

Improvement and security analysis of multi-ring discrete modulation continuous variable quantum secret sharing scheme

Huan-Yao Jiang(姜欢窈), Min Nie(聂敏), Guang Yang(杨光), Ai-Jing Sun(孙爱晶), Mei-Ling Zhang(张美玲), and Chang-Xing Pei(裴昌幸)

Citation: Chin. Phys. B, 2024, 33 (**7**): 070303. DOI: 10.1088/1674-1056/ad3b81
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Broadband multi-channel quantum noise suppression and phase-sensitive modulation based on entangled beam

Ke Di(邸克), Shuai Tan(谈帅), Anyu Cheng(程安宇), Yu Liu(刘宇), and Jiajia Du(杜佳佳)
Chin. Phys. B, 2023, 32 (**10**): 100302. DOI: 10.1088/1674-1056/acd8a8

Improving source-in-the-middle continuous-variable quantum key distribution using a heralded hybrid linear amplifier

Lei-Xin Wu(伍磊鑫), Yan-Yan Feng(冯艳艳), and Jian Zhou(周健)
Chin. Phys. B, 2023, 32 (**7**): 070310. DOI: 10.1088/1674-1056/ac9b39

Analysis of atmospheric effects on the continuous variable quantum key distribution

Tao Liu(刘涛), Shuo Zhao(赵硕), Ivan B. Djordjevic, Shuyu Liu(刘舒宇), Sijia Wang(王思佳), Tong Wu(吴彤), Bin Li(李斌), Pingping Wang(王平平), and Rongxiang Zhang(张荣香)
Chin. Phys. B, 2022, 31 (**11**): 110303. DOI: 10.1088/1674-1056/ac6b1f

Parameter estimation of continuous variable quantum key distribution system via artificial neural networks

Hao Luo(罗浩), Yi-Jun Wang(王一军), Wei Ye(叶炜), Hai Zhong(钟海), Yi-Yu Mao(毛宜钰), and Ying Guo(郭迎)
Chin. Phys. B, 2022, 31 (**2**): 020306. DOI: 10.1088/1674-1056/ac2807

Quantum metrology with coherent superposition of two different coded channels

Dong Xie(谢东), Chunling Xu(徐春玲), and Anmin Wang(王安民)
Chin. Phys. B, 2021, 30 (**9**): 090304. DOI: 10.1088/1674-1056/ac0bae

---

Improvement and security analysis of multi-ring discrete modulation continuous variable quantum secret sharing scheme

Huan-Yao Jiang(姜欢窈)[1,†], Min Nie(聂敏)[1], Guang Yang(杨光)[1], Ai-Jing Sun(孙爱晶)[1], Mei-Ling Zhang(张美玲)[1], and Chang-Xing Pei(裴昌幸)[2]

[1] *School of Communications and Information Engineering & School of Artificial Intelligence, Xi'an University of Posts and Telecommunications, Xi'an* 710121, *China*

[2] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*

(Received 26 December 2023; revised manuscript received 29 February 2024; accepted manuscript online 7 April 2024)

In order to avoid the complexity of Gaussian modulation and the problem that the traditional point-to-point communication DM-CVQKD protocol cannot meet the demand for multi-user key sharing at the same time, we propose a multi-ring discrete modulation continuous variable quantum key sharing scheme (MR-DM-CVQSS). In this paper, we primarily compare single-ring and multi-ring M-symbol amplitude and phase-shift keying modulations. We analyze their asymptotic key rates against collective attacks and consider the security key rates under finite-size effects. Leveraging the characteristics of discrete modulation, we improve the quantum secret sharing scheme. Non-dealer participants only require simple phase shifters to complete quantum secret sharing. We also provide the general design of the MR-DM-CVQSS protocol. We conduct a comprehensive analysis of the improved protocol's performance, confirming that the enhancement through multi-ring M-PSK allows for longer-distance quantum key distribution. Additionally, it reduces the deployment complexity of the system, thereby increasing the practical value.

Keywords: discrete modulation, continuous variable, quantum secret sharing scheme

PACS: 03.67.Hk, 03.67.Dd, 03.67.–a **DOI:** 10.1088/1674-1056/ad3b81

1. Introduction

Secret sharing[1,2] is a kind of special cryptographic protocol, which is mainly produced in order to let multiple participants manage the key together and reduce the risk of key leakage. With the rapid development of quantum information, the extension of secret sharing to quantum states has received extensive attention in the theoretical field,[3,4] quantum secret sharing (QSS) is a secret sharing protocol based on quantum technology, which uses the physical laws of quantum mechanics to securely deliver multiple keys to a group of remote users.[5,6] Only when these users work together can they jointly share an unconditionally secure quantum key.[7]

According to the encoding mode at the source end, QSS can be categorized into discrete variable quantum secret sharing scheme (DV-QSS) and continuous variable quantum secret sharing scheme (CV-QSS).[8–10] In the DV protocol, the key information is modulated onto the canonical components of the light field; for example, the orthogonal phase and the orthogonal amplitude of the light field. The typical DV protocol is the BB84 protocol,[11] where the receiver uses coherent detection to obtain the key. In terms of the generated key rate, the CV protocol holds more advantages. Unlike the DV protocol, the CV protocol does not require selecting a measurement basis. It allows simultaneous measurement of both phase and amplitude information. In contrast, the DV protocol is limited to measuring only one of the orthogonal variables.

According to the modulation mode of the coherent state, it can be divided into Gaussian modulation (GM) protocol[12] and discrete modulation (DM) protocol. GM is able to achieve high key rates because the coherent state distribution follows a continuous Gaussian distribution, allowing for more locations on the optical phase space. However, since GM is only a theoretical idealization, in practice the modulator has a limited range and precision.[13] Although there are many related techniques to improve the efficiency of Gaussian modulation, the calculation involved has a high cost, which reduces the application of Gaussian modulation in practice. On the contrary, since the coherent state distribution of discrete modulation is not continuous but discrete, it can accommodate more excess noise. In the case of discrete modulation, the legitimate parties can use advanced error correction codes, so that it has a higher key rate[14] over long transmission distances under different signal-to-noise ratios. The DM protocol can make use of the high efficiency and easy realization of homodyne or heterodyne detection in GM protocol, and at the same time it can make use of the high efficiency modulation and error correction mechanism of discrete variable protocol, which provides a new direction for the development of long-distance DM protocol.

The concept of quantum secret sharing was first proposed in 1999 based on the three-particle entangled state GHZ.[3] In 2013, Hoi-Kwan Lau and Christian Weedbrook extended the cluster-state quantum secret sharing form to the continuous

[†]Corresponding author. E-mail: 1134319164@qq.com

© 2024 Chinese Physical Society and IOP Publishing Ltd

variable mechanism.[15] In 2019, Everrier *et al.* established a lower bound on the key rate by formulating the problem as a semi-definite program. At the same time, it is applied to more complex QAM modulation. This opened the way for complete security of discrete modulation continuous variable variable protocol.[16] In 2021, Margarida Almeida *et al.* investigated the application of multi-ring M-DM in quantum key distribution, where the maximum transmission distance of 4-ring 64-PSK could reach nearly three times that of 8-PSK.[17] In 2023, Qin Liao applied multi-ring M-DM to QSS, and the error probability of multi-ring discretely-modulated coherent states (DMCS) was much lower than that of the original single-ring discretely-modulated CVQSS.[18]

Inspired by the discrete modulated continuous variable quantum key distribution scheme (DM-CV-QKD),[19,20] we apply the multi-ring M-PSK constellation scheme to our quantum secret sharing method. Here, each participant utilizes a simple phase shifter instead of a complex laser and modulator to facilitate the quantum secret sharing process. This adaptation is driven by the increasing demand for secure key sharing among multiple users. We present the general design of the CVQSS protocol for multi-ring discrete modulation. We conduct a thorough performance analysis of our improved protocol and compare it with three other CVQSS protocols proposed to date. Our results confirm that our proposed enhancements enable longer-distance quantum secret sharing, while also reducing the deployment complexity and cost of quantum secret sharing systems through the utilization of discrete modulation constellation graphs' characteristics.

The structure of this article is as follows. In Section 2, we propose the general design of the multi-ring M-DM-CVQSS protocol. Section 3 provides calculations for the asymptotic key rate as well as the key rate under finite-size effects. In Section 4, we perform a performance analysis. Section 5 gives our conclusions and future prospects.

2. M-PSK quantum secret sharing protocol

In the basic DM-CVQSS modulation method, we aim to increase the amount of information carried by each coherent state by increasing the number of coherent states. However, there are limits to what can be achieved by simply increasing the number of coherent states in a ring (see Appendix B).[17,21] To address this issue, we can apply a multi-ring structure to DM-CVQSS, allowing for different amplitude discrete modulations of coherent states with phase shift keying (PSK) modulation, thereby obtaining coherent states with different amplitudes. The multi-ring structure can increase the key distribution rate of QSS.[18]

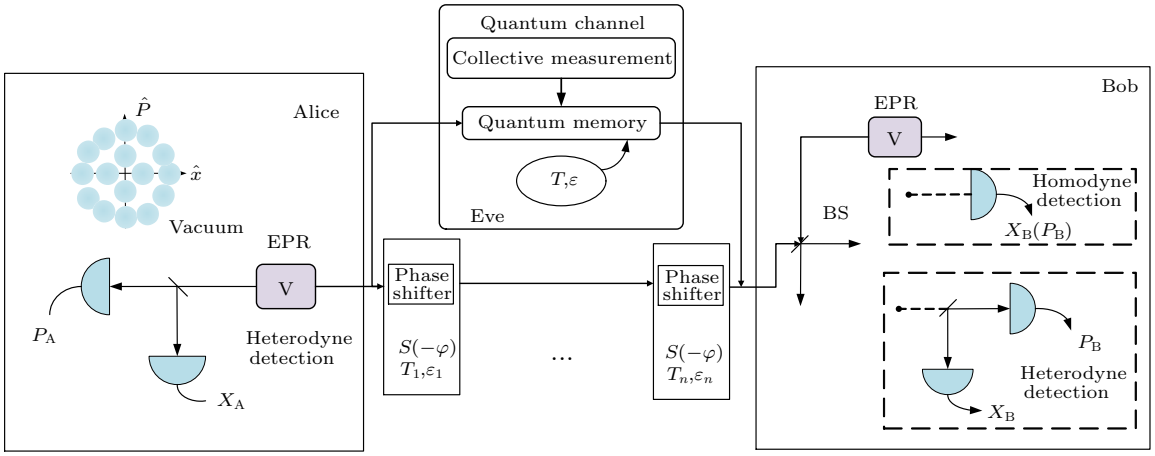


Fig. 1. Entanglement-based scheme for the MR-DM-CVQSS with homodyne or heterodyne detection.

In traditional QSS, each participant is equipped with a laser and a modulator. When the participant's communication device is replaced with a phase shifter and the modulation mode is altered, the entire quantum communication system only needs to require the initial user to employ a laser and a modulator to prepare the quantum state. Subsequently, a heterodyne detector is utilized at the legitimate user's end to detect the quantum state.[22] Therefore, the whole communication system reduces the use of communication devices, thus simplifying its deployment difficulty and reducing the deployment cost of communication system. This allows legitimate users to share secrets with multiple remote users over unsecured quantum channels. Researchers equate the QSS protocol to the entanglement-based scheme[23] of CVQKD for analysis, as depicted in the system diagram in Fig. 1. Therefore, we can directly use the security analysis method of DM-CVQKD to study the security of DM-CVQSS. In this protocol, we primarily consider (n,n) threshold schemes, where the original secret can only be correctly and completely recovered when all users cooperate simultaneously. In this scenario, the first user (Alice) and the dealer (Bob) are responsible for preparing and measuring quantum states, while the remaining par-

ticipants only need to perform phase shift operations on the quantum states to complete quantum secret sharing. In the subsequent security analysis, we base our assessment on the quantum channel length and excess noise between Alice and Bob, while the operations on quantum states by other participants are considered as channel noise.[24]

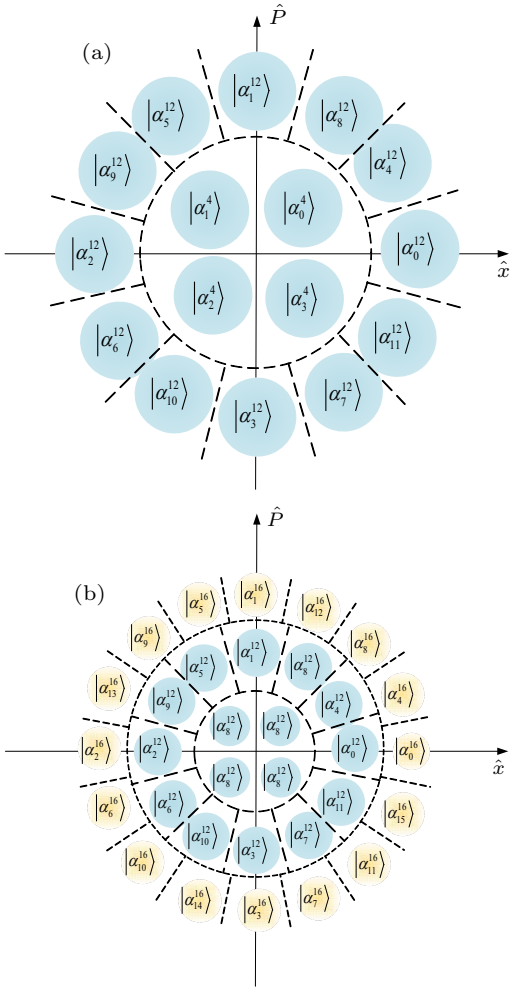


Fig. 2. Panel (a) shows the double-ring 16-PSK (4–12), and panel (b) shows the triple-ring 32-PSK (4–12–16).

DM-CVQSS mainly consists of two parts: the first is the quantum part of the communication between the two parties to exchange quantum states and obtain the relevant variables, and the second is the classical post-processing process to extract the same key from the relevant variables. In the preparation and measurement scheme, Alice chooses M ($M=2^l$) base modulation to select coherent states with a certain probability, assuming that the probability of choosing each coherent state is equal. The coherent state coding rules are as follows: $\left|\alpha_{a_k mn}^{4a_k}\right\rangle=(a_k;m,n)$, where $4a_1+4a_2+4a_3+\cdots+4a_k=2^l=M$, l is the number of code bits, and $4a_k$ is the number of coherent states in each ring. a_k ($a_k=1,2,\ldots$) is the number of groups in each ring. $(a_k;m,n)$, where a_k is the binary number corresponding to the group number arranged from the inner ring to the outer ring. There are only four coherent states in each group. As shown in Fig. 2, in 16-PSK (4–12) there is one group in the inner ring and three groups in the outer ring. In 32-PSK (4–12–16), there is one group in the inner ring, three groups in the middle ring, and four groups in the outer ring. The significance of this grouping is that in the case of not knowing which coherent state Alice sends, after the participant performs the phase shift operation, the coherent state will only fall into the corresponding grouping and will not fall into the illegal region. In Fig. 2, Alice probabilistically selects a coherent state, and in the case of the double-ring 16-state (assuming equal probability for each coherent state), the probability of choosing a coherent state from the inner ring is $1/4$, and from the outer ring is $3/4$. Compared with the case of single-ring DM-CVQSS in Ref. [22], the encoding method in this paper is more general.

Taking the double-ring 16-PSK (4–12) protocol as an example, the process of the DM-CVQSS protocol is as follows:

Step 1 Alice selects a random bit string of length $4L$ ($x=(x_0,x_1,\ldots,x_{4L-1})$), and encodes the continuous bit string into the coherent state of the form $\left|\alpha_k^N\right\rangle=\left|\hat{x}_{\mathrm{A}}+\mathrm{i}\hat{p}_{\mathrm{A}}\right\rangle=\left|\alpha_r\exp(\frac{2\mathrm{i}k}{N})\right\rangle$, $k\in\{0,1,\cdots,N-1\}$, where α_r corresponds to the radius (amplitude) of the r-th ring. Afterward, $\left|\alpha_k^N\right\rangle$ is transmitted to the next neighboring participant P_2 via an untrusted quantum channel. In the original DM-CVQSS protocol, $k=8x_0+4x_1+2x_2+x_3$.

Step 2 Participant P_1 performs a phase shift operation on the coherent state sent by Alice using a phase shifter and then forwards it to the next participant. The phase shift operation can use $\varphi=\left\{0,\frac{\pi}{2},\frac{3\pi}{2},2\pi\right\}$, corresponding to the coding $\{(0,0),(0,1),(1,0),(1,1)\}$, which is equivalent to counterclockwise rotation in the phase space. The matrix is expressed as

$$S(-\varphi)=\begin{pmatrix}\cos\varphi & -\sin\varphi\\ -\sin\varphi & \cos\varphi\end{pmatrix}. \tag{1}$$

According to the encoding rules, participant P_1 gets the key K_1.

Step 3 Participants P_2 to P_n do the same as P_1, that is, phase shifting the coherent state sent by the previous participant, and then they send the coherent state to the next participant via a quantum channel. According to the same encoding rules, participants P_2 to P_n get the original keys K_2 to K_n respectively.

Step 4 For Bob, the two quadrature components are measured using heterodyne detection, and at the same time, this string is transformed into a $4L$-bit original key. The transformation rules and the phase diagram are shown in Fig. 3:

$$\begin{cases}\left|\alpha_{000}^4\right\rangle=(0,0,0,0),\\ \left|\alpha_{001}^4\right\rangle=(0,0,0,1),\\ \left|\alpha_{010}^4\right\rangle=(0,0,1,0),\\ \left|\alpha_{011}^4\right\rangle=(0,0,1,1),\end{cases} \tag{2}$$

$$\begin{cases} \left|\alpha_{1mn}^{12}\right\rangle = (0,1,m,n), & \frac{\pi}{2}(2m+n) - \frac{\pi}{12} \le z \le \frac{\pi}{2}(2m+n) + \frac{\pi}{12}, \\ \left|\alpha_{2mn}^{12}\right\rangle = (1,0,m,n), & \frac{\pi}{2}(2m+n) + \frac{\pi}{12} \le z \le \frac{\pi}{2}(2m+n) + \frac{\pi}{4}, \\ \left|\alpha_{3mn}^{12}\right\rangle = (1,1,m,n), & \frac{\pi}{2}(2m+n) + \frac{\pi}{4} \le z \le \frac{\pi}{2}(2m+n) + \frac{5\pi}{12}. \end{cases} \tag{3}$$

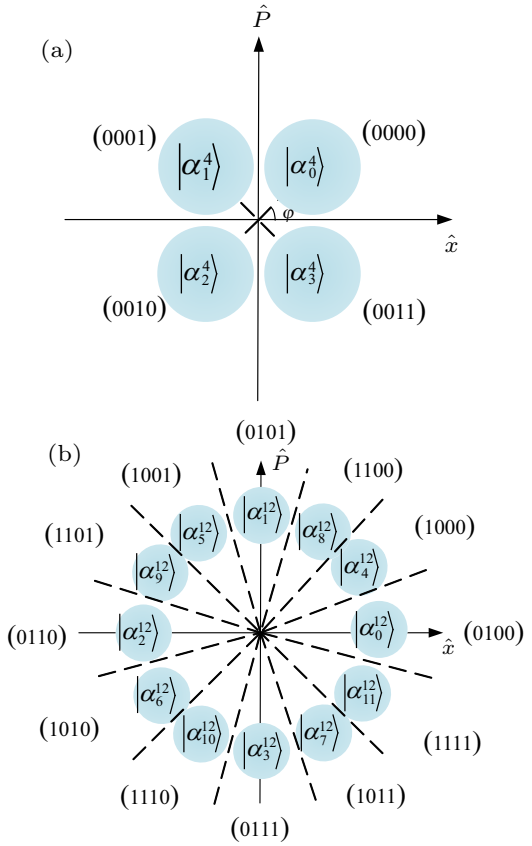


Fig. 3. Panel (a) shows that the inner ring has four states and panel (b) shows that the outer ring has 12 states.

Step 5 The above steps are repeated multiple times, followed by the classical post-processing stage. Between Alice, Bob and the participants, they can proceed with reverse reconciliation.[25] After Bob completes the measurement in the reconciliation phase, the message M is encoded as $E = M \oplus K$, where $\oplus$ represents modulo-2 addition and $K = K_1 \oplus K_2 \cdots K_n$. The encoded message E is then broadcast through the classical channel to correct the modulation information held by Alice and the participants. In general, even in the absence of eavesdropping and any channel noise, the classical value decoded by Bob differs from the initial value sent by Alice due to inherent quantum uncertainty.[21] Alice and Bob conduct parameter estimates to determine the amount of information likely to be obtained by Eve's eavesdroppers. Simultaneously, based on the channel estimation parameters, the amplitude α_r can be flexibly adjusted. Finally, Alice and Bob continue this process until they have collected enough data to perform classical error correction and privacy amplification, resulting in a shared key that is completely unknown to potential adversaries.

3. Key rate calculation

What Bob receives is a mixed state represented by the density matrix as follows:

$$\rho_N = \frac{1}{N}\sum_{k=0}^{N-1} \left|\alpha_k^N\right\rangle \left\langle\alpha_k^N\right|. \tag{4}$$

For performance analysis, the mixed state is purified:

$$\begin{aligned} \left|\Phi_N\right\rangle &= \sum_{k=0}^{N-1} \sqrt{\xi_k^N}\left|\phi_k^N\right\rangle \left|\phi_k^N\right\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \left|\psi_k^N\right\rangle \left|\alpha_k^N\right\rangle, \end{aligned} \tag{5}$$

where $\xi_k^N = \mathrm{e}^{-\alpha^2}\sum\limits_{n=0}^{\infty}\frac{\left(\alpha^2\right)^{Nn+k}}{(Nn+k)!}$.

$$\left|\phi_k^N\right\rangle = \frac{\mathrm{e}^{-\frac{\alpha^2}{2}}}{\sqrt{\xi_k^N}}\sum_{n=0}^{\infty}(-\mathrm{i})^{\frac{Nn}{2}}\frac{\alpha^{Nn+k}}{(Nn+k)!}\left|Nn+k\right\rangle, \tag{6}$$

$$\left|\psi_k^N\right\rangle = \frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}\mathrm{e}^{\mathrm{i}\frac{(1+2k)m\pi}{N}}\left|\phi_m^N\right\rangle. \tag{7}$$

At the Bob end, the received quantum state $\left|\beta^N\right\rangle$ is measured using homodyne or heterodyne detection. In heterodyne detection, the signal is divided using a beam splitter, and the two conjugate quadratures $\hat{x}$ and $\hat{p}$ are measured. This process results in obtaining the quantum state $\left|\beta^N\right\rangle = \left|\hat{x}_{\mathrm{B}} + \mathrm{i}\hat{p}_{\mathrm{B}}\right\rangle$. In the entanglement-based scheme, the covariance matrix of the dichotomous states is expressed as

$$\gamma_{\mathrm{AB}}^N = \begin{pmatrix} XI_2 & Z_N\sigma_z \\ Z_N\sigma_z & YI_2 \end{pmatrix}. \tag{8}$$

After transmission through a quantum channel with channel transmittance of T and channel excess noise of ζ, Bob performs projection measurement and its covariance matrix is as follows:

$$\gamma_{\mathrm{AB}}^{\prime N} = \begin{pmatrix} VI_2 & \sqrt{T}Z_N\sigma_z \\ \sqrt{T}Z_N\sigma_z & T(V+\chi_{\mathrm{line}})I_2 \end{pmatrix}, \tag{9}$$

where $I_2 = \mathrm{diag}(1,1)$, $\sigma_z = \mathrm{diag}(1,-1)$.

$$\begin{aligned} X &= \left\langle\Phi_N\right| 1 + 2a^{\dagger}a \left|\Phi_N\right\rangle \\ &= \left\langle\Phi_N\right| 1 + 2b^{\dagger}b \left|\Phi_N\right\rangle = 1 + 2\alpha^2, \end{aligned} \tag{10}$$

where $\hat{a}$, $\hat{a}^{\dagger}$ and $\hat{b}$, $\hat{b}^{\dagger}$ are annihilation and production operators on the Alice and Bob modules, respectively. The formula for calculating Z_N is as follows:

$$Z_N = \left\langle\Phi_N\right| \hat{a}\hat{b} + \hat{a}^{\dagger}\hat{b}^{\dagger} \left|\Phi_N\right\rangle$$

$$= 2\alpha^2 \sum_{i=0}^{N-1} \frac{\left(\xi_{k-1}^N\right)^{3/2}}{\left(\xi_k^N\right)^{1/2}}. \tag{11}$$

The ξ_k^N expression is an infinite sum, and we can use the discrete Fourier transform to simplify the calculation (see Appendix A).

Since the reverse reconciliation scheme can break the 3-dB limit and reduce the messages obtained by Eve, the reverse reconciliation scheme is commonly used in most security analyses. At the same time, because Gaussian attack is the optimal[26,27] in all collective attacks, we can directly use the covariance matrix between Alice and Bob under Gaussian attack to calculate the security bitrate. The analysis of CVQSS can be greatly simplified. In the reverse reconciliation, Gaussian collective attack, Bob adopts a heterodyne detection system security rate[28]

$$\mathrm{SKR} = \beta I(\mathrm{A};\mathrm{B}) - \chi_{\mathrm{Holevo}}(\mathrm{B};\mathrm{E}), \tag{12}$$

where $I(\mathrm{A};\mathrm{B})$ is Shannon mutual information between Alice's modulation data and Bob's measurement data

$$I(\mathrm{A};\mathrm{B}) = \log \frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}. \tag{13}$$

The reconciliation efficiency in classical post-processing is β, usually between 90% and 95%. The Holevo boundary $\chi_{\mathrm{Holevo}}(\mathrm{B};\mathrm{E})$ between Bob's measurement data and the quantum states held by Eve, which represents the limit of mutual information Eve can extract,

$$\chi_{\mathrm{Holevo}}(\mathrm{B};\mathrm{E}) = S(\rho_E) - \sum_y p(y) S(\rho_{E/y}), \tag{14}$$

where $S(\rho_E)$ is the von Neumann entropy, which can be determined by the symplectic eigenvalues of the symplectic matrix γ_{AB}^N

$$S(E:y) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{4} G\left(\frac{\lambda_i - 1}{2}\right). \tag{15}$$

Here, $G(x) = (1+x)\log_2(1+x) - x\log_2(x)$. $\lambda_{1,2}$ is the symplectic eigenvalue of γ_{AB}^N calculated by

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\varsigma}\right)}. \tag{16}$$

with

$$\begin{cases} \Delta = \det\gamma_a + \det\gamma_b + 2\det\sigma_{ab}, \\ \varsigma = \det\gamma_{\mathrm{AB}}^N. \end{cases} \tag{17}$$

The $\lambda_{3,4}$ is the symplantine eigenvalue of the covariance matrix of Alice's modulus after Bob's heterodyne detection

$$\lambda_{3,4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)}, \tag{18}$$

where C and D are given by

$$C_{\mathrm{het}} = \frac{\Delta\chi_{\mathrm{het}}{}^2 + \varsigma + 1 + 2\chi_{\mathrm{het}}B + 2TZ_N^2}{\left[(V+\chi_{\mathrm{tot}})T\right]^2}, \tag{19}$$

$$D_{\mathrm{het}} = \frac{\left(V + \sqrt{\varsigma}\chi_{\mathrm{het}}\right)^2}{\left[(V+\chi_{\mathrm{tot}})T\right]^2}, \tag{20}$$

with $B = V\sqrt{\varsigma} + T(V+\chi_{\mathrm{line}})$.

According to the system block diagram of the entanglement-based scheme, Alice and Bob are located at both ends of the system, and the other N participants are evenly distributed between Alice and Bob. Therefore, according to CVQSS security analysis method, the key rate of the whole system is the key rate between Alice and Bob, and the operation of other participants on the quantum state prepared by Alice is equivalent to interference noise, so it is generally equivalent to channel noise.

The characteristics of the channel can be described by two parameters. One is the channel transmittance T, and the other is the channel excess noise ε. Channel transmittance T in DM-QSS can be regarded as the farthest distance among the participants, that is, the distance between Alice and Bob. The channel transmittance of the j-th participant can be expressed as

$$T_j = 10^{-\frac{\mu l_j}{10}}, \tag{21}$$

where $l_j = \frac{n-j+1}{n}L$ is the distance between Alice and the j-th participant. μ means the loss coefficient of optical fibers, the unit is dB/km, usually takes 0.2 dB/km.

Channel excess noise ε is the sum of the noise generated by n participants, and the channel excess noise of the j-th participant can be expressed as

$$\varepsilon_j = \frac{T_j}{T_1}\varepsilon_0. \tag{22}$$

The total added noise of the channel in the unit of shot noise can be expressed as[24]

$$\chi_{\mathrm{line}} = \frac{1}{T_1} - 1 + \sum_{j=1}^{n} \varepsilon_j. \tag{23}$$

The detector at the Bob side can be represented by the detection efficiency η and the electrical noise $\varepsilon_{\mathrm{ele}}$, and the noise under heterodyne detection is expressed as

$$\chi_{\mathrm{het}} = [1 + (1-\eta) + 2\varepsilon_{\mathrm{ele}}]/\eta. \tag{24}$$

In the case of reconciliation, the total noise is

$$\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{het}}/T. \tag{25}$$

Since it is impossible to exchange infinite data between Alice and Bob in the actual situation, the finite-size effect is closer to the actual situation.[29] The key rate under the finite-size effect is calculated as follows:[25]

$$\mathrm{SKR}_{\mathrm{fin}} = \frac{n}{M}\left(\beta I(\mathrm{A};\mathrm{B}) - \chi_{\varepsilon_{\mathrm{PA}}}(\mathrm{B};\mathrm{E}) - \Delta(n)\right), \tag{26}$$

where M represents the total number of signals in the protocol used for the exchange, and n represents the number of signals used for the final key generation. The algorithm between mutual information is consistent with the asymptotic key rate, and β is the reconciliation efficiency. $\chi_{\in PE}(\mathrm{B};\mathrm{E})$ is defined as the maximum number of Holevo information that is statistically compatible except for the probability $\varepsilon_{\mathrm{PA}}$, where $\varepsilon_{\mathrm{PA}}$ is the failure probability of parameter estimation, and $\Delta(n)$ is a parameter related to privacy amplification, usually expressed as

$$\Delta(n)=(2\dim H_X+3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}+\frac{2}{n}\log_2(1/\varepsilon_{\mathrm{PA}}). \quad (27)$$

The symbols $\varepsilon_{\mathrm{PA}}$ and $\bar{\varepsilon}$ represent the probability of failure for the privacy amplification procedure and the smoothing parameter, respectively. $\dim H_X$ denotes the Hilbert space of the original key processing, and this paper assumes $\dim H_X=2$, indicating binary encoding. ε represents the overall failure probability of the protocol, given by $\varepsilon=\varepsilon_{PE}+\varepsilon_{EC}+\bar{\varepsilon}+\varepsilon_{\mathrm{PA}}\approx 10^{-10}$. Additionally, the covariance matrix between Alice and Bob is as follows:

$$\gamma_{\mathrm{AB}}=\begin{pmatrix} VI_2 & t_{\min}Z_N\sigma_z \\ t_{\min}Z_N\sigma_z & (t_{\min}^2V_{\mathrm{A}}+\zeta_{\max}^2)I_2 \end{pmatrix}, \quad (28)$$

where $t_{\min}$ and $\zeta_{\max}^2$ denote the minimum value of t and the maximum value of ζ^2, respectively, which are consistent with the sampled data when the error probability is $\varepsilon_{PE}/2$. This is determined by the maximum likelihood estimate

$$\begin{cases} t_{\min}\approx\sqrt{T}-z_{\varepsilon PE/2}\sqrt{\dfrac{1+T\varepsilon}{mV_{\mathrm{A}}}}, \\ \zeta_{\max}^2\approx 1+T\varepsilon+z_{\varepsilon PE/2}\dfrac{\sqrt{2}(1+T\varepsilon)}{\sqrt{m}}. \end{cases} \quad (29)$$

Through the security analysis of DM-CVQSS, we can obtain a positive key rate satisfying composable security.[31] This is because in the general framework for describing cryptographic protocols and analyzing their security,[32] it ensures that the protocol maintains its security under any circumstances.

Many security proofs related to CVQSS do not consider the impact of user device information leakage, making QSS systems vulnerable to Trojan-horse attacks (THAs).[33,34] Eavesdropper (Eve) can inject strong light into the QSS system devices, and by measuring the characteristics of the reflected photons, Eve can obtain information related to the modulation devices. There are typically two ways to defend against the threats posed by THAs. First, from a practical perspective, we can implement methods for real-time detection and monitoring of any potential side channels, and enhance the isolation of relevant devices. Second, from a theoretical analysis perspective, we can relax the strict assumptions of most current security proofs to incorporate these potential impacts into security analysis.[35] In the security analysis of CVQSS, when Eve employs a THA, it always has a certain impact on the excess noise of the CVQSS system. This impact is easily noticed by Alice and Bob, hence the failure of the attack. By incorporating the excess noise generated by Eve into the security analysis, the security boundary of the system is determined.[36]

4. Performance analysis

In this section, we analyze the security of the asymptotic key rate and consider the security of the key rate under finite-size effects. The covariance matrix describing the state between Alice and Bob depends on the parameter Z_N. For arbitrary modulation, the Z^* parameter can be numerically calculated from[13]

$$Z^*(T,\varepsilon)=2\sqrt{T}\,\mathrm{tr}\left(\tau^{1/2}\hat{a}\tau^{1/2}\hat{a}^\dagger\right)-\sqrt{2T\varepsilon\omega}, \quad (30)$$

$$\tau=\sum_{k=0}^{M-1}p_k|\alpha_k\rangle\langle\alpha_k|, \quad (31)$$

where $\omega=\sum_k p_k\left(\langle\alpha_k|\hat{a}_\tau^\dagger\hat{a}_\tau|\alpha_k\rangle-|\langle\alpha_k|\hat{a}_\tau|\alpha_k\rangle|^2\right)$. The density matrix τ is used to describe the state that Alice sends. $\hat{a}_\tau=\tau^{\frac{1}{2}}\hat{a}\tau^{-\frac{1}{2}}$, the $\hat{a}$ and $\hat{a}^\dagger$, respectively, represent Alice's annihilate and produce operators in the system. For Gaussian modulation Z_{G}^* can be computed as follows: $Z_{\mathrm{G}}^*=\sqrt{V_{\mathrm{A}}^2+2V_{\mathrm{A}}}$.

From the Fig. 4, it can be observed that as the number of constellation points increases, the value of Z^* approaches the Gaussian Z_{G}^*. At the same time, we can also see that the value Z^* can be increased by increasing the number of rings. The double-ring 16-PSK is closer to Gaussian Z_{G}^* than the single ring 16-PSK.

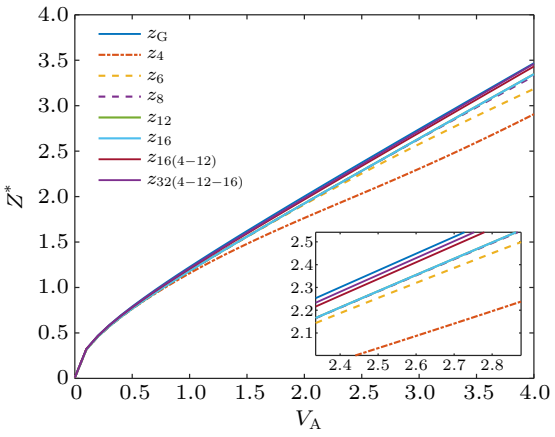


Fig. 4. The Z^* as a function of the modulation variance. The curves from top to bottom are Gaussian modulation, triple-ring 32-PSK, double-ring 16-PSK, 16-PSK, 12-PSK, 8-PSK, 6-PSK, and 4-PSK, in which the inner ring of the double-ring 16-PSK has four states and the outer ring has 12 states. Here $d=10$ km, $\alpha=0.2$ dB/km, $\varepsilon=0.003$.

Figure 5 shows the relationship between key rate and variance, and the key rate corresponds to different optimal modulation variances for different modulation modes and the number of participants. For the double-ring, it is relatively flat near

the maximum key rate, and the modulation variance range is wider than that of the single ring, which increases the flexibility of the system.

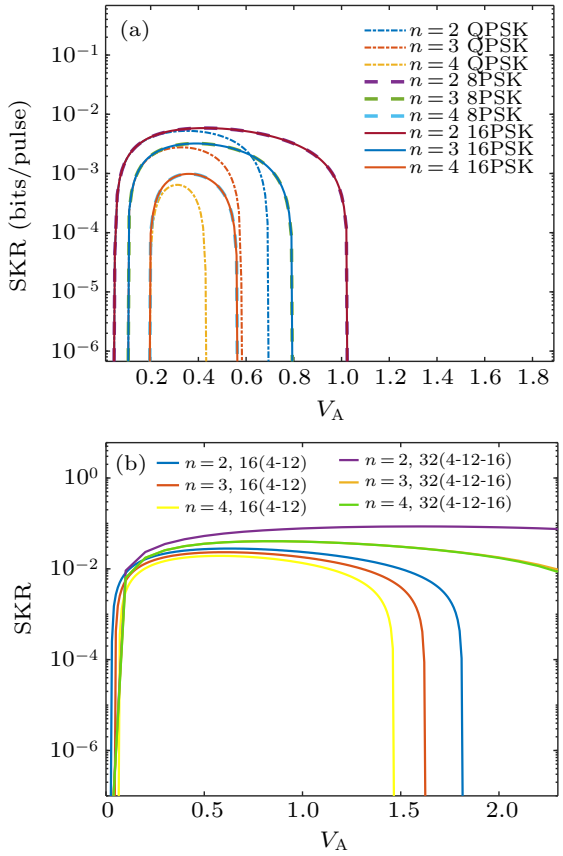


Fig. 5. The relationship between key rate and variance. Panel (a) shows the modulation variance of single-ring 4-PSK, 8-PSK, and 16-PSK in relation to the modulation mode and the number of participants. Panel (b) shows the relationship between the variance and the number of participants for double-ring 16-PSK modulation and triple-ring 32-PSK modulation, from the outside to the inside, respectively, the number of participants is 2, 3, and 4. Here $\alpha = 0.2$ dB/km, $\varepsilon = 0.001$, $\beta = 0.95$, $\eta = 0.6$, $\varepsilon_{\text{ele}} = 0.05$.

The two main factors affecting the mutual information between Alice and Bob are modulation variance and distance. When $V_A = 2.2$ and the distance $d = 100$ km, the mutual information between Alice and Bob decreases by 98%. Numerical results show that the Holevo bound of the curve from bottom to top is GM, triple-ring 32-PSK, double-ring 16-PSK, 16-PSK, 8-PSK, and 4-PSK. GM has the lowest Helevo bound. Under the same modulation variance and transmission distance, GM can extract the largest unknown information of the eavesdropping. In general, achieving absolute Gaussian modulation is usually not feasible due to the differences between the theoretical model and the experimental setup. In fact, since the Gaussian distribution is not only continuous but also unbounded, ideal Gaussian modulation cannot be achieved. It can be proved that the impact on security is not significant when the Gaussian distribution is replaced by a bounded discrete approximation.[37,38]

As can be seen from Fig. 7, the increase in the distance between Alice and Bob is the main source of channel excess noise. Moreover, since the operation of QSS participants on the quantum state is regarded as noise, more participants will generate more excess noise.

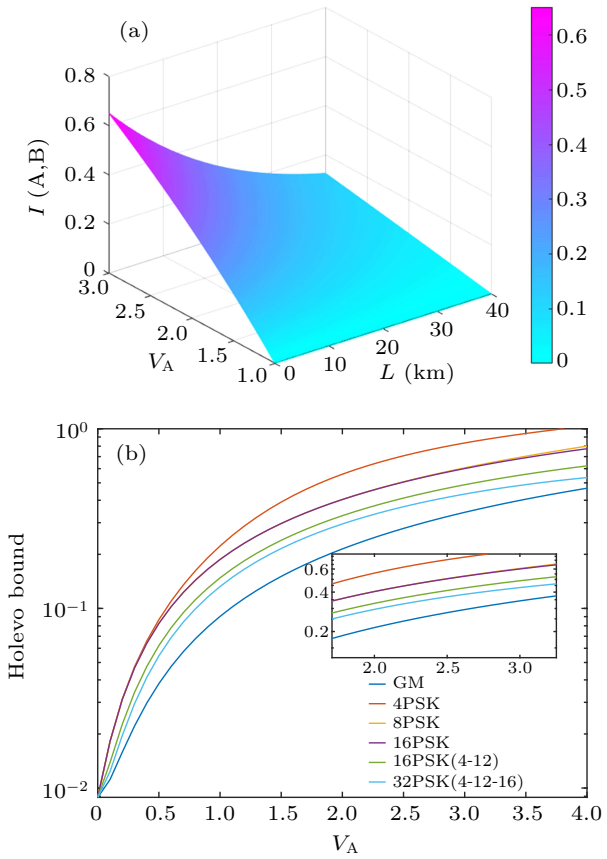


Fig. 6. Panel (a) shows that the mutual information between Alice and Bob is a function of the modulation variance and the distance between the two sides. Panel (b) shows the relationship between Holevo and variance. Here $\alpha = 0.2$ dB km, $\varepsilon = 0.001$, $\beta = 0.95$, $\eta = 0.6$, $\varepsilon_{\text{ele}} = 0.05$.

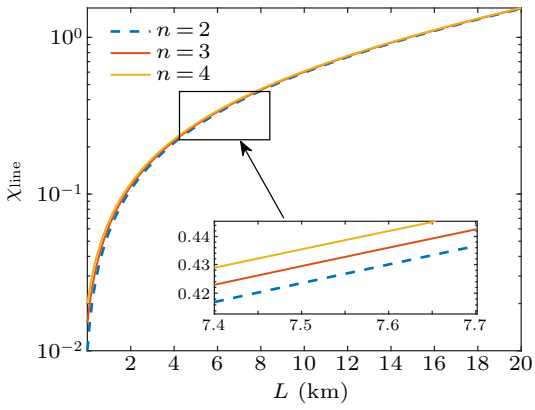


Fig. 7. Channel excess noise is a function of the transmission distance and the number of QSS participants. Here $\alpha = 0.2$ dB/km, $\eta = 0.6$, $\varepsilon_{\text{ele}} = 0.05$, $\varepsilon = 0.001$.

In Fig. 8, the modulation variances for all modulation methods have been optimized. We can conclude that increasing the number of coherent states can increase the information content of each quantum state, but there are certain limitations on the key rate generated and the transmission distance. Using double-ring constellation modulation can increase the transmission distance and cope with stronger channel excess noise.

From the inside out they are 4-PSK, 8-PSK (16-PSK), double-ring 16-PSK, triple-ring 32-PSK, and GM.

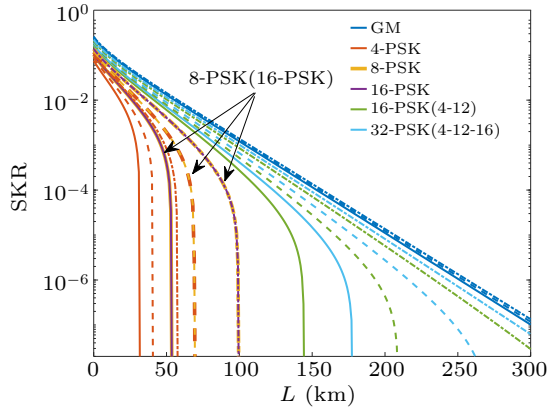


Fig. 8. The relationship between key rate and transmission distance in the asymptotic case. Among them, the channel excess noise of the dot solid line $\varepsilon = 0.001$, the channel excess noise of the dotted line is $\varepsilon = 0.003$, and the channel excess noise of the solid line $\varepsilon = 0.005$. Here $\alpha = 0.2$ dB/km, $\beta = 0.95$, $\eta = 0.6$, $\varepsilon_{\text{ele}} = 0.05$.

Figure 9 shows the relationship between the secret key rate, distance, and the number of participants under finite-size effects. The modulation variances for all modulation methods have been optimized. From the inner to the outer, they are 4-PSK, 8-PSK (16-PSK), dual-ring 16-PSK, triple-ring 32-PSK, and GM. The solid line is $M = 10^9$, the dashed line is $M = 10^{11}$, and the dotted-dashed line is $M = 10^{14}$. Under the finite-size effect, as the number of information exchange increases and Alice and Bob's knowledge of quantum channel increases, the key rate of the finite-size effect will gradually approach the asymptotic key rate.

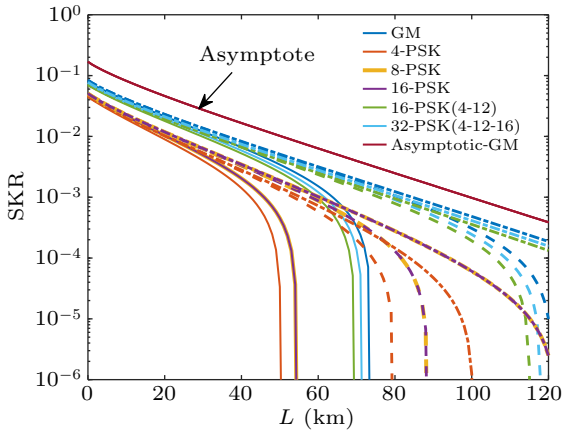


Fig. 9. The relationship between key rate and distance and number of participants under finite-size effect. We consider $\alpha = 0.2$ dB/km, $\beta = 0.9$, $\eta = 0.6$, $\varepsilon_{\text{ele}} = 0.05$, $\varepsilon = 0.001$, $\varepsilon = \varepsilon_{PE} = \varepsilon_{EC} = \bar{\varepsilon} = \varepsilon_{\text{PA}} \approx 10^{-10}$, and $n/M = 0.5$.

5. Conclusion

The practicality and performance of the QSS system are enhanced overall by simplifying the instruments and equipment through the use of discrete modulation. This is achieved by employing discrete modulation, including double-ring or even multi-ring discrete modulation, to approximate the performance of Gaussian modulation. In this paper, on the basis of the original four states and eight states, double-ring 16-PSK and triple-ring 32-PSK are used, and the distribution characteristics of the inner ring and the outer ring are utilized, and an angle phase shifter is used to complete the process. At the end of this paper, the relationship between the key rate and the modulation variance, that is, the average number of photons per pulse, was comprehensively analyzed and the maximum variance value of the key rate was obtained under different numbers of participants. At the same time, we obtain the relationship between the key rate magnitude and the modulation scheme. Finally, considering the actual situation, the relationship between the key rate and the number of participants and the transmission distance under the finite-size effect is given.

Constellation shaping and probability shaping are effective approaches to enhancing the key rate. In scenarios with low channel transmittance and high excess noise, M-QAM modulation can yield a positive SKR.[30] In M-QAM, M coherent states are modulated to be equidistant from each other in the optical phase space. By assigning a non-uniform probability to each coherent state, M-QAM can be adjusted to a discrete Gaussian distribution to further increase the mutual information between Alice and Bob. Therefore, how to use the distribution of M-QAM space to apply it to quantum secret sharing scheme and how to the reverse reconciliation remain to be solved.

