Discrete-modulation continuous-variable quantum key distribution with high key rate

Pu Wang,1 Jianqiang Liu,1 Zhenguo Lu,1 Xuyang Wang,1,2 and Yongmin Li1,2

1State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, People’s Republic of China
2Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, People’s Republic of China

(Dated: October 1, 2021)

Discrete-modulation continuous-variable quantum key distribution has the potential for large-scale deployment in the secure quantum communication networks due to low implementation complexity and compatibility with the current telecom systems. The security proof for four coherent states phase-shift keying (4-PSK) protocol has recently been established by applying numerical methods. However, the achievable key rate is relatively low compared with the optimal Gaussian modulation scheme. To enhance the key rate of discrete-modulation protocol, we first show that 8-PSK increases the key rate by about 60% in comparison to 4-PSK, whereas the key rate has no significant improvement from 8-PSK to 12-PSK. We then expand the 12-PSK to two-ring constellation structure with four states in the inner ring and eight states in the outer ring, which significantly improves the key rate to be 2.4 times of that of 4-PSK. The key rate of the two-ring constellation structure can reach 70% of the key rate achieved by Gaussian modulation in long distance transmissions, making this protocol an attractive alternative for high-rate and low-cost application in secure quantum communication networks.

I. INTRODUCTION

Quantum key distribution (QKD)1,2, as one of the most prominent application of quantum information sciences, allows two distant parties to share a common secret key, where the security is guaranteed by the fundamental laws of quantum physics3,4. Continuous-variable (CV) QKD encodes the key information into continuous-spectrum quantum observables, such as the quadratures components of the light field, which has the potential to offer larger key rates at metropolitan distances5–8. CV-QKD can employ the similar components as classical telecom systems and has received extensive attentions and witnessed rapid development both theoretically and experimentally9–35.

At present, most of the CV-QKD schemes are based on Gaussian modulation, meaning that Alice displaces the quadratures of the sent states according to a Gaussian distribution, which reaches the channel capacity and compatibility with the current telecom systems. The security proof for four coherent states phase-shift keying (4-PSK) protocol has recently been established by applying numerical methods. However, the achievable key rate is relatively low compared with the optimal Gaussian modulation scheme. To enhance the key rate of discrete-modulation protocol, we first show that 8-PSK increases the key rate by about 60% in comparison to 4-PSK, whereas the key rate has no significant improvement from 8-PSK to 12-PSK. We then expand the 12-PSK to two-ring constellation structure with four states in the inner ring and eight states in the outer ring, which significantly improves the key rate to be 2.4 times of that of 4-PSK. The key rate of the two-ring constellation structure can reach 70% of the key rate achieved by Gaussian modulation in long distance transmissions, making this protocol an attractive alternative for high-rate and low-cost application in secure quantum communication networks.

1,2

In this paper, we focus on the design of the optimized discrete-modulation protocol. To this end, we first extend the 4-PSK protocol to more signal states, eight states (8-PSK) and twelve states (12-PSK), and derive the asymptotic secure key rate by numerical methods considering the realistic trusted noisy detection. The results show that 8-PSK increases the key rate by about 60%, compared with the original 4-PSK protocol, while the key rate has only small improvement from 8-PSK to 12-PSK. This is because the performance of 8-PSK has tended to be saturated for a single-ring constellation protocol, and further increasing the number of states would not gain more advantages. To enlarge the distribution range of states in phase space and further improve the performance, we propose to use the two-ring constellation scheme, where not only the phase quadrature but the amplitude quadrature is modulated. By optimizing the amplitudes and the probabilities assigned to each states,
and the boundary between the two rings, the two-ring constellation with twelve states (four states in the inner ring and eight states in the outer ring) get a superior performance. In comparison with the original 4-PSK protocol, the secret key rate is increased to 2.4 times. This value is about 70% of the key rate achievable for Gaussian modulation and therefore the performance of the two-ring constellation protocol is close to the Gaussian modulation protocol, but the implementation is simpler, which makes it very attractive for practical applications.

The rest of the paper is organized as follows. In Sec. II, we analyze the performance of discrete-modulation protocol of 8-PSK and 12-PSK with single-ring constellation. In Sec. III, we apply the two-ring constellation structure to 12-PSK, and investigate the dependence of key rate on various parameters to optimize the protocol. The results are compared with Gaussian modulation CV-QKD protocol under realistic trusted noisy detection. Our conclusions are drawn in Sec. IV.

II. DISCRETE-MODULATION CV-QKD WITH SINGLE-RING CONSTELLATION

A. The protocol description

The schematic of single-ring signal constellation for discrete-modulation CV-QKD of 8-PSK and 12-PSK is illustrated in Fig. 1. For 8-PSK, the sender Alice prepares the coherent state \( |\alpha_x\rangle = |\alpha e^{ix\pi/4}\rangle \) with \( x \in \{0, 1, 2, 3, 4, 5, 6, 7\} \), each coherent state is chosen with an equal probability \( p_x = 1/8 \). Similarly, for 12-PSK, Alice randomly selects a state from the set \( \{|\alpha_x\rangle = |\alpha e^{ix\pi/6}\rangle, \ x = 0, \cdots, 11\} \), where \( \alpha \) is a predetermined amplitude and can be optimized. The prepared states are sent to Bob through an insecure quantum channel to generate secret keys. Bob measures the received states with heterodyne detection and records the measurement outcome \( y \in \mathbb{C} \).

If the parameter estimation passes, they use the remaining string by a key map. Specifically, Bob labels each outcome \( y = |y\rangle e^{i\theta} \) according to the region \( R_j \) as

\[
z = \begin{cases} 
  j, \text{if } \theta \in \left(\frac{(2j-1)\pi}{8}, \frac{(2j+1)\pi}{8}\right) & \Rightarrow \ y \in R_j, \ 8\text{-PSK} \\
  j, \text{if } \theta \in \left(\frac{(2j-1)\pi}{12}, \frac{(2j+1)\pi}{12}\right) & \Rightarrow \ y \in R_j, \ 12\text{-PSK}
\end{cases}
\]

(1)

where \( j \in \{0, \cdots, 7\} \) for 8-PSK and \( j \in \{0, \cdots, 11\} \) for 12-PSK. The raw key string of Alice consists of the label \( x \) of her randomly selected state \( \alpha_x \). Finally, Alice and Bob implement error correction and privacy amplification procedures to extract secret keys.

B. Secret key rate

For convenience of security analysis, we consider the equivalent entanglement-based (EB) scheme. Here, we mainly use the numerical security proof method presented in Ref. [43, 54] to obtain the secure key rate. In the EB scheme, Alice initially prepares the bipartite state

\[
|\psi\rangle_{AA'} = \sum_x \sqrt{p_x}|x\rangle_A \langle x|_{A'},
\]

(2)

where \( |x\rangle \) is an orthonormal basis for register \( A \). Alice keeps \( A \) and sends the register \( A' \) to Bob. To establish the equivalence between the EB scheme and the original prepare-and-measure scheme, Alice applies a local projective measurement on register \( A \), which can be described by a POVM \( M^A = \{M^A_x = |x\rangle \langle x|\} \). When obtaining a measurement outcome \( x \) with probability \( p_x \), the state sent to Bob is effectively collapsed to \( |\alpha_x\rangle \). After the quantum channel transmission, the joint state shared by Alice and Bob is

\[
\rho_{AB} = (\text{id}_A \otimes \mathcal{E}_{A' \rightarrow B})(|\psi\rangle \langle \psi|_{AA'}),
\]

(3)

where \( \text{id}_A \) is the identity channel acting on \( A \) and \( \mathcal{E}_{A' \rightarrow B} \) describes the quantum channel, which is a completely positive and trace-preserving (CPTP) map. Bob uses his POVM \( G_y \) on register \( B \) to perform realistic trusted noisy detection.

With the reverse reconciliation, the asymptotic secret key rate against collective attacks is expressed as [49]

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

(4)

where \( D(\rho||\sigma) = \text{Tr}(\rho \log_2 \rho) - \text{Tr}(\rho \log_2 \sigma) \) is the quantum relative entropy; \( \mathcal{G} \) describes a completely positive and trace nonincreasing map for postprocessing steps; \( \mathcal{Z} \) denotes a pinching quantum channel that reads out the result of key map; \( \mathcal{S} \) represents the set of available density operators compatible with experimental observations; \( p_{\text{pass}} \) is the sifting probability of data for key generation; \( \delta_{\text{EC}} \) stands for the leaked information of per
signal pulse during the error correction phase and can be computed as follows
\[
\delta_{EC} = H(Z) - \beta I(X;Z) = (1 - \beta) H(Z) + \beta H(Z|X),
\]
where \(\beta\) is the reconciliation efficiency. \(X\) and \(Z\) represent the raw key string of Alice and Bob, respectively.

In order to compute the expected secret key rate, the key point is to find the minimum value of \(D(G(\rho_{AB})\|Z[G(\rho_{AB})])\), which is a convex optimization problem matching some constraints and expressed as
\[
\text{minimize } D(G(\rho_{AB})\|Z[G(\rho_{AB})])
\]
subject to
\[
\begin{align*}
\text{Tr} \left[ \rho_{AB} \left( |x\rangle \langle x|_A \otimes \hat{F}_Q \right) \right] &= p_x \langle \hat{F}_Q \rangle_x, \\
\text{Tr} \left[ \rho_{AB} \left( |x\rangle \langle x|_A \otimes \hat{F}_P \right) \right] &= p_x \langle \hat{F}_P \rangle_x, \\
\text{Tr} \left[ \rho_{AB} \left( |x\rangle \langle x|_A \otimes \hat{S}_Q \right) \right] &= p_x \langle \hat{S}_Q \rangle_x, \\
\text{Tr} \left[ \rho_{AB} \left( |x\rangle \langle x|_A \otimes \hat{S}_P \right) \right] &= p_x \langle \hat{S}_P \rangle_x, \\
\text{Tr} [\rho_{AB}] &= 1, \\
\rho_{AB} &\geq 0,
\end{align*}
\]
where \(\hat{F}_Q\) and \(\hat{F}_P\) (\(\hat{S}_Q\) and \(\hat{S}_P\)) represent the first-moment (second-moment) observables of quadrature operators \(\hat{q}\) and \(\hat{p}\), respectively. Also notice that Eve cannot access Alice’s system, thus there is an additional constraint
\[
\text{Tr}_B [\rho_{AB}] = \rho_A = \sum_{i,j=0}^{n} \sqrt{p_ip_j} (\alpha_j|\alpha_i\rangle \langle i| \langle j|_A),
\]
where \(n\) takes 7 or 11 according to 8-PSK or 12-PSK.

The postprocessing map \(\mathcal{G}\) and pinching quantum channel \(Z\) can be written as
\[
\begin{align*}
\mathcal{G}(\sigma) &= K\sigma K^\dagger, \\
K &= \sum_{z=0}^{n} |z\rangle_R \otimes I_A \otimes \left(\sqrt{R_z}\right)_B, \\
Z(\sigma) &= \sum_{j=0}^{n} (|j\rangle \langle j|_R \otimes I_{AB}) \sigma (|j\rangle \langle j|_R \otimes I_{AB}).
\end{align*}
\]

To numerically minimize the objective function, available \(\rho_{AB}\) must be a finite dimension. The dimension of Alice’s system is determined by the number of different signal states that she prepares, which is finite. However the receiver Bob’s state is in an infinite dimensional Hilbert space. This can be circumvented by applying the photon-number cutoff assumption. When the photon number cutoff parameter \(N_c\) is chosen to be large enough, this assumption is reasonable. Here, we set an appropriate parameter value of \(N_c\) such that the probability of photon number of the received signal state smaller than \(N_c\) is close to 1, and larger \(N_c\) has no meaningful improvement for the key rate. Then, the matrix expressions of the first-moment observables \(\hat{F}_Q, \hat{F}_P, \hat{S}_Q, \hat{S}_P, \) and the region operators \(R_j\) in the photon-number basis can be obtained

A tight lower bound on the key rate can be achieved by using a two-step procedure developed in Ref. \[51\]. At the first step, the Frank-Wolfe algorithm is used to approximately minimize the convex function, and hence obtaining an upper bound on the key rate. At the second step, converting this upper bound to a reliable lower bound by taking the numerical imprecision into account. By using the two-step procedure and defining
\[
\min_{\rho \in \mathcal{S}} f(\rho) = f(\rho) - \text{Tr} (\rho \hat{F}_Q f(\rho)) + f_{d_{max}} - \zeta_e, 
\]
where \(\rho_1\) is the suboptimal state obtained in the first step. \(\epsilon\) is the perturbation parameter and \(f_{d_{max}} := D(\mathcal{G}_c(\rho_1)||Z[\mathcal{G}_c(\rho_1)])\). \(\zeta_e = 2\epsilon (d' - 1) \log_2 \frac{d'}{d' - 1}\), where \(d'\) is the dimension of \(\mathcal{G}(\rho)\). The gradient \(\nabla f(\rho_1)\) is given by
\[
\nabla f(\rho_1)^T = \mathcal{G}_c^\dagger (\log_2 \mathcal{G}_c(\rho_1)) - \mathcal{G}_c^\dagger (\log_2 Z[\mathcal{G}_c(\rho_1)]).
\]

\(f_{d_{max}}\) is the dual function and written as
\[
f_{d_{max}}(\epsilon, \mathcal{S}) = \max_{(\bar{v}, \mathcal{S})} \left( \bar{v} \cdot \epsilon - \epsilon \sum_{i=1}^{nc} s_i \right)
\]
subject to
\[
-\bar{s} \leq \bar{v} \leq \bar{s},
\]
\[
\sum_{i=1}^{nc} v_i \Gamma_i \leq \nabla f(\rho_1),
\]
where \(\Gamma_i\) and \(\gamma_i\) refer to both sides of the equality constraint, respectively, with the form \(\text{Tr}(\Gamma_i \rho) = \gamma_i\). \(nc\) represents the number of all constraints. \(\epsilon'\) is the security parameter related to the numerical imprecision.

We are now in a position to assess the performance of the protocol based on the above approach.

C. Performance analysis

Considering a typical phase-insensitive Gaussian channel in the context of the optical fiber communication. The simulated statistics are given by
\[
\begin{align*}
\langle \hat{F}_Q \rangle_x &= \sqrt{2\eta T} \text{Re}(\alpha_x), \\
\langle \hat{F}_P \rangle_x &= \sqrt{2\eta T} \text{Im}(\alpha_x), \\
\langle \hat{S}_Q \rangle_x &= 2\eta T \text{Re}(\alpha_x)^2 + 1 + \frac{1}{2} \eta T \xi + v_e, \\
\langle \hat{S}_P \rangle_x &= 2\eta T \text{Im}(\alpha_x)^2 + 1 + \frac{1}{2} \eta T \xi + v_e,
\end{align*}
\]
where $T$ and $\xi$ represent the transmittance and excess noise of the channel, respectively, and $\eta$ and $v_\text{el}$ denote the detection efficiency and electronic noise of the detector.

The probability density function for the result $y$ of a heterodyne measurement conditioned on Alice’s choice $x$ is

$$P(y|x) = \frac{1}{\pi(1 + \frac{1}{2}\eta T \xi + v_\text{el})} \exp \left[-\frac{|y - \sqrt{\eta T} \xi_0|^2}{1 + \frac{1}{2}\eta T \xi + v_\text{el}} \right].$$

(13)

Then, according to the key mapping area, the probability that Bob obtains the discretized key value $Z = z$ conditioned on Alice’s choice $x$ is

$$\tilde{P}(z|x) = \left\{ \begin{array}{ll}
\int_0^\infty rdr \int_{(2z-1)\pi/8}^{(2z+1)\pi/8} P(re^{i\theta}|x) d\theta & \text{(8-PSK)} \\
\int_0^\infty rdr \int_{(2z-1)\pi/12}^{(2z+1)\pi/12} P(re^{i\theta}|x) d\theta & \text{(12-PSK)}
\end{array} \right..$$

(14)

To extract the optimal secret key rate and fairly compare the performance of different protocols, we first investigate the dependence of the key rate on the coherent state amplitude $\alpha$. In Fig. 2(a), we plot the key rate versus the choice of $\alpha$ for 8-PSK and 12-PSK protocols, at a transmission distance of 50 km. Here, we consider the realistic parameters: reconciliation efficiency $\beta = 0.95$, excess noise $\xi = 0.01$, detection efficiency $\eta = 0.552$, and electronic noise $v_\text{el} = 0.015$. The dashed line represents the result of step 1 of our algorithm, which gives an upper bound on the key rate, and solid line is the result after step 2, which provides an achievable lower secure bound on the key rate. The gap between step 1 and step 2 is small, hence the obtained bound is tight. We carry out a coarse-grained search for $\alpha$ in the interval $[0.7, 1.1]$ with a step size of 0.05. It is clear that there is an optimal value of $\alpha$ to maximize the key rate. At 50 km, the optimal $\alpha$ for 8-PSK and 12-PSK is 0.9 and 0.92, respectively. In Fig. 2(b), we give the optimal values of $\alpha$ at different transmission distances and the results of 4-PSK protocol are also shown for comparison. Compared with the 4-PSK protocol, 8-PSK allows larger optimal value of $\alpha$, thus providing higher signal-to-noise ratio (SNR). The difference between the optimal $\alpha$ for the 8-PSK and 12-PSK protocols gradually decreases with the increase of transmission distance and is almost indistinguishable over long distances.

In Fig. 3 we present the achievable key rates at different transmission distances for different discrete-modulation protocols and Gaussian modulation protocol. The key rate has been optimized by adopting the optimal modulation amplitude (Fig. 2(b)) and variance. In addition, we have applied the postselection technology to the 4-PSK protocol to obtain the optimal key rate $50$. We can see that the 8-PSK protocol improves the key rate by about 60% over the 4-PSK protocol. Within 10 km, the key rate can be further improved by 10% - 30% if 12-PSK is employed. However, beyond 10 km, the key rate can only be increased by about 4%, which means that the performance of 8-PSK modulation is close to saturation and adding more signal states will not make much difference. Compared with the Gaussian-modulation protocol, the achievable key rate of discrete-modulation is still relatively low. Taking 50 km as an example, the key rates per pulse of the 4-PSK, 8-PSK, 12-PSK and Gaussian modulation protocols are 0.00602, 0.00966, 0.01008, and 0.02103 bits/pulse, respectively. The 4-PSK and 8-PSK protocols can reach approximately 28% and 45% of the key rate of Gaussian modulation. The data postselection is also an interesting strategy to further improve the key rate by 8% for 8-PSK and 12-PSK protocols (see Appendix).
The dependence of key rate on these parameters are compared with two different amplitudes $\alpha_1 = 1.6$, $\alpha_2 = 0.85$, $p_1 = 7/48$ and $p_2 = 5/96$. In this case, we achieve a key rate of 0.01459 bits/pulse, which is 50% higher than that of 8-PSK protocol and 140% higher than that of 4-PSK protocol. By varying the constellation geometry from the single-ring PSK structure to the two-ring constellation structure, we effectively overcomes the limitation of states distribution in phase space, and significantly improves the performance of the 4-PSK discrete-modulation protocol.

In Fig. 6 we give the optimal choice of parameters $\alpha_1$, $\alpha_2$, $\alpha_c$ and $p_1$ at different transmission distances. The cutoff value of photon number $N_c$ is selected from the interval [14, 22] according to the modulation amplitudes. The optimal $p_1$ is obtained via a coarse-grained search in the interval $[1/48, 11/48]$ with a step size $1/48$. We can see that the optimal $\alpha_c$ is closer to $\alpha_1$ and $p_1$ is greater than $p_2$, which result in an approximate Gaussian distribution in phase space. Next, we employ the optimal parameters values to obtain the optimal key rate and analyze the performance of the protocol.

In Fig. 7 we compare the key rate of the two-ring constellation protocol with the previous PSK protocols and Gaussian modulation protocol. We observe that the key rate of the two-ring constellation with twelve states is higher than that of PSK protocols, and the gap of the key rate between two-ring constellation protocol and Gaussian modulation protocol decreases gradually with the increase of transmission distance. As shown in Fig. 8 for long distance transmission distance above 50 km, the two-ring constellation with twelve states can reach above 70% of key rate of Gaussian modulation protocol. Notice that two-ring constellation with twelve states require only 1-bit discretization for the amplitude of the light field and 3-bit discretization for the phase of the light field. Therefore, we proof that the concise two-ring constellation with
FIG. 5. Secure key rate versus the choices of $\alpha_1$, $\alpha_2$, $\alpha_c$, and $p_1$. The simulation parameters are $\beta = 0.95$, $\xi = 0.01$, $\eta = 0.552$, $\nu_{el} = 0.015$, and $L = 50$ km. (a) The optimal $\alpha_1$ is obtained via a coarse-grained search in the interval $[0.5, 0.9]$ with a step size 0.05. The other parameters are set to $\alpha_2 = 1.6$, $\alpha_c = 0.85$, and $p_1 = 7/48$. (b) The value of $\alpha_2$ is changed with a step size 0.05 in the interval $[1.45, 1.85]$. The other parameters are set to $\alpha_1 = 0.7$, $\alpha_c = 0.85$, $p_1 = 7/48$. (c) The value of $\alpha_c$ is changed with a step size 0.05 in the interval $[0.75, 1.1]$. The other parameters are set to $\alpha_1 = 0.7$, $\alpha_2 = 1.6$, $p_1 = 7/48$. (d) The value of $p_1$ is searched in the interval $[4/48, 11/48]$ with a step size $1/48$. The other parameters are set to $\alpha_1 = 0.7$, $\alpha_2 = 1.6$, and $\alpha_c = 0.85$.

twelve states can exhibit superior performance, which is very close to that of Gaussian modulation protocol.

IV. CONCLUSIONS

The optimized constellation design schemes were proposed to significantly improve the performance of the discrete-modulation CV-QKD protocol. The asymptotic secure key rate in the trusted detector noise scenario is obtained by applying the advanced numerical methods. For the sake of fair comparison, we optimized the coherent state amplitude at each transmission distance. Our numerical results showed that 8-PSK can increase the key rate by about 60% over conventional 4-PSK protocol, however adding the 8-PSK to 12-PSK does not significantly improve the key rate. Interestingly, by allocating twelve coherent states to a two-ring constellation that enlarges the distribution range of coherent states in phase space, the key rate with 140% higher than that of 4-PSK protocol was achieved. This key rate reaches about 70% of that of the Gaussian modulation protocol for transmission distance above 50 km. Our results confirm that the discrete-modulation protocol with ten or so appropriate constellation and optimal modulation parameters can approximate the key rate of Gaussian modulation protocol. We believe that the proposed discrete-modulation protocol can find promising applications in high-rate and low-cost secure quantum communication networks.

The future works include the optimization of the key rate of the discrete-modulation protocol in the short distance transmission by extending current state constellation or other new constellation design schemes, finding better data postselection strategies, extending our security analysis to include the impact of finite-size is also an important future task.
FIG. 8. Ratio of the key rate of various discrete-modulation protocols to Gaussian modulation protocol. TRC represents two-ring constellation protocol with twelve states and GM represents the Gaussian modulation protocol.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (NSFC) (Grants No.11774209); the Aeronautical Science Foundation of China (20200020115001); Key Research and Development Program of Guangdong Province (2020B0303040002); Shanxi 1331KSC.

Appendix A: POSTSELECTION

In this Appendix, we apply the postselection technology to our proposed protocol. Postselection is useful to improve the key rate of the four state protocol [50]. It also reduces the amount of data for post-processing. In Fig. 9 taking the 8-PSK as an example, we illustrate the concept of postselection. There is a cut-off area at the center of the phase space, which is defined by a circle with radius $\alpha_0$. The data inside the circle is discarded and the data outside the circle is retained. Hence, the key mapping results of Bob become

$$z =\begin{cases} j, & \text{if } \theta \in \left(\frac{(2j-1)\pi}{8}, \frac{(2j+1)\pi}{8}\right) \text{ and } |y| \geq \alpha_0, \\ \perp, & \text{otherwise} \end{cases}$$

(A1)

where $\alpha_0$ is the postselection parameter, and $\alpha_0 = 0$ corresponds to the protocol without postselection.

The sifting factor is defined as $p_{\text{pass}} = \sum_{x,z} \tilde{P}(x) \tilde{P}(z|x)$, where

$$\tilde{P}(z|x) = \int_{\alpha_0}^{\infty} rdr \int_{(2z-1)\pi/8}^{(2z+1)\pi/8} P(re^{i\theta}|x) d\theta,$$

(A2)

$$\tilde{P}(x)$$ is the probability that Alice chooses to send the state $\alpha_x$.

In Fig. 10(a), we plot the key rate versus the postselection parameter $\alpha_0$ for the 8-PSK and 12-PSK protocols at the distance $L = 50$ km. We observe that there exists an optimal postselection parameter to maximize the key rate. The optimal postselection parameter value for 8-PSK and 12-PSK protocols is $\alpha_0 = 0.55$. Compared with the original protocol without postselection, the key rate is increased by 8% for both 8-PSK and 12-PSK protocols. By inserting $\alpha_0 = 0.55$ into Eq. (A2), we can obtain the value of the sifting factor $p_{\text{pass}} = 0.75$, which means that the amount of data used for post-processing is reduced by 25%.

