

Continuous-variable quantum secure direct communication based on *N*-APSK with Boltzmann-Maxwell distribution

Zheng-Wen Cao(曹正文), Yu-Jie Zhang(张昱洁), Geng Chai(柴庚), Zhang-Tao Liang(梁章韬), Xin-Lei Chen(陈欣蕾), Lei Wang(王磊), and Yu-Jie Wang(王禹杰)

Citation: Chin. Phys. B, 2025, 34 (**3**): 030303. DOI: 10.1088/1674-1056/ada549
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Mask-coding-assisted continuous-variable quantum direct communication with orbital angular momentum multiplexing

Zhengwen Cao(曹正文), Yujie Wang(王禹杰), Geng Chai(柴庚), Xinlei Chen(陈欣蕾), and Yuan Lu(卢缘)
Chin. Phys. B, 2025, 34 (**2**): 020308. DOI: 10.1088/1674-1056/ad9ff7

Measurement-device-independent one-step quantum secure direct communication

Jia-Wei Ying(应佳伟), Lan Zhou(周澜), Wei Zhong(钟伟), and Yu-Bo Sheng(盛宇波)
Chin. Phys. B, 2022, 31 (**12**): 120303. DOI: 10.1088/1674-1056/ac8f37

Measurement-device-independent quantum dialogue

Guo-Fang Shi(石国芳)
Chin. Phys. B, 2021, 30 (**10**): 100303. DOI: 10.1088/1674-1056/ac140a

Two-step quantum secure direct communication scheme with frequency coding

Xue-Liang Zhao(赵学亮), Jun-Lin Li(李俊林), Peng-Hao Niu(牛鹏皓), Hong-Yang Ma(马鸿洋), Dong Ruan(阮东)
Chin. Phys. B, 2017, 26 (**3**): 030302. DOI: 10.1088/1674-1056/26/3/030302

Cryptanalysis of quantum broadcast communication and authentication protocol with a one-time pad

Ya Cao(曹雅), Fei Gao(高飞)
Chin. Phys. B, 2016, 25 (**11**): 110305. DOI: 10.1088/1674-1056/25/11/110305

SPECIAL TOPIