IOP Publishing New J. Phys. 25 (2023) 023019 https://doi.org/10.1088/1367-2630/acb964

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
25 November 2022

REVISED
23 January 2023

ACCEPTED FOR PUBLICATION
6 February 2023

PUBLISHED
15 February 2023

PAPER

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

Pu Wang[1,2,3], **Yu Zhang**[1,2], **Zhenguo Lu**[1,2], **Xuyang Wang**[1,2] **and Yongmin Li**[1,2,*]

[1] State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, People's Republic of China
[2] Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, People's Republic of China
[3] School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, People's Republic of China
[*] Author to whom any correspondence should be addressed.

E-mail: yongmin@sxu.edu.cn

Keywords: quantum key distribution, continuous-variable, quantum cryptography, discrete-modulation, numerical method, high rate

Abstract

Discrete-modulation continuous-variable (CV) quantum key distribution has the potential for large-scale deployment in secure quantum communication networks owing to its low implementation complexity and compatibility with the current coherent optical telecommunication. However, current discrete-modulation protocols require relatively large constellation sizes to achieve a key rate comparable to that of the Gaussian modulation. Here, we show that a high key rate comparable to the Gaussian modulation can be achieved using only ten or so coherent states by implementing suitable key map and numerical convex optimization techniques. Specifically, the key rate of the two-ring constellation with 12 coherent states (four states in the inner ring and eight states in the outer ring) can reach 2.4 times of that of original quadrature phase shift keying and 70% of the Gaussian modulation protocol at 50 km. Such an approach can easily be applied to existing systems, making the discrete-modulation protocol an attractive alternative for high-rate and low-cost applications in secure quantum communication networks.

1. Introduction

Quantum key distribution (QKD) [1, 2], one of the most prominent applications 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 physics [3, 4]. Continuous-variable (CV) QKD encodes the key information into continuous-spectrum quantum observables, such as the quadrature components of the light field, which can offer larger key rates at metropolitan distances [5–11]. CV-QKD can employ similar components as classical telecom systems and has received extensive attention and witnessed rapid development both theoretically and experimentally [12–37].

At present, most CV-QKD schemes are based on the Gaussian modulation, meaning that Alice displaces the quadratures of the sent states according to a Gaussian distribution, which reaches the channel capacity and achieves a high key rate. However, this type of protocol imposes many requirements on modulation devices and the error-correction procedure. Moreover, a perfect Gaussian modulation cannot be met in realistic applications owing to the finite range and precision of practice modulators. In practice, the Gaussian modulation is approximated by a modulation constellation with a finite number of states, and it has been shown that at least 8100 states (90×90 size constellation) are needed to satisfactorily simulate a Gaussian distribution [38]. To release these stringent restrictions and simplify the protocol, researchers have proposed discrete-modulation schemes for CV-QKD [39–45].

The discrete-modulation CV-QKD prepares a small number of coherent states to avoid the complexity of the Gaussian modulation. M-symbol phase shift keying is a coded modulation scheme where Alice sends

coherent states of the form $|\alpha_x\rangle = \left|\alpha e^{ix2\pi/M}\right\rangle$ for some $\alpha > 0$. Such constellations can be generated by rotating a coherent state in the position-momentum phase space. Another modulation scheme is the M-symbol quadrature amplitude modulation, where M coherent states are modulated to be distributed equidistantly with each other in the phase space. The 4-phase-shift keying (PSK) modulation scheme, also known as the quadrature PSK scheme, has attracted some interest owing to its relatively good performance. However, unlike the Gaussian modulation, which can apply the proof method of Gaussian attacks' optimality [46–48], the discrete modulation CV-QKD is more complex in terms of the security analysis. Previous security proofs for the 4-PSK protocol have been restricted to Gaussian attacks [49–51], which are believed to be suboptimal for discrete modulation schemes; thus, the key rate obtained cannot be considered secure.

Numerical techniques are attractive for obtaining reliable secret key rate bounds [52, 53]. Recently, the security proofs for discrete-modulation CV-QKD have been established by applying numerical-method-based convex optimization techniques [54, 55]. An analytical lower bound of the asymptotic secret key rate was derived for arbitrary modulation schemes [56]. Experimental demonstrations of discrete modulation CV-QKD were also reported recently [57–59]. However, current discrete-modulation protocols require relatively large constellation sizes to achieve a key rate comparable to that of the Gaussian modulation. Without using the Gaussian optimality proof method, the approach in [55] provides a tighter bound and thus a higher key rate. At present, this approach is only applied to analyze the 4-PSK protocol, which still exhibits a relatively low key rate compared with the optimal Gaussian modulation, about a quarter of the key rate achievable for the Gaussian modulation, making it less attractive.

In this paper, we design discrete-modulation protocols with a constellation size of about ten that can achieve a high key rate close to that of the Gaussian modulation. To this end, we first extend the 4-PSK protocol to more signal states, eight states (8-PSK) and 12 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 makes only a small improvement from 8-PSK to 12-PSK. This is because the performance of 8-PSK approaches the limit of a single-ring constellation protocol, so further increasing the number of states is not more advantageous. To enlarge the distribution range of states in phase space and further improve the performance, we propose using the two-ring constellation scheme, where not only the phase quadrature but also the amplitude quadrature is modulated. By applying appropriate key mapping and parameter optimization techniques, the two-ring constellation with 12 states (four states in the inner ring and eight states in the outer ring) achieves superior performance. Compared with the original 4-PSK protocol, the secret key rate is increased to 2.4 times, which reaches 70% of the key rate achievable for the Gaussian modulation. With performance close to the Gaussian modulation protocol, the presented protocol with fewer constellation points is easier to implement with high speed, consumes less random numbers, and has less state preparation noise (the main source for the excess noise of the CV-QKD system), making the protocol highly attractive for practical applications.

The rest of the paper is organized as follows. In section 2, we analyze the performance of the discrete-modulation protocol of 8-PSK and 12-PSK with a single-ring constellation. In section 3, we give the two-ring constellation modulation and key map schemes and then investigate the dependence of the key rate on various parameters to optimize the protocol. The results are compared with the Gaussian modulation CV-QKD protocol under realistic trusted noisy detection. In section 4, we apply the post-selection technology to our proposed protocol. Our conclusions are given in section 5.

2. Discrete-modulation CV-QKD with a single-ring constellation

2.1. The protocol description

The schematic of single-ring signal constellation for discrete-modulation CV-QKD of 8-PSK and 12-PSK is illustrated in figure 1. The process of the protocol can be described as follows.

2.1.1. State preparation, distribution and measurement

For 8-PSK, the sender, Alice, prepares the coherent state $|\alpha_x\rangle = \left|\alpha e^{ix\pi/4}\right\rangle$ with $x \in \{0,1,2,3,4,5,6,7\}$, and 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 $\left\{|\alpha_x\rangle = \left|\alpha e^{ix\pi/6}\right\rangle,\ x = 0,\ldots,11\right\}$, where α is a predetermined amplitude and can be optimized. The prepared states are sent to the receiver, Bob, through an insecure quantum channel. After receiving Alice's state, Bob performs a heterodyne measurement on the state and records the measurement outcome $y \in \mathbb{C}$.

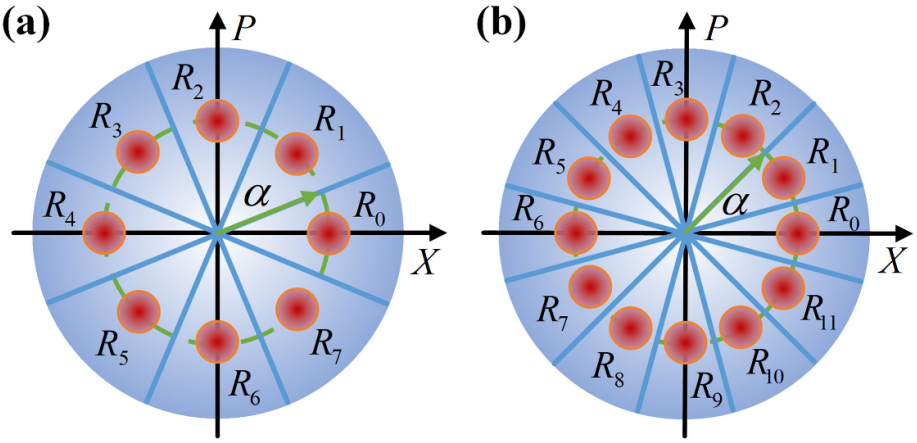

Figure 1. Schematic diagram of the single-ring constellation for multiple signal states: (a) 8-PSK, (b) 12-PSK. R_j represents the key mapping region, where Bob maps the measurement outcomes to the corresponding discretized key values. Notice that coherent states have distribution ranges from negative infinity to positive infinity in phase space, the orange circle illustrates the error circle of the coherent state, i.e. one standard deviation of shot noise.

2.1.2. Parameter estimation

After obtaining enough data (x, y), Alice and Bob randomly select a small part of the data for parameter estimation. They use the remaining data to extract the keys. Alice and Bob disclose all the information of the data selected for parameter estimation that allow them to constrain the joint state ρ_{AB} and calculate the secret key rate. If the key rate is less than zero, they abort the protocol. Otherwise, they proceed.

2.1.3. Reverse reconciliation key map

Bob obtains his raw key string by a key map. Specifically, Bob labels each outcome $y = |y| e^{i\theta}$ according to the region R_j as

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

where $j \in \{0, \ldots, 7\}$ for 8-PSK and $j \in \{0, \ldots, 11\}$ for 12-PSK.

2.1.4. Error correction and privacy amplification

Finally, Alice and Bob implement suitable error correction and privacy amplification procedures to extract secret keys.

2.2. Performance analysis

The secure key rate can be calculated by the numerical method. (Refer to appendix for the key steps.) Considering a typical phase-insensitive Gaussian channel in the context of the optical fiber communication, the simulated statistics are given by [60]

$$\begin{aligned} \left\langle \hat{F}_Q \right\rangle_x &= \sqrt{2\eta T}\,\mathrm{Re}\left(\alpha_x\right), \\ \left\langle \hat{F}_P \right\rangle_x &= \sqrt{2\eta T}\,\mathrm{Im}\left(\alpha_x\right), \\ \left\langle \hat{S}_Q \right\rangle_x &= 2\eta T\,\mathrm{Re}(\alpha_x)^2 + 1 + \frac{1}{2}\eta T\xi + v_{el}, \\ \left\langle \hat{S}_P \right\rangle_x &= 2\eta T\,\mathrm{Im}(\alpha_x)^2 + 1 + \frac{1}{2}\eta T\xi + v_{el}, \end{aligned} \tag{2}$$

where T and ξ represent the transmittance and excess noise of the channel, respectively, and η and v_{el} denote the detection efficiency and electronic noise of the detector, respectively.

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

$$P(y|x) = \frac{1}{\pi\left(1 + \frac{1}{2}\eta T\xi + v_{el}\right)} \exp\left[-\frac{\left|y - \sqrt{\eta T}\alpha_x\right|^2}{1 + \frac{1}{2}\eta T\xi + v_{el}}\right]. \tag{3}$$

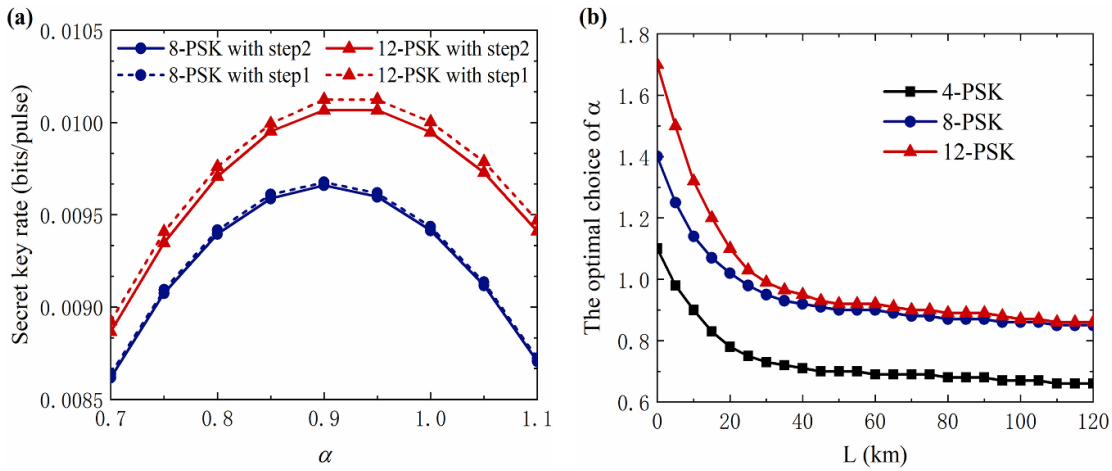

Figure 2. (a) Secret key rates as a function of the coherent state amplitude α for 8-PSK and 12-PSK protocols at the transmission distance of $L = 50$ km. (b) The optimal choice of α at different transmission distances for the 4-PSK, 8-PSK, and 12-PSK protocols.

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

$$\tilde{P}(z|x) = \begin{cases} \int_0^\infty r dr \int_{(2z-1)\pi/8}^{(2z+1)\pi/8} P\left(re^{i\theta}|x\right) d\theta & \text{(8-PSK)} \\ \int_0^\infty r dr \int_{(2z-1)\pi/12}^{(2z+1)\pi/12} P\left(re^{i\theta}|x\right) d\theta & \text{(12-PSK)} \end{cases}. \tag{4}$$

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 α. In figure 2(a), we plot the key rate versus the choice of α 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 $v_{\text{el}} = 0.015$ [21]. The dashed line represents the result of step 1 of our algorithm, which gives an upper bound on the key rate, and the 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, so the obtained bound is tight. We carry out a coarse-grained search for α in the interval [0.7, 1.1] with a step size of 0.05. Clearly, there is an optimal value of α to maximize the key rate. At 50 km, the optimal α for 8-PSK and 12-PSK is 0.9 and 0.92, respectively. In figure 2(b), we give the optimal values of α at different transmission distances, and the results of the 4-PSK protocol are also shown for comparison. The optimal α (modulation variance) decreases and gradually converges to a constant when the transmission distance increases, which is consistent with the Gaussian modulation protocol [61]. Compared with the 4-PSK protocol, 8-PSK allows for a larger optimal value of α, thus providing a higher signal-to-noise ratio. The difference between the optimal α for the 8-PSK and 12-PSK protocols gradually decreases with the increase in the transmission distance and is almost indistinguishable over long distances.

In figure 3, we present the achievable key rates at different transmission distances for different discrete-modulation protocols and the Gaussian modulation protocol. The key rate has been optimized by adopting the optimal modulation amplitude (figure 2(b)) and variance. In addition, we have applied the post-selection technology to the 4-PSK protocol to obtain the optimal key rate [60]. The upper solid curve is the Pirandola–Laurenza–Ottaviani–Banchi bound, which represents the maximum secret key rate achievable in a repeater-less and lossy channel system [62]. 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 the discrete-modulation protocol is still relatively low. Taking 50 km as an example, we find that the key rates per pulse of the 4-PSK, 8-PSK, 12-PSK, and Gaussian modulation protocols are 0.00 602, 0.00 966, 0.01 008, and 0.02 103 bits/pulse, respectively. The 4-PSK and 8-PSK protocols can reach approximately 28% and 45% of the key rate of the Gaussian modulation.