With the similar procedure, we search for the optimal postselection parameter for the two-ring constellation protocol with twelve states, as shown in Fig. 10(b). The result suggests that the optimal value is $\alpha_0 = 0$. Therefore, we do not need to postselect the data for the two-ring constellation scheme. It should be noted that there may be other postselection strategies that can improve the performance of the protocol, which is left for future work.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M.
The modulation amplitude is set to $\alpha = 0.9$ for 8-PSK protocol and $\alpha = 0.92$ for 12-PSK protocol. (b) Secure key rate versus postselection parameter for the two-ring constellation protocol at 50 km, where the parameters value are set to $\alpha_1 = 0.7$, $\alpha_2 = 1.6$, $\alpha_v = 0.85$ and $p_1 = 7/48$. The optimal postselection parameter is obtained via a coarse-grained search for $\alpha_0$ in the interval $[0, 0.7]$ for (a) and $[0, 0.4]$ for (b) with a step size 0.05. Other parameters for simulations are set to $\beta = 0.95$, $\xi = 0.01$, $\eta = 0.552$, and $v_{cl} = 0.015$.

Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).

[3] H.-K. Lo and H.F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances, Science 283, 2050 (1999).

[4] F.-H. Xu, X.-F. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan. Secure quantum key distribution with realistic devices, Rev. Mod. Phys. 92, 025002 (2020).

[5] S.L. Braunstein and P. van Loock. Quantum information with continuous variables, Rev. Mod. Phys. 77, 513 (2005).

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

[7] E. Diamanti and A. Leverrier. Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy 17, 6072 (2015).

[8] 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. Photon. 12, 1012 (2020).

[9] T.C. Ralph. Continuous variable quantum cryptography, Phys. Rev. A 61, 010303 (1999).

[10] N.J. Cerf, M. Levy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states, Phys. Rev. A 63, 052311 (2001).

[11] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. 88, 057902 (2002).

[12] F. Grosshans, G. Van Assche, J. Wenger, R. Brouil. N.J. Cerf, and P. Grangier. Quantum key distribution using gaussian-modulated coherent states, Nature 421, 238 (2003).

[13] 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).

[14] 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).

[15] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karlov, E. Diamanti, T. Debuisscher, 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).

[16] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, Phys. Rev. A 76, 052323 (2007).

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

[18] F. Furrer, T. Franz, M. Berta, A. Leverrier, V.B. Scholz, M. Tomamichel, and R.F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks, Phys. Rev. Lett. 109, 100502 (2012).

[19] L.S. Madsen, V.C. Usenko, M. Lassen, R. Filip, and U.L. Andersen. Continuous variable quantum key distribution with modulated entangled states, Nat. Commun. 3, 1083 (2012).

[20] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics 7, 378 (2013).

[21] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R.F. Werner, and R. Schnabel. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, Nat. Commun. 6, 8795 (2015).

[22] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S.L. Braunstein, S. Lloyd, T. Gehring, C.S. Jacobsen, and U.L. Andersen. High-rate measurement-device-independent quantum cryptography, Nat. Photonics 9, 397 (2015).

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

[24] D. Huang, P. Huang, H.S. Li, T. Wang, Y.-M. Zhou, and G.-H. Zeng. Field demonstration of a continuous-variable quantum key distribution network, Opt. Lett. 41, 3511 (2016).

[25] N. Walk, S. Hosseini, J. Geng, O. Thearle, J.Y. Haw, S. Armstrong, S.M. Assad, J. Janousek, T.C. Ralph, T. Symul, et al. Experimental demonstration of gaussian protocols for one-sided device-independent quantum key distribution, Optica 3, 634 (2016).

[26] A. Leverrier. Security of continuous-variable quantum key distribution via a gaussian de finetti reduction, Phys. Rev. Lett. 118, 200501 (2017).

[27] X.-Y. Wang, W.-Y. Liu, P. Wang, and Y.-M. Li. Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution, Phys. Rev. A 95, 062330 (2017).

[28] F. Furrer and W.J. Munro. Repeaters for continuous-variable quantum communication, Phys. Rev. A 98, 032335 (2018).

[29] F. Karinou, H.H. Brunner, C.F. Fung, L.C. Comandar, S. Betteli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, and E. Diamanti. Gaussian modulated coherent-state quantum key distribution, Nat. Photonics 13, 726 (2009).
D. Wang, C. Xie, et al., Toward the integration of cv quantum key distribution in deployed optical networks, IEEE Photonics Technol. Lett. **30**, 650 (2018).