Appendix A: Simplify the summation

The ξ_k^N contains an infinite sum. We can simplify it using discrete Fourier transform[13]

$$\xi_k^N = \mathrm{e}^{-\alpha^2} \sum_{n=0}^{\infty} \frac{(\alpha^2)^{Nn+k}}{(Nn+k)!}.$$

Define ν_j as follows:

$$\begin{aligned}\nu_j :&= \sum_{k=0}^{N-1} \mathrm{e}^{ijk\theta} \xi_k = \sum_{k=0}^{N-1} \sum_{n=0}^{\infty} \mathrm{e}^{ijk\theta} \frac{(\alpha^2)^{Nn+k}}{(Nn+k)!} \\ &= \sum_{m=0}^{\infty} \mathrm{e}^{ijm\theta} \frac{\alpha^{2m}}{m!} = \mathrm{e}^{\alpha^2 \mathrm{e}^{ij\theta}},\end{aligned}$$

where $\mathrm{e}^{ijn\theta} = \mathrm{e}^{ij(n \bmod M)\theta}$. Using the inverse Fourier transform, we can obtain

$$\xi_k^N = \frac{1}{M} \sum_{k=0}^{N-1} \mathrm{e}^{-ijk\theta} \mathrm{e}^{\alpha^2 \mathrm{e}^{ij\theta}}.$$

Appendix B

In classical PSK communication, we can increase the amount of information carried by each symbol by increasing the number of symbols. According to information theory, taking binary as an example, two symbols carry 1 bit of information, four symbols carry 2 bits, eight symbols carry 3 bits,

and 16 symbols can carry 4 bits of information.[39] However, in CVQSS communication, simply increasing the number of coherent states does not increase the key rate. This is because we can compare it with the equivalent excess noise of discrete modulation. The channel transmittance T_{G} and channel excess noise ε_{G} of the quantum channel are defined as

$$T_{\mathrm{G}} = \frac{T}{F} \approx T,$$
$$\varepsilon_{\mathrm{G}} = F\varepsilon + (F-1)V_{\mathrm{A}} \approx \varepsilon + (F-1)V_{\mathrm{A}},$$

where $F = (Z_{\mathrm{G}}/Z_{\mathrm{d}})^2$. The equivalent excess noise under discrete modulation can be expressed as $\Delta\varepsilon = (F-1)V_{\mathrm{A}}$.[14] The following figure shows the relationship between the equivalent excess noise and the modulation variance for 4-PSK, 8-PSK, and 16-PSK.

From Fig. B1, we can see that the equivalent excess noise for single-ring 16-state modulation is slightly lower than that for single-ring 8-state modulation, but the difference is not significant.

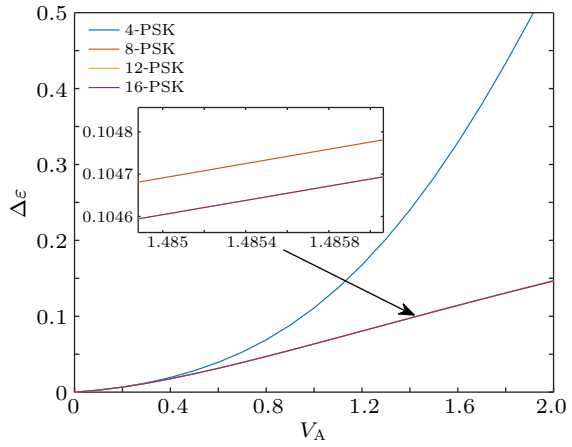


Fig. B1. The relationship between equivalent excess noise and variance for discrete modulation.

Acknowledgement

Project supported by the National Natural Science Foundation of China (Grant Nos. 61971348 and 61201194).

References

[1] Blakley G R 1979 *Managing Requirements Knowledge, International Workshop on* IEEE-CS p. 313
[2] Adi S 1979 *Commun. ACM* **22** 612
[3] Hillery M, Buek V and Berthiaume 2002 *Phys. Rev. A* **59** 1829
[4] Cleve R, Gottesman D and Lo H K 2002 *Phys. Rev. Lett.* **83** 648
[5] Wootters W K and Zurek W H 1982 *Nature* **299** 125012
[6] Bang J Y and Berger M S 2006 *Phys. Rev. D* **74** 125012
[7] Pirandola S, Andersen U L, Banchi L, *et al.* 2020 *Adv. Opt. Photon.* **12** 1012
[8] Pirandola S, Ottaviani C, Spedalieri G, *et al.* 2015 *Nat. Photonics* **9** 397
[9] Leverrier A and Grangier P 2011 *Phys. Rev. A* **83** 042312
[10] Leverrier A, Grangier P 2009 *Phys. Rev. Lett* **102** 180504
[11] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[12] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[13] Denys A, Brown P and Leverrier A 2021 *Quantum* **5** 540
[14] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[15] Lau H K and Weedbrook C 2013 *Phys. Rev. A* **88** 042313
[16] Ghorai S, Grangier P, Diamanti E, *et al.* 2019 *Phys. Rev. X* **9** 021059
[17] Almeida M, Pereira D, Muga N J, *et al.* 2021 *Opt. Express* **29** 38669
[18] Liao Q, Liu X, Ou Bo and Fu X 2023 *IEEE Trans. Commun* **71** 6051
[19] Weedbrook C,Pirandola S, García-Patrón R, *et al.* 2012 *Rev. Mod. Phys* **84** 621
[20] Djordjevic I 2019 *IEEE Photonics Journal* **11** 1
[21] Becerra F E, Fan J, Baumgartner G, *et al.* 2013 *Nat. Photonics* **7** 147
[22] Ding J Z 2022 *Research on Improvement of Discrete Modulation Continuous Variable Quantum Key Distribution Scheme* (Hunan: Central South University) (in Chinese)
[23] Curty M, Lewenstein M and Lütkenhaus N 2004 *Phys. Rev. Lett.* **92** 217903
[24] Grice W P and Qi B 2019 *Phys. Rev. A* **100** 022339
[25] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343
[26] Navascués M, Grosshans F and Acin A 2006 *Phys. Rev. Lett.* **97** 190502
[27] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett* **97** 190503
[28] Lodewyck J, Bloch M, García-Patrón R, *et al.* 2007 *Phys. Rev. A* **76** 042305
[29] Chen Z, Zhang Y, Wang G, Li Z and Guo H 2022 *Phys. Rev. A* **98** 012314
[30] Sayat M, Shajilal B, Kish S P, *et al.* 2022 *IEEE Trans. Commun.* **98** 012314
[31] Furrer F, Franz T, Berta M, *et al.* 2012 *Phys. Rev. Lett.* **109** 100502
[32] Canetti R 2001 *Proceedings* 42*nd IEEE Symposium on Foundations of Computer Science* p. 136
[33] Jain N, Anisimova E, Khan I, *et al.* 2014 *New J. Phys.* **16** 123030
[34] Stiller B, Khan I, Jain N, *et al.* 2015 *Conference on Lasers and Electro-Optics* p. 1
[35] Navarrete Á and Curty M 2022 *Quantum Sci. Technol.* **7** 035021
[36] Pan Y, Zhang L and Huang D 2020 *Appl. Sci.* **10** 7788
[37] Jouguet P, Kunz-Jacques S, Diamanti E, *et al.* 2012 *Phys. Rev. A***86** 032309
[38] Lupo C 2020 *Phys. Rev. A* **102** 022623
[39] Shannon C E 1948 *The Bell System Technical Journal* **27** 379