Current results show that the Gaussian modulation scheme provides an optimal theoretical secure key rate, and there exists an optimal modulation variance given the transmission distance. Notice that the 4-PSK

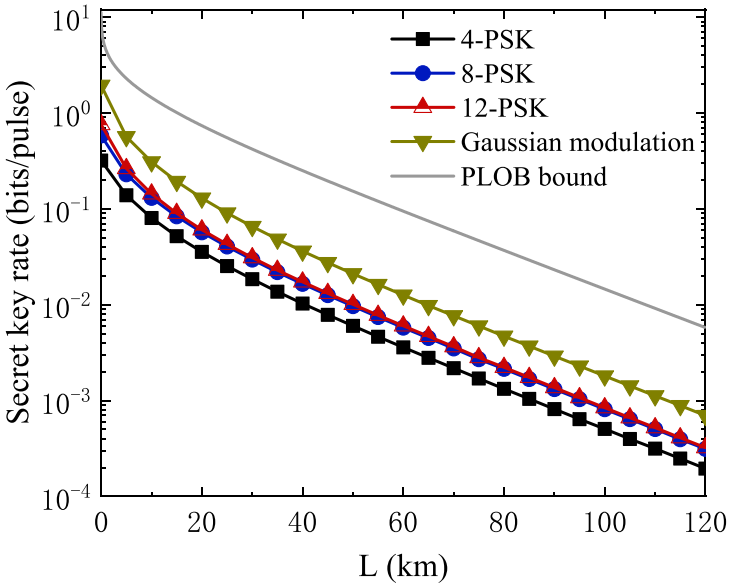

Figure 3. Achievable secret key rate versus the transmission distance for different protocols. The modulation amplitude and variance have been optimized. Other parameters are set to $\beta = 0.95$, $\xi = 0.01$, $\eta = 0.552$, and $v_{el} = 0.015$.

scheme only approximates to a Gaussian modulation scheme at a small modulation variance that is lower than the optimal value of the Gaussian modulation. Under the premise of good Gaussian approximation of the state distribution in phase space, the n-PSK scheme with a large n can increase the effective modulation variance (corresponding to the optimal values of α) to a certain extent. Therefore, the optimal values of α of 8-PSK and 12-PSK are larger than that of 4-PSK (figure 2(b)), and the performance of the 12-PSK and 8-PSK is better than that of the 4-PSK protocol (figure 3).

The performance of the n-PSK scheme with a larger n is always better than that of the n-PSK scheme with a lower n owing to the higher fidelity between its state distribution in phase space and the Gaussian distribution. However, to maintain good Gaussian approximation for the state distribution, we must impose an upper bound for the effective modulation variance even if n tends to infinity. Therefore, the difference between the optimal α of the 8-PSK and 12-PSK protocols is much smaller than that of the 4-PSK and 8-PSK protocols (figure 2(b)), and the performance of 8-PSK modulation is close to that of 12-PSK and tends to saturation (figure 3). However, the optimal modulation variance decreases when the transmission distance increases so that the difference between the optimal α and the key rate for the 8-PSK and 12-PSK protocols gradually decreases with the increase in the transmission distance.

3. Discrete-modulation CV-QKD with a two-ring constellation

To break the limitation of the n-PSK protocol, we propose employing the multiple-symbol amplitude and PSK. Here, we show the two-ring constellation modulation and key mapping method with 12 signal states. In this case, the state distribution range can be further enlarged, and the Gaussian approximation is well maintained. This results in an increase in both the modulation variance and secret key rate.

As shown in figure 4, different from the single-ring PSK protocol, in the designed two-ring constellation, the states are prepared with two different amplitudes α_1 and α_2. The four states in the inner ring are expressed as $\left\{|\alpha_x\rangle = \left|\alpha_1 e^{ix\pi/2}\right\rangle\right\}_{x=0,\ldots,3}$, where each of the states is chosen according to an equal probability p_1. The eight states in the outer ring take the form of $\left\{|\alpha_x\rangle = \left|\alpha_2 e^{i(x-4)\pi/4}\right\rangle\right\}_{x=4,\ldots,11}$, each of which is chosen with an equal probability p_2, which satisfies $p_1 + 2p_2 = 1/4$. Alice transmits the randomly selected state α_x to Bob and records the sequence of the state sent. Upon receiving the state, Bob performs heterodyne detection and obtains the measurement outcome y. According to the region R_j, Bob maps his outcome $y = |y|\, e^{i\theta}$ to the discretized raw keys as follows:

$$z = \begin{cases} j, & \text{if } \theta \in \left[\frac{(2j-1)\pi}{4}, \frac{(2j+1)\pi}{4}\right),\ |y| \in [0, \alpha_c) \quad \{R_j\}_{0 \leqslant j \leqslant 3} \\ j, & \text{if } \theta \in \left[\frac{(2j-9)\pi}{8}, \frac{(2j-7)\pi}{8}\right),\ |y| \in [\alpha_c, \infty) \quad \{R_j\}_{4 \leqslant j \leqslant 11} \end{cases}, \tag{5}$$

where α_c is the amplitude corresponding to the boundary between the inner and outer regions.

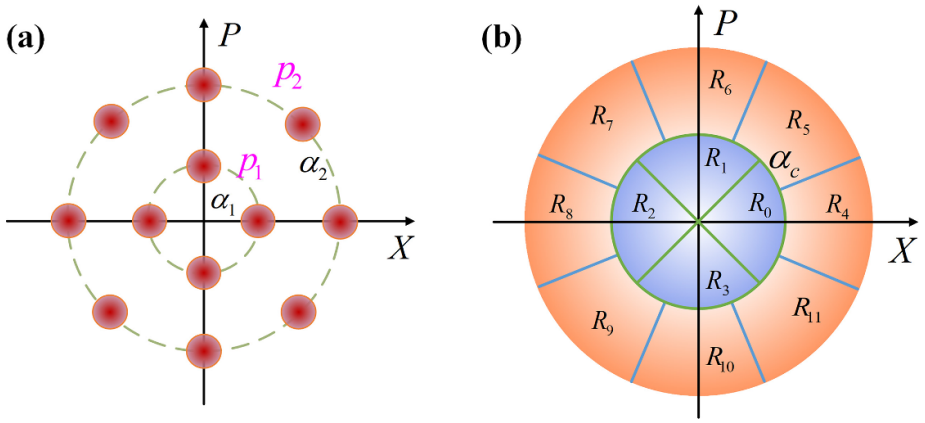

Figure 4. Schematic diagram of the proposed two-ring constellation structure with 12 signal states. (a) State modulation at Alice's side, (b) Key map in terms of Bob's measurement outcome.

As described above, the primary differences between the two-ring constellation and single-ring constellation protocols are the signal states preparation and key map. The different signal states preparation of Alice gives different Bob's observation results, which are used to constrain the joint state ρ_{AB}. The key map is reflected in the region operators R_j. The R_j in the photon-number basis for the two-ring constellation modulation is expressed as

$$\langle m|R_j|n\rangle = \begin{cases} C_{m,n}\frac{i\left[e^{i(m-n)(2j-1)\pi/4}-e^{i(m-n)(2j+1)\pi/4}\right]}{m-n}\int_0^{\alpha_c} f(r)\,dr & 0\leqslant j\leqslant 3 \\ C_{m,n}\frac{i\left[e^{i(m-n)(2j-9)\pi/8}-e^{i(m-n)(2j-7)\pi/8}\right]}{m-n}\int_{\alpha_c}^{\infty} f(r)\,dr & 4\leqslant j\leqslant 11 \end{cases}. \tag{6}$$

When $m=n$, we have

$$\langle n|R_j|n\rangle = \begin{cases} \frac{\pi}{2}C_n\int_0^{\alpha_c} f(r)\,dr & 0\leqslant j\leqslant 3 \\ \frac{\pi}{4}C_n\int_{\alpha_c}^{\infty} f(r)\,dr & 4\leqslant j\leqslant 11 \end{cases}. \tag{7}$$

The region operator R_j is included in the postprocessing map $\mathcal{G}$, which is part of the objective function of the present optimization problem. By employing the region operator, the secure key rates can be calculated.

To maximize the secure key rate of the two-ring constellation scheme with 12 states, we should optimize four relevant parameters: the modulation amplitudes α_1, α_2, the choice probability p_1, and the boundary of the inner and outer regions α_c. The dependence of the key rate on these parameters is shown in figure 5. To reduce the computing time of the optimization process, we perform the coarse-grained global optimization for the four parameters. First, the large search ranges and step sizes are used to obtain the rough intervals into which the optimal values fall. Then, we adopt smaller search step sizes to obtain the near-optimal estimated values of the parameters, which result in the near-optimal secure key rates.

For the transmission distance of 50 km, the optimal choices of the parameters are $\alpha_1=0.7$, $\alpha_2=1.6$, $\alpha_c=0.85$, $p_1=7/48$ and $p_2=5/96$. In this case, we achieve a key rate of 0.014 59 bits/pulse, which is 50% higher than that of the 8-PSK protocol and 140% higher than that of the 4-PSK protocol. By varying the constellation geometry from the single-ring PSK structure to the two-ring constellation structure, we effectively overcome the limitation of the states distribution range in phase space and significantly improve the performance of the 4-PSK discrete-modulation protocol.

In figure 6, we give the optimal choice of parameters α_1, α_2, α_c and p_1 at different transmission distances. The cutoff value of photon number N_c is selected from the interval [12, 22] according to the modulation amplitudes. Similarly to the n-PSK protocol in figure 2, both the optimal coherent state amplitudes α_1 and α_2 decrease as the transmission distance increases. We can see that the optimal α_c is closer to α_1 and that p_1 is greater than p_2, resulting in an approximate Gaussian distribution in phase space. With the increase in the transmission distance, the probability p_1 increases correspondingly. Next, we employ the optimal parameter values to obtain the optimal key rate and analyze the performance of the protocol.

In figure 7, we give the simulation results of the two-ring constellation with 12 states and compare it with the previous PSK protocols and Gaussian modulation protocol. We observe that the key rate of the two-ring

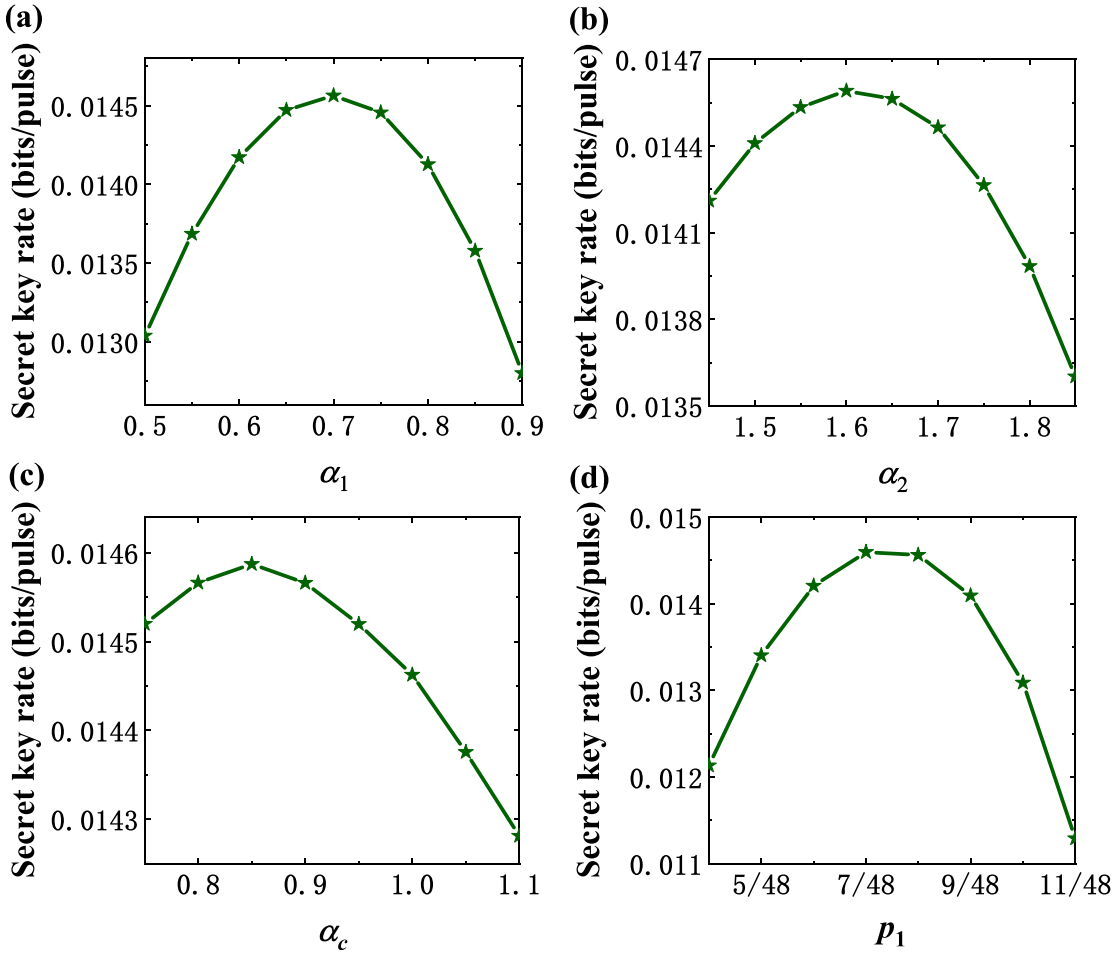

Figure 5. Secure key rate versus the choices of α_1, α_2, α_c, and p_1. The simulation parameters are $\beta = 0.95$, $\xi = 0.01$, $\eta = 0.552$, $v_{el} = 0.015$, and $L = 50$ km. (a) The optimal α_1 is obtained via a coarse-grained search in the interval [0.5, 0.9] with a step size of 0.05. The other parameters are set to $\alpha_2 = 1.6$, $\alpha_c = 0.85$, and $p_1 = 7/48$. (b) The value of α_2 is changed with a step size of 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 α_c is changed with a step size of 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 of 1/48. The other parameters are set to $\alpha_1 = 0.7$, $\alpha_2 = 1.6$, and $\alpha_c = 0.85$.

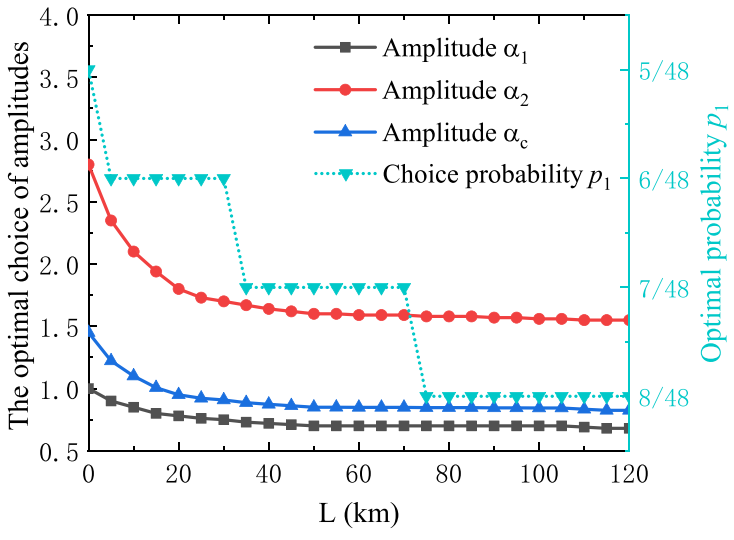

Figure 6. The optimal choice of parameters α_1, α_2, α_c and p_1 at different transmission distances for a two-ring constellation protocol with 12 signal states.

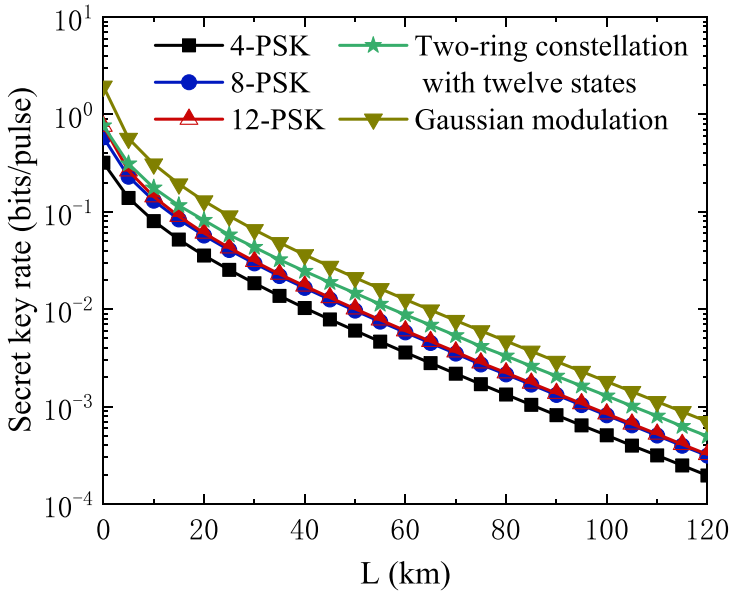

Figure 7. Achievable secret key rate versus the transmission distance for different protocols. Other parameters are set to $\beta = 0.95$, $\xi = 0.01$, $\eta = 0.552$, and $v_{el} = 0.015$.

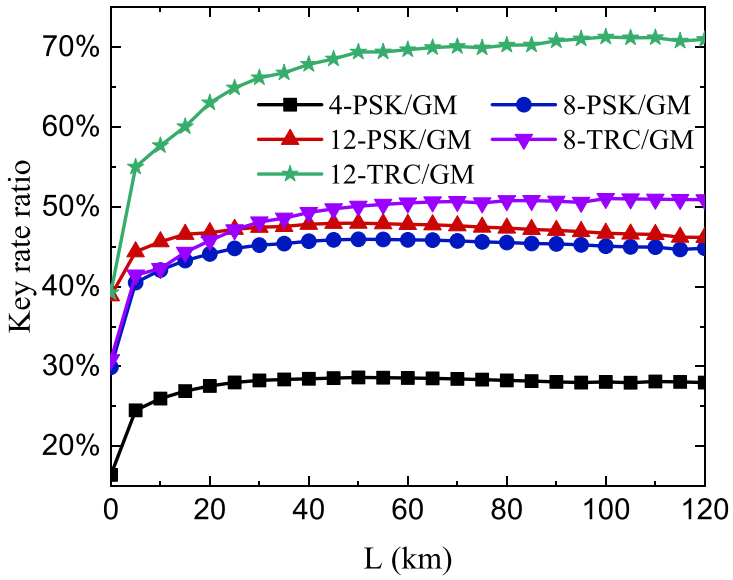

Figure 8. Ratio of the key rate of various discrete-modulation protocols to the Gaussian modulation protocol. TRC represents the two-ring constellation protocol, and GM represents the Gaussian modulation protocol.

constellation with 12 states is significantly higher than that of the 4, 8, and 12-PSK protocols. As shown in figure 8, the performance of the two-ring protocol with eight states (four states in the inner ring and four states in the outer ring) is superior to that of 8-PSK and better than that of 12-PSK at transmission distances longer than 25 km. For long-distance transmission distances above 50 km, the two-ring constellation with 12 states can exceed 70% of the key rate of the Gaussian modulation protocol. The gap of the key rates between the two-ring constellation protocol and Gaussian modulation protocol decreases gradually with the increase in the transmission distance. Notice that two-ring constellation with 12 states requires only 1-bit discretization for the amplitude of the light field and 3-bit discretization for the phase of the light field. This proves that the concise two-ring constellation with 12 states can exhibit superior performance, which is extremely close to that of the Gaussian modulation protocol.

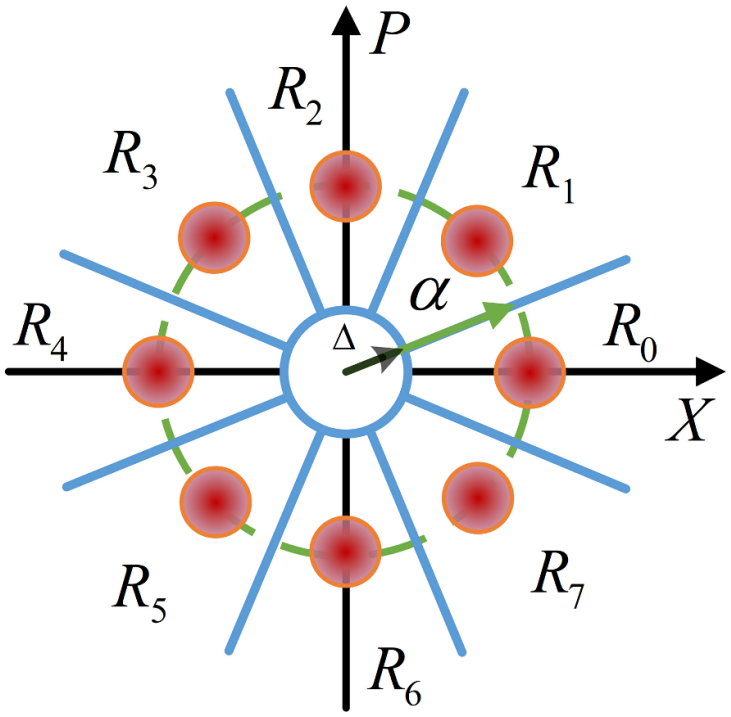

Figure 9. The key mapping for the 8-PSK protocol when post-selection is considered.

4. Post-selection

Post-selection is useful to improve the key rate of the four state protocols [60]. It also reduces the amount of data for post-processing. Then, we apply the post-selection technology to our proposed protocol. In figure 9, taking the 8-PSK as an example, we illustrate the concept of post-selection. There is a cutoff area at the center of the phase space, which is defined by a circle with the radius Δ.The data inside the circle are discarded, and the data outside the circle are retained. Hence, the key mapping results of Bob become

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

where Δ is the post-selection parameter. ⊥ means that the data should be discarded.

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

$$\tilde{P}(z|x)=\int_{\Delta}^{\infty}rdr\int_{(2z-1)\pi/8}^{(2z+1)\pi/8}P\left(re^{i\theta}\middle|x\right)d\theta, \tag{9}$$

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

The key rate can be potentially improved by discarding extremely noisy data, where Eve has more advantages on determining the key than Alice and Bob. We consider a simple post-selection scheme that removes measurement results close to ordinate origin. Technically, this is realized by adding an additional symbol (⊥) to the key map, which is assigned whenever a signal lies within the discarded area. The post-selection is introduced by modifying the key map procedure. Mathematically, the key map is included in the post-processing map $\mathcal{G}$. By a simple modification of the postprocessing map $\mathcal{G}$ and taking the sifting probability p_{pass} and the information leakage in the error-correction phase δ_{EC} into account, we can calculate the key rate during post-selection. For the 8-PSK and 12-PSK protocols, our security proof technique allows us to consider post-selection with $\Delta>0$. In this case, it can reduce the length of the raw key and simplify the error correction as well as higher key rate.

In figure 10(a), we plot the key rate versus the post-selection parameter Δ for the 8-PSK and 12-PSK protocols at the distance $L=50$ km. We observe that there exists an optimal post-selection parameter to maximize the key rate. The optimal post-selection parameter value for the 8-PSK and 12-PSK protocols is $\Delta=0.55$. Compared with the original protocol without post-selection, the key rate is increased by 8% for

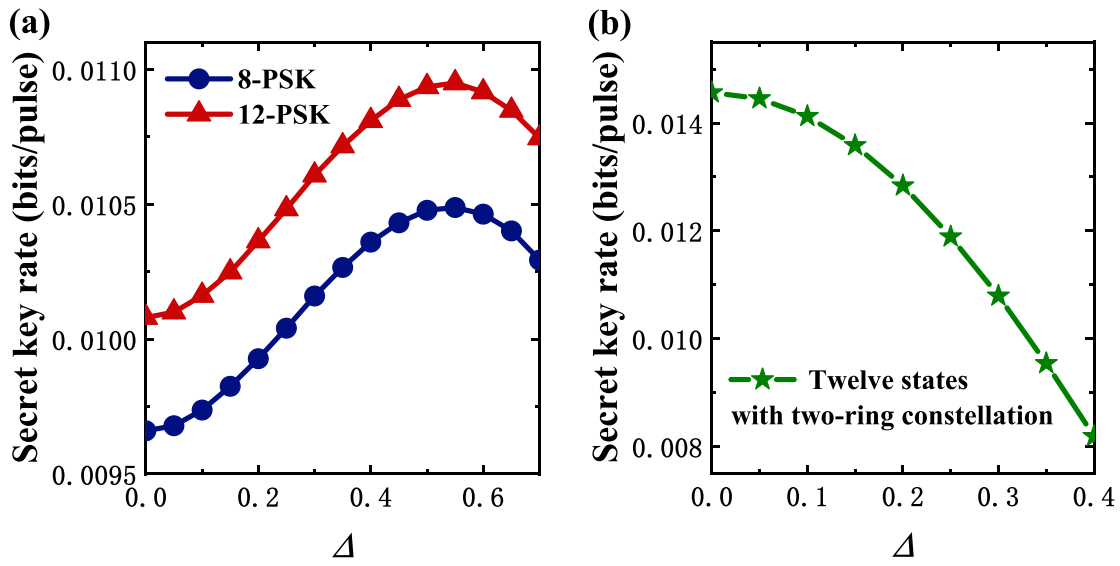

Figure 10. (a) Secure key rate versus the post-selection parameter for the 8-PSK and 12-PSK protocols at the transmission distance of 50 km. The modulation amplitude is set to $\alpha = 0.9$ for the 8-PSK protocol and $\alpha = 0.92$ for the 12-PSK protocol. (b) Secure key rate versus post-selection parameter for the two-ring constellation protocol at 50 km, where the parameter value is set to $\alpha_1 = 0.7$, $\alpha_2 = 1.6$, $\alpha_c = 0.85$ and $p_1 = 7/48$. The optimal post-selection parameter is obtained via a coarse-grained search for α_0 in the interval [0, 0.7] for (a) and [0, 0.4] for (b) with a step size of 0.05. Other parameters for simulations are set to $\beta = 0.95$, $\xi = 0.01$, $\eta = 0.552$, and $v_{el} = 0.015$.

both 8-PSK and 12-PSK protocols. By inserting $\Delta = 0.55$ into equation (9), we can obtain the value of the sifting factor $p_{pass} = 0.75$, which means that the amount of data used for post-processing is reduced by 25%.

With a similar procedure, we search for the optimal post-selection parameter for the two-ring constellation protocol with 12 states, as shown in figure 10(b). The result suggests that the optimal value is $\Delta = 0$. Therefore, we do not need to post-select the data for the two-ring constellation scheme along the radial direction. The possible reason for this result is to approximate the Gaussian modulation in the phase space, where the states are modulated according to the Gaussian distribution and have a large probability in the center of the phase space. Note that the angular post-selection may be useful, and other post-selection strategies should be developed, which we will leave for future work.

5. Conclusions

The two-ring constellation schemes are 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 convex optimization techniques without the Gaussian optimality proof method. Our results show that 8-PSK can increase the key rate by about 60% over conventional the 4-PSK protocol; however, adding the 8-PSK to 12-PSK does not significantly improve the key rate. Interestingly, by allocating 12 coherent states to a two-ring constellation that enlarges the distribution range of coherent states in phase space, we can obtain an achieved key rate that is 140% higher than that of the 4-PSK protocol. This key rate reaches about 70% of that of the Gaussian modulation protocol for transmission distances above 50 km. Our results confirm that the discrete-modulation protocol with ten or so appropriate constellation points and optimal modulation parameters can approach the key rate of the Gaussian modulation protocol. Thus, the proposed discrete modulation protocol has promising applications in high-rate and low-cost secure quantum communication networks.

In our current work, we employ numerical methods to estimate the secure key rate, which is computationally challenging. As the constellation size increases, this process is more time-consuming. It is desirable to find better algorithms or derive analytical solutions for the optimization problem. We observe that the key rate of our protocol is not very close to the Gaussian modulation protocol at the short-distance transmission. It is desirable to improve the key rate at short distances by extending the current state constellations or employing other new constellation design schemes [63]. In addition, our current work is restricted to the asymptotic scenario. Extending our security analysis to include the impact of finite size is an important future task [64–68]. The future work will also include finding better data post-selection strategies to improve the key rate [69, 70].

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Acknowledgments

P Wang would like to thank Dr J Lin for the helpful discussions. This work is supported by the National Natural Science Foundation of China (NSFC) (Grant Nos. 62175138, 62205188, 12174232), Aeronautical Science Foundation of China (20200020115001), and Key Research and Development Program of Guangdong Province (2020B0303040002), as well as Shanxi 1331KSC.

Appendix. Secret key rate

For convenience of the security analysis, we consider the equivalent entanglement-based (EB) scheme. Here, we explore the numerical security proof method presented in [55, 60] to obtain the secure key rate. In the EB scheme, Alice initially prepares the bipartite state

$$|\psi\rangle_{AA'}=\sum_{x}\sqrt{p_x}|x\rangle_A|\alpha_x\rangle_{A'}, \tag{A.1}$$

where $|x\rangle$ is an orthonormal basis for register A. Alice keeps A and sends 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 $M^A=\left\{M_x^A=|x\rangle\langle x|\right\}$. When we obtain 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

$$\rho_{AB}=\left(\mathrm{id}_A\otimes\mathcal{E}_{A'\to B}\right)\left(|\psi\rangle\langle\psi|_{AA'}\right), \tag{A.2}$$

where id_A is the identity channel acting on A, and $\mathcal{E}_{A'\to B}$ describes the quantum channel, which is a completely positive and trace-preserving 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 [55]

$$K^{\infty}=\min_{\rho_{AB}\in\mathcal{S}}D\left(\mathcal{G}\left(\rho_{AB}\right)\|\,\mathcal{Z}\left[\mathcal{G}\left(\rho_{AB}\right)\right]\right)-p_{\mathrm{pass}}\delta_{\mathrm{EC}}, \tag{A.3}$$

where $D(\rho\|\sigma)=\mathrm{Tr}\left(\rho\log_2\rho\right)-\mathrm{Tr}\left(\rho\log_2\sigma\right)$ 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_{pass} is the sifting probability of data for key generation; δ_{EC} stands for the leaked information of the per-signal pulse during the error correction phase and can be computed as follows:

$$\begin{aligned}\delta_{\mathrm{EC}}&=H(Z)-\beta I(X;Z)\\&=(1-\beta)H(Z)+\beta H(Z|X),\end{aligned} \tag{A.4}$$

where β is the reconciliation efficiency. X and Z represent the raw key string of Alice and Bob, respectively.

To compute the expected secret key rate, we make it a key point to find the minimum value of $D\left(\mathcal{G}\left(\rho_{AB}\right)\|\,\mathcal{Z}\left[\mathcal{G}\left(\rho_{AB}\right)\right]\right)$, which is a convex optimization problem matching some constraints and is expressed as [60]

$$\begin{aligned}&\text{minimize } D\left(\mathcal{G}\left(\rho_{AB}\right)\|\,\mathcal{Z}\left[\mathcal{G}\left(\rho_{AB}\right)\right]\right)\\&\text{subject to}\\&\quad\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A\otimes\hat{F}_Q\right)\right]=p_x\langle\hat{F}_Q\rangle_x\\&\quad\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A\otimes\hat{F}_P\right)\right]=p_x\langle\hat{F}_P\rangle_x\\&\quad\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A\otimes\hat{S}_Q\right)\right]=p_x\left\langle\hat{S}_Q\right\rangle_x\\&\quad\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A\otimes\hat{S}_P\right)\right]=p_x\left\langle\hat{S}_P\right\rangle_x\\&\quad\mathrm{Tr}\left[\rho_{AB}\right]=1\\&\quad\rho_{AB}\geqslant 0\end{aligned} \tag{A.5}$$

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. In addition, notice that Eve cannot access Alice's system, so there is an additional constraint

$$\mathrm{Tr}_B\left[\rho_{AB}\right]=\rho_A=\sum_{i,j=0}^{n}\sqrt{p_i p_j}\left\langle\alpha_j|\alpha_i\right\rangle|i\rangle\left\langle j\right|_A, \tag{A.6}$$

where n takes 7 or 11 for 8-PSK or 12-PSK, respectively.

The post-processing map $\mathcal{G}$ and pinching quantum channel $\mathcal{Z}$ can be written as [60]

$$\begin{aligned}\mathcal{G}(\sigma)&=K\sigma K^{\dagger},\\ K&=\sum_{z=0}^{n}|z\rangle_R\otimes \mathrm{I}_A\otimes\left(\sqrt{R_z}\right)_B,\\ \mathcal{Z}(\sigma)&=\sum_{j=0}^{n}\left(|j\rangle\left\langle j\right|_R\otimes \mathrm{I}_{AB}\right)\sigma\left(|j\rangle\left\langle j\right|_R\otimes \mathrm{I}_{AB}\right).\end{aligned} \tag{A.7}$$

To numerically minimize the objective function, the available ρ_{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, Bob's state is in an infinite dimensional Hilbert space. This can be circumvented by applying the photon-number cutoff assumption. When the chosen photon number cutoff parameter N_c is large enough, this assumption is reasonable. Here, we set an appropriate parameter value of N_c such that the probability of the photon number of the received signal state being larger than N_c is less than 0.1%, and a larger N_c produces no meaningful improvement in the key rate. Then, the region operators R_j in the photon-number basis can be expressed as (taking the 12-PSK as an example)

$$\begin{aligned}\langle m|R_j|n\rangle&=\int_0^{\infty}rdr\int_{(2j-1)\pi/12}^{(2j+1)\pi/12}d\theta\,\langle m|G_{re^{i\theta}}|n\rangle\\ &=\begin{cases}C_{m,n}\frac{i\left[e^{i(m-n)(2j-1)\pi/12}-e^{i(m-n)(2j+1)\pi/12}\right]}{m-n}\int_0^{\infty}f(r)\,dr & for\ m\neq n\\ \frac{\pi}{6}C_n\int_0^{\infty}f(r)\,dr & for\ m=n\end{cases},\end{aligned} \tag{A.8}$$

where $C_{m,n}=\left[\pi^{-1}\eta^{(m-n)/2-1}\right](m!/n!)^{1/2}\left[n_d^m(1+n_d)^{-(n+1)}\right]$ and $C_n=(\pi\eta)^{-1}\times\left[n_d^n(1+n_d)^{-(n+1)}\right]$. n_d is the total noise introduced by each realistic homodyne detector relative to the signal input and defined as $n_d=(1-\eta+v_{el})/\eta$. The function $f(r)$ has form

$$f(r)=\exp\left[-\frac{r^2}{\eta(1+n_d)}\right]L_m^{(n-m)}\left[-\frac{r^2}{\eta n_d(1+n_d)}\right]r^{n-m+1}, \tag{A.9}$$

where $L_k^{(j)}(x)$ is the generalized Laguerre polynomial of degree k with a parameter j in the variable x.

Similarly, the matrix expressions of the first-moment observables $\hat{F}_Q$, $\hat{F}_P$ and second-moment observables $\hat{S}_Q$, $\hat{S}_P$ can be obtained [60].

A tight lower bound on the key rate can be achieved using a two-step procedure developed in [53]. At the first step, the Frank–Wolfe algorithm is used to approximately minimize the convex function, thus obtaining an upper bound on the key rate. At the second step, we convert this upper bound to a reliable lower bound by taking the numerical imprecision into account. Using the two-step procedure and defining $f(\rho)=D\left(\mathcal{G}(\rho)\|\,\mathcal{Z}\left[\mathcal{G}(\rho)\right]\right)$, we have

$$\min_{\rho\in\mathcal{S}}f(\rho)\geqslant f_{\epsilon}(\rho_1)-\mathrm{Tr}\left(\rho_1^T\nabla f_{\epsilon}(\rho_1)\right)+f_d^{\max}-\zeta_{\epsilon}, \tag{A.10}$$

where ρ_1 is the suboptimal state obtained in the first step. ε is the perturbation parameter, and $f_\epsilon(\rho_1) := D(\mathcal{G}_\epsilon(\rho_1)\|\mathcal{Z}[\mathcal{G}_\epsilon(\rho_1)])$. $\zeta_\epsilon = 2\epsilon(d'-1)\log_2\frac{d'}{\epsilon(d'-1)}$, where d' is the dimension of $\mathcal{G}(\rho)$. The gradient $\nabla f_\epsilon(\rho_1)$ is given by

$$[\nabla f_\epsilon(\rho_1)]^T = \mathcal{G}_\epsilon^\dagger(\log_2\mathcal{G}_\epsilon(\rho_1)) - \mathcal{G}_\epsilon^\dagger(\log_2\mathcal{Z}[\mathcal{G}_\epsilon(\rho_1)]). \tag{A.11}$$

$f_d^{\max}$ is the dual function and is written as

$$\begin{aligned} f_d^{\max} = \max_{(\vec{v},\vec{s})} & \left(\vec{\tilde{\gamma}}\cdot\vec{v} - \epsilon'\sum_{i=1}^{nc} s_i\right) \\ \text{subject to} & \\ & -\vec{s} \leqslant \vec{v} \leqslant \vec{s} \quad , \\ & \sum_{i=1}^{nc} v_i\tilde{\Gamma}_i^T \leqslant \nabla f_\epsilon(\rho_1) \\ & (\vec{v},\vec{s}) \in (\mathbb{R}^{nc},\mathbb{R}^{nc}) \end{aligned} \tag{A.12}$$

where Γ_i and γ_i refer to both sides of the equality constraint, respectively, with the form $\mathrm{Tr}(\Gamma_i\rho) = \gamma_i$. nc represents the number of all constraints. ϵ' is the security parameter related to the numerical imprecision.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50
[3] Lo H K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances *Science* **283** 2050–6
[4] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[5] Braunstein S L and van Loock P 2005 Quantum information with continuous variables *Rev. Mod. Phys.* **77** 513–77
[6] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Gaussian quantum information *Rev. Mod. Phys.* **84** 621–69
[7] Diamanti E and Leverrier A 2015 Distributing secret keys with quantum continuous variables: principle, security and implementations *Entropy* **17** 6072–92
[8] Laudenbach F, Pacher C, Fung C H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P and Hübel H 2018 Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations *Adv. Quantum Technol.* **1** 1800011
[9] Pirandola S *et al* 2020 Advances in quantum cryptography *Adv. Opt. Photon.* **12** 1012–236
[10] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 High-rate measurement-device-independent quantum cryptography *Nat. Photon.* **9** 397–402
[11] Karinou F *et al* 2018 Toward the integration of cv quantum key distribution in deployed optical networks *IEEE Photonics Technol. Lett.* **30** 650–3
[12] Ralph T C 1999 Continuous variable quantum cryptography *Phys. Rev.* A **61** 010303
[13] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Phys. Rev. Lett.* **88** 057902
[14] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 Quantum key distribution using gaussian-modulated coherent states *Nature* **421** 238–41
[15] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 No-switching quantum key distribution using broadband modulated coherent light *Phys. Rev. Lett.* **95** 180503
[16] Lodewyck J *et al* 2007 Quantum key distribution over 25 km with an all-fiber continuous-variable system *Phys. Rev.* A **76** 042305
[17] Qi B, Huang L L, Qian L and Lo H K 2007 Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers *Phys. Rev.* A **76** 052323
[18] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 Continuous-variable quantum cryptography using two-way quantum communication *Nat. Phys.* **4** 726–30
[19] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks *Phys. Rev. Lett.* **109** 100502
[20] Madsen L S, Usenko V C, Lassen M, Filip R and Andersen U L 2012 Continuous variable quantum key distribution with modulated entangled states *Nat. Commun.* **3** 1083
[21] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Experimental demonstration of long-distance continuous-variable quantum key distribution *Nat. Photon.* **7** 378–81
[22] Usenko V C and Grosshans F 2015 Unidimensional continuous-variable quantum key distribution *Phys. Rev.* A **92** 062337
[23] Huang D, Huang P, Li H, Wang T, Zhou Y and Zeng G 2016 Field demonstration of a continuous-variable quantum key distribution network *Opt. Lett.* **41** 3511–14
[24] Walk N *et al* 2016 Experimental demonstration of gaussian protocols for one-sided device-independent quantum key distribution *Optica* **3** 634–42
[25] Leverrier A 2017 Security of continuous-variable quantum key distribution via a gaussian de finetti reduction *Phys. Rev. Lett.* **118** 200501
[26] Wang X, Liu W, Wang P and Li Y 2017 Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution *Phys. Rev.* A **95** 062330
[27] Wang T, Huang P, Zhou Y, Liu W, Ma H, Wang S and Zeng G 2018 High key rate continuous-variable quantum key distribution with a real local oscillator *Opt. Express* **26** 2794–806

