent states are $|\alpha_{A''}\rangle$ and $|\alpha_F\rangle$. The input coherent state $|\alpha_{A'}\rangle$ can be rewritten with displacement operator $\hat{D}(\alpha_{A'})$ as

$$|\alpha_{A'}\rangle = \hat{D}(\alpha_{A'})|0\rangle_{A'}, \quad (\text{B1})$$

where

$$\hat{D}(\alpha_{A'}) = \exp\left(\alpha_{A'}\hat{\alpha}_{A'}^\dagger - \alpha_{A'}^*\hat{\alpha}_{A'}\right). \quad (\text{B2})$$

The beam-splitter operator can be expressed as

$$\hat{S}(\theta) = \exp[\theta(\hat{a}_{A'}^\dagger\hat{a}_R - \hat{a}_{A'}\hat{a}_R^\dagger)], \quad (\text{B3})$$

where θ is related to transmittance η_s by $\eta_s = 1/(1 + \tan^2 \theta)$. It can also be written in matrix form as

$$\begin{pmatrix} \hat{a}_{A''} \\ \hat{a}_F \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{a}_{A'} \\ \hat{a}_R \end{pmatrix}. \quad (\text{B4})$$

Thus, we have

$$\hat{a}_{A'} = \sqrt{\eta}\hat{a}_{A''} + \sqrt{1-\eta}\hat{a}_F. \quad (\text{B5})$$

Substitute Eqs. (B2) and (B3) into Eq. (B5)

$$\begin{aligned} \hat{S}(\eta)\tilde{D}(\alpha_{A'})\hat{S}^\dagger(\eta) &= \exp\left(\sqrt{\eta}(\alpha_{A'}\hat{a}_{A''}^\dagger - \alpha_{A'}^*\hat{a}_{A''})\right) \\ &\times \exp\left(\sqrt{1-\eta}(\alpha_{A'}\hat{a}_F^\dagger - \alpha_{A'}^*\hat{a}_F)\right). \end{aligned} \quad (\text{B6})$$

Let $\hat{A} = \alpha_{A'}\hat{a}_{A''}^\dagger - \alpha_{A'}^*\hat{a}_{A''}$ and $\hat{B} = \alpha_{A'}\hat{a}_F^\dagger - \alpha_{A'}^*\hat{a}_F$. The commutator between \hat{A} and \hat{B} can be calculated as

$$[\hat{A}, \hat{B}] = [\alpha_{A'}\hat{a}_{A''}^\dagger - \alpha_{A'}^*\hat{a}_{A''}, \alpha_{A'}\hat{a}_F^\dagger - \alpha_{A'}^*\hat{a}_F] = 0. \quad (\text{B7})$$

Using the Baker–Campbell–Hausdorff formula, we obtain

$$\begin{aligned} \hat{S}(\eta)\hat{D}_{A'}(\alpha_{A'})\hat{S}(\eta)^\dagger &= \exp\left(\sqrt{\eta}\hat{A}\right)\exp\left(\sqrt{1-\eta}\hat{B}\right) \\ &= \exp\left(\sqrt{\eta}(\alpha_{A'}\hat{a}_{A''}^\dagger - \alpha_{A'}^*\hat{a}_{A''})\right) \\ &\times \exp\left(\sqrt{1-\eta}(\alpha_{A'}\hat{a}_F^\dagger - \alpha_{A'}^*\hat{a}_F)\right), \\ &= \hat{D}_{A''}(\sqrt{\eta}\alpha_{A'})\hat{D}_F(\sqrt{1-\eta}\alpha_{A'}). \end{aligned} \quad (\text{B8})$$

Therefore, after the coherent state $|\alpha_{A'}\rangle$ passes through the beam splitter,

$$\begin{aligned} |\alpha_{A'}\rangle &\rightarrow \tilde{D}_{A''}(\sqrt{\eta}\alpha_{A'})\tilde{D}_F(\sqrt{1-\eta}\alpha_{A'})|0\rangle_{A'} \\ &= |\sqrt{\eta}\alpha_{A'}\rangle_{A''} |\sqrt{1-\eta}\alpha_{A'}\rangle_F. \end{aligned} \quad (\text{B9})$$