[30] N. Wang, S.-N. Du, W.-Y. Liu, X.-Y. Wang, Y.-M. Li, and K.-C. Peng, Long-distance continuous-variable quantum key distribution with entangled states, Phys. Rev. Appl. **10**, 064028 (2018).

[31] Y.-C. Zhang, Z.-Y. Li, Z.-Y. Chen, C. Weedbrook, Y.-J. Zhao, X.-Y. Wang, Y.-D. Huang, C.-C. Xu, X.-X. Zhang, Z.-Y. Wang, et al., Continuous-variable qkd over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[32] S.-N. Du, Y. Tian, and Y.-M. Li, Impact of four-wave-mixing noise from dense wavelength-division-multiplexing systems on entangled-state continuous-variable quantum key distribution, Phys. Rev. Appl. **14**, 024013 (2020).

[33] B. Qi, H. Günther, P.G. Evans, B.P. Williams, R.M. Camacho, and N.A. Peters, Experimental passive-state preparation for continuous-variable quantum communications, Phys. Rev. Appl. **13**, 054065 (2020).

[34] Y.-C. Zhang, Z.-Y. Chen, S. Pirandola, X.-Y. Wang, C. Zhou, B.-J. Chu, Y.-J. Zhao, B.-J. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.51 km of fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[35] D. Dequal, L. Trigo Vidarte, V. Roman Rodríguez, G. Vallone, P. Villoresi, A. Leverrier, and S. Pirandola, Feasibility of satellite-to-ground continuous-variable quantum key distribution, npj Quantum Inform. **7**, 3 (2021).

[36] E. Kaur, S. Guha, and M.M. Wilde, Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution, Phys. Rev. A **103**, 012412 (2021).

[37] 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).

[38] 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).

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

[40] X.-Y. Wang, Z.-L. Bai, S.-F. Wang, Y.-M. Li, and K.-C. Peng, Four-state modulation continuous-variable quantum key distribution over a 30-km fiber and analysis of excess noise, Chin. Phys. Lett. **30**, 010305 (2013).

[41] K. Brádler and C. Weedbrook, Security proof of continuous-variable quantum key distribution using three coherent states, Phys. Rev. A **97**, 022310 (2018).

[42] R. García-Patrón and N.J. Cerf, Unconditional optimality of gaussian attacks against continuous-variable qkd, Phys. Rev. Lett. **97**, 190503 (2006).

[43] M. Navascués, F. Grosshans, and A. Acín, Optimality of gaussian attacks in continuous-variable quantum cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[44] A. Leverrier and P. Grangier, Simple proof that gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation, Phys. Rev. A **81**, 062314 (2010).

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

[46] L. Trigo Vidarte, V. Roman Rodríguez, G. Vallone, P. Villoresi, A. Leverrier, and S. Pirandola, Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels, Phys. Rev. A **98**, 012340 (2018).

[47] 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).

[48] T. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, Phys. Rev. X **9**, 041064 (2019).

[49] 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).

[50] A. Winick, N. Lütkenhaus, and P.J. Coles, Reliable numerical key rates for quantum key distribution, Quantum **2**, 77 (2018).

[51] F. Jardel, T.A. Eriksson, C. Ménassé, A. Ghazisaeidi, F. Buchali, W. Idler, and J.J. Boutros, Exploring and experimenting with shaping designs for next-generation optical communications, J. Lightw. Technol. **36**, 5298 (2018).

[52] C. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous variable quantum cryptography: Beating the 3 db loss limit, Phys. Rev. Lett. **89**, 167901 (2002).

[53] H.M. Chrzanowski, N. Walk, S.M. Assad, J. Janousek, S. Hosseini, T.C. Ralph, T. Symul, and P.K. Lam, Measurement-based noiseless linear amplification for quantum communication, Nat. Photonics **8**, 333 (2014).

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

[55] D. Bunandar, L.C.G. Govia, H. Krovi, and D. Englund, Numerical finite-key analysis of quantum key distribution, npj Quantum Inform. **6**, 104 (2020).

[56] T. Matsumura, K. Maeda, T. Sasaki, and M. Koashi, Finite-size security of continuous-variable quantum key distribution with digital signal processing, Nat. Commun. **12**, 252 (2021).