[28] Wang N, Du S, Liu W, Wang X, Li Y and Peng K 2018 Long-distance continuous-variable quantum key distribution with entangled states *Phys. Rev. Appl.* **10** 064028
[29] Zhang Y *et al* 2019 Continuous-variable QKD over 50 km commercial fiber *Quantum Sci. Technol.* **4** 035006
[30] Du S, Tian Y and Li Y 2020 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
[31] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M and Peters N A 2020 Experimental passive-state preparation for continuous-variable quantum communications *Phys. Rev. Appl.* **13** 054065
[32] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S and Guo H 2020 Long-distance continuous-variable quantum key distribution over 202.81 km of fiber *Phys. Rev. Lett.* **125** 010502
[33] Dequal D, Trigo Vidarte L, Roman Rodriguez V, Vallone G, Villoresi P, Leverrier A and Diamanti E 2021 Feasibility of satellite-to-ground continuous-variable quantum key distribution *npj Quantum Inform.* **7** 3
[34] Pirandola S 2021 Satellite quantum communications: fundamental bounds and practical security *Phys. Rev. Res.* **3** 023130
[35] Pirandola S 2021 Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks *Phys. Rev. Res.* **3** 043014
[36] Tian Y, Wang P, Liu J, Du S, Liu W, Lu Z, Wang X and Li Y 2022 Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber *Optica* **9** 492–500
[37] Jain N *et al* 2022 Practical continuous-variable quantum key distribution with composable security *Nat. Commun.* **13** 4740
[38] Kaur E, Guha S and Wilde M M 2021 Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution *Phys. Rev.* A **103** 012412
[39] Leverrier A and Grangier P 2009 Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation *Phys. Rev. Lett.* **102** 180504
[40] Zhao Y B, Heid M, Rigas J and Lütkenhaus N 2009 Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks *Phys. Rev.* A **79** 012307
[41] Sych D and Leuchs G 2010 Coherent state quantum key distribution with multi letter phase-shift keying *New J. Phys.* **12** 053019
[42] Wang X Y, Bai Z L, Wang S F, Li Y M and Peng K C 2013 Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise *Chin. Phys. Lett.* **30** 010305
[43] Brádler K and Weedbrook C 2018 Security proof of continuous-variable quantum key distribution using three coherent states *Phys. Rev.* A **97** 022310
[44] Liao Q, Xiao G, Xu C G, Xu Y and Guo Y 2020 Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source *Phys. Rev.* A **102** 032604
[45] Liao Q, Xiao G, Zhong H and Guo Y 2020 Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution *New J. Phys.* **22** 083086
[46] García-Patrón R and Cerf N J 2006 Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution *Phys. Rev. Lett.* **97** 190503
[47] Navascués M, Grosshans F and Acín A 2006 Optimality of gaussian attacks in continuous-variable quantum cryptography *Phys. Rev. Lett.* **97** 190502
[48] Leverrier A and Grangier P 2010 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
[49] Leverrier A and Grangier P 2011 Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation *Phys. Rev.* A **83** 042312
[50] Hirano T, Ichikawa T, Matsubara T, Ono M, Oguri Y, Namiki R, Kasai K, Matsumoto R and Tsurumaru T 2017 Implementation of continuous-variable quantum key distribution with discrete modulation *Quantum Sci. Technol.* **2** 024010
[51] Papanastasiou P, Lupo C, Weedbrook C and Pirandola S 2018 Quantum key distribution with phase-encoded coherent states: asymptotic security analysis in thermal-loss channels *Phys. Rev.* A **98** 012340
[52] Coles P J, Metodiev E M and Lütkenhaus N 2016 Numerical approach for unstructured quantum key distribution *Nat. Commun.* **7** 11712
[53] Winick A, Lütkenhaus N and Coles P J 2018 Reliable numerical key rates for quantum key distribution *Quantum* **2** 77
[54] Ghorai S, Grangier P, Diamanti E and Leverrier A 2019 Asymptotic security of continuous-variable quantum key distribution with a discrete modulation *Phys. Rev.* X **9** 021059
[55] Lin J, Upadhyaya T and Lütkenhaus N 2019 Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution *Phys. Rev.* X **9** 041064
[56] Denys A, Brown P and Leverrier A 2021 Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation *Quantum* **5** 540
[57] Pereira D, Almeida M, Facão M F, Pinto A N and Silva N A 2022 Probabilistic shaped 128-apsk cv-qkd transmission system over optical fibres *Opt. Lett.* **47** 3948–51
[58] Pan Y, Wang H, Shao Y, Pi Y, Li Y, Liu B, Huang W and Xu B 2022 Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system *Opt. Lett.* **47** 3307–10
[59] Roumestan F, Ghazisaeidi A, Renaudier J, Vidarte L T, Diamanti E and Grangier P 2021 High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam *2021 European Conf. on Optical Communication* (*ECOC*) pp 1–4
[60] Lin J and Lütkenhaus N 2020 Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution *Phys. Rev. Appl.* **14** 064030
[61] Wang X, Guo S, Wang P, Liu W and Li Y 2019 Realistic rate-distance limit of continuous-variable quantum key distribution *Opt. Express* **27** 13372–86
[62] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications *Nat. Commun.* **8** 15043
[63] Jardel F, Eriksson T A, Méasson C, Ghazisaeidi A, Buchali F, Idler W and Boutros J J 2018 Exploring and experimenting with shaping designs for next-generation optical communications *J. Lightw. Technol.* **36** 5298–308
[64] Leverrier A, Grosshans F and Grangier P 2010 Finite-size analysis of a continuous-variable quantum key distribution *Phys. Rev.* A **81** 062343
[65] Bunandar D, Govia L C G, Krovi H and Englund D 2020 Numerical finite-key analysis of quantum key distribution *npj Quantum Inform.* **6** 104
[66] Papanastasiou P and Pirandola S 2021 Continuous-variable quantum cryptography with discrete alphabets: composable security under collective gaussian attacks *Phys. Rev. Res.* **3** 013047

[67] George I, Lin J and Lütkenhaus N 2021 Numerical calculations of the finite key rate for general quantum key distribution protocols *Phys. Rev. Res.* **3** 013274
[68] Zhou H, Sasaki T and Koashi M 2022 Numerical method for finite-size security analysis of quantum key distribution *Phys. Rev. Res.* **4** 033126
[69] Chrzanowski H M, Walk N, Assad S M, Janousek J, Hosseini S, Ralph T C, Symul T and Lam P K 2014 Measurement-based noiseless linear amplification for quantum communication *Nat. Photon.* **8** 333–8
[70] Kanitschar F and Pacher C 2022 Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection *Phys. Rev. Appl.* **18** 034073