Similarly,

$$|\alpha_R\rangle \rightarrow |\sqrt{1-\eta}\alpha_R\rangle_{A''} |-\sqrt{\eta}\alpha_R\rangle_F. \quad (\text{B10})$$

Thus, we can obtain the output quantum state as

$$|\alpha_{A''}\rangle = |\sqrt{\eta}\alpha_{A'} + \sqrt{1-\eta}\alpha_R\rangle_{A''}. \quad (\text{B11})$$

APPENDIX C: OPTIMIZATION OF SECRET-KEY RATE

The secret-key-rate-optimization method is based on Ref. [51]. Given annihilation operator \hat{a} and creation operator \hat{a}^\dagger satisfying the basic commutation relation $[\hat{a}, \hat{a}^\dagger] =$

1, the quadrature operators \hat{q} and \hat{p} are defined as

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \quad \hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}). \quad (\text{C1})$$

Next, we discuss how to calculate the secret-key rate of the protocol with the imperfect-source model based on the entanglement-based scheme. The Devetak–Winter formula can be rewritten in the form [38]

$$R^\infty = \min_{\rho_{AB} \in \mathcal{S}} D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}[\mathcal{G}(\rho_{AB})]) - p_{\text{pass}}\delta_{\text{EC}}, \quad (\text{C2})$$

where \mathcal{G} is a CPTP map that outlines several classical post-processing procedures of the protocol, \mathcal{Z} is a pinching quantum channel that is used to access results of the key map, $D(\rho || \sigma) = \text{Tr}(\rho \log_2 \rho) - \text{Tr}(\rho \log_2 \sigma)$ is the quantum relative entropy between the quantum states ρ and σ , and \mathcal{S} is the set of density matrices satisfying experimental constraints. The key of the problem lies in the first term of the formula—namely, the optimization problem $\min_{\rho_{AB} \in \mathcal{S}} D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}[\mathcal{G}(\rho_{AB})])$. The optimization problem can be expressed as

$$\begin{aligned} \text{minimize} \quad & \min_{\rho_{AB} \in \mathcal{S}} D(\mathcal{G}(\rho_{AB}) || \mathcal{Z}[\mathcal{G}(\rho_{AB})]) \\ \text{subject to} \quad & \begin{cases} \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{F}_Q)] = p_x \langle \hat{F}_Q \rangle_x, \\ \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{F}_P)] = p_x \langle \hat{F}_P \rangle_x, \\ \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{S}_Q)] = p_x \langle \hat{S}_Q \rangle_x, \\ \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{S}_P)] = p_x \langle \hat{S}_P \rangle_x, \\ \text{Tr}[\rho_{AB}] = 1, \\ \text{Tr}_B[\rho_{AB}] = \rho_A, \end{cases} \end{aligned} \quad (\text{C3})$$

where index $x \in \{0, 1, 2, 3\}$, and $\langle \hat{F}_Q \rangle$, $\langle \hat{F}_P \rangle$, $\langle \hat{S}_Q \rangle$, and $\langle \hat{S}_P \rangle_x$ are expectation values of operators \hat{F}_Q , \hat{F}_P , \hat{S}_Q , and \hat{S}_P for the conditional state ρ_B^x respectively. The observable operators are

$$\begin{aligned} \hat{F}_Q &= \int \frac{y + y^*}{\sqrt{2}} G_y d^2 y, \\ \hat{F}_P &= \int \frac{i(y^* - y)}{\sqrt{2}} G_y d^2 y, \\ \hat{S}_Q &= \int \left(\frac{y + y^*}{\sqrt{2}} \right)^2 G_y d^2 y, \\ \hat{S}_P &= \int \left[\frac{i(y^* - y)}{\sqrt{2}} \right]^2 G_y d^2 y. \end{aligned} \quad (\text{C4})$$

In addition, in the last constraint, ρ_A is calculated as Eq. (15). To perform postselection, the region operators are

defined as

$$R_z = \int_{y \in \mathcal{A}_z} G_y d^2 y, \quad (\text{C5})$$

where \mathcal{A}_z is the region of integration corresponding to the regions shown in Fig. 11. For reverse reconciliation, the CPTP map $\mathcal{G}(\sigma) = K\sigma K^\dagger$ with input state σ , where K is the Kraus map as

$$K = \sum_{z=0}^3 |z\rangle_R \otimes I_A \otimes (\sqrt{R_z})_B. \quad (\text{C6})$$

The pinching quantum channel is described by

$$\mathcal{Z}(\sigma) = \sum_{j=0}^3 (|j\rangle\langle j|_R \otimes I_{AB}) \sigma (|j\rangle\langle j|_R \otimes I_{AB}). \quad (\text{C7})$$

For the second term of the secret-key-rate formula, p_{pass} is the sifting probability and δ_{EC} is the cost of error correction. This part is classical and computable. For the reverse-reconciliation scheme, The cost of error correction δ_{EC} can be described as

$$\delta_{\text{EC}} = H(\mathbf{Z}) - \beta I(\mathbf{X}; \mathbf{Z}), \quad (\text{C8})$$

where $H(\mathbf{Z})$ represents the classical information entropy of the raw key \mathbf{Z} , β signifies the reconciliation efficiency, and $I(\mathbf{X}; \mathbf{Z})$ denotes the classical mutual information. To sum up, the optimization problem can be solved, subsequently enabling derivation of the secret-key rate.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, USA, 1984), p. 175.
- [2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [4] C. Portmann and R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.* **94**, 025008 (2022).
- [5] T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* **61**, 010303(R) (1999).
- [6] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [7] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum cryptography without switching, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [8] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: Past, present, and future, *Appl. Phys. Rev.* **11**, 011318 (2024).
- [9] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, *Phys. Rev. Lett.* **114**, 070501 (2015).
- [10] A. Leverrier, Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction, *Phys. Rev. Lett.* **118**, 200501 (2017).
- [11] S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks, *Phys. Rev. Res.* **3**, 043014 (2021).
- [12] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, *Phys. Rev. Lett.* **125**, 010502 (2020).
- [13] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, *Optica* **9**, 492 (2022).
- [14] A. A. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator, *Sci. Adv.* **10**, eadi9474 (2024).
- [15] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, *et al.*, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, *Nat. Photonics* **13**, 839 (2019).
- [16] L. Li, T. Wang, X. Li, P. Huang, Y. Guo, L. Lu, L. Zhou, and G. Zeng, Continuous-variable quantum key distribution with on-chip light sources, *Photonics Res.* **11**, 504 (2023).
- [17] A. A. E. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver, *Optica* **11**, 1197 (2024).
- [18] Y. Bian, Y. Li, X. Xu, T. Zhang, Y. Pan, W. Huang, S. Yu, L. Zhang, Y. Zhang, and B. Xu, Highly stable power control for chip-based continuous-variable quantum key distribution system, *Opt. Lett.* **49**, 2521 (2024).
- [19] Y. Bian, Y. Pan, X. Xu, L. Zhao, Y. Li, W. Huang, L. Zhang, S. Yu, Y. Zhang, and B. Xu, Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip, *Appl. Phys. Lett.* **124**, 174001 (2024).
- [20] S. Du, P. Wang, J. Liu, Y. Tian, and Y. Li, Continuous variable quantum key distribution with a shared partially characterized entangled source, *Photonics Res.* **11**, 463 (2023).
- [21] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, High-rate point-to-multipoint quantum key distribution using coherent states, *ArXiv:2302.02391*.
- [22] A. A. Hajomer, I. Derkach, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, Continuous-variable quantum passive optical network, *ArXiv:2402.16044*.
- [23] Y. Pan, Y. Bian, Y. Li, X. Xu, L. Ma, H. Wang, Y. Luo, J. Dou, Y. Pi, J. Yang, *et al.*, High-rate 16-node quantum access network based on passive optical network, *ArXiv:2403.02585*.
- [24] 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).
- [25] Z. Li, Y.-C. Zhang, and H. Guo, User-defined quantum key distribution, [ArXiv:1805.04249](https://arxiv.org/abs/1805.04249).
- [26] 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).
- [27] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, *Phys. Rev. X* **9**, 041064 (2019).
- [28] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, Finite-size security of continuous-variable quantum key distribution with digital signal processing, *Nat. Commun.* **12**, 1 (2021).
- [29] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian quantum states, *Phys. Rev. Lett.* **96**, 080502 (2006).
- [30] R. García-Patrón and N. J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [31] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian attacks in continuous-variable quantum cryptography, *Phys. Rev. Lett.* **97**, 190502 (2006).
- [32] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, *Phys. Rev. A* **86**, 032309 (2012).
- [33] A. Denys, P. Brown, and A. Leverrier, Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation, *Quantum* **5**, 540 (2021).
- [34] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, *et al.*, Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area, *Commun. Phys.* **5**, 162 (2022).
- [35] Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system, *Opt. Lett.* **47**, 3307 (2022).
- [36] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres, *Opt. Lett.* **47**, 3948 (2022).
- [37] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, Shaped constellation continuous variable quantum key distribution: Concepts, methods and experimental validation, *J. Light. Technol.* **44**, 5182 (2024).
- [38] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Numerical approach for unstructured quantum key distribution, *Nat. Commun.* **7**, 11712 (2016).
- [39] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* **2**, 77 (2018).
- [40] W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance, *PRX Quantum* **2**, 040334 (2021).
- [41] T. Upadhyaya, T. van Himbeek, J. Lin, and N. Lütkenhaus, Dimension reduction in quantum key distribution for continuous-and discrete-variable protocols, *PRX Quantum* **2**, 020325 (2021).
- [42] F. Kanitschar and C. Pacher, Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection, *Phys. Rev. Appl.* **18**, 034073 (2022).
- [43] Y. Tian, Y. Zhang, S. Liu, P. Wang, Z. Lu, X. Wang, and Y. Li, High-performance long-distance discrete-modulation continuous-variable quantum key distribution, *Opt. Lett.* **48**, 2953 (2023).
- [44] F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols, *PRX Quantum* **4**, 040306 (2023).
- [45] S. Bäuml, C. P. García, V. Wright, O. Fawzi, and A. Acín, Security of discrete-modulated continuous-variable quantum key distribution, [ArXiv:2303.09255](https://arxiv.org/abs/2303.09255).
- [46] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [47] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations, *Adv. Quantum Technol.* **1**, 1800011 (2018).
- [48] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, *et al.*, Quantum key distribution over 25 km with an all-fiber continuous-variable system, *Phys. Rev. A* **76**, 042305 (2007).
- [49] 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).
- [50] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: A threat and a defense, *Entropy* **18**, 20 (2016).
- [51] J. Lin and N. Lütkenhaus, Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution, *Phys. Rev. Appl.* **14**, 064030 (2020).
- [52] L. Fan, Y. Bian, M. Wu, Y. Zhang, and S. Yu, Quantum hacking against discrete-modulated continuous-variable quantum key distribution using modified local oscillator intensity attack with random fluctuations, *Phys. Rev. Appl.* **20**, 024073 (2023).
- [53] V. C. Usenko and R. Filip, Feasibility of continuous-variable quantum key distribution with noisy coherent states, *Phys. Rev. A* **81**, 022318 (2010).
- [54] Y. Shen, X. Peng, J. Yang, and H. Guo, Continuous-variable quantum key distribution with Gaussian source noise, *Phys. Rev. A* **83**, 052304 (2011).
- [55] Y. Shen, J. Yang, and H. Guo, Security bound of continuous-variable quantum key distribution with noisy

- coherent states and channel, *J. Phys. B: At. Mol. Opt. Phys.* **42**, 235506 (2009).
- [56] J. Yang, B. Xu, and H. Guo, Source monitoring for continuous-variable quantum key distribution, *Phys. Rev. A* **86**, 042314 (2012).
- [57] B. Chu, Y. Zhang, Y. Huang, S. Yu, Z. Chen, and H. Guo, Practical source monitoring for continuous-variable quantum key distribution, *Quantum Technol.* **6**, 025012 (2021).
- [58] L. Ma, J. Yang, T. Zhang, Y. Shao, J. Liu, Y. Luo, H. Wang, W. Huang, F. Fan, C. Zhou, *et al.*, Practical continuous-variable quantum key distribution with feasible optimization parameters, *Sci. China Inf. Sci.* **66**, 180507 (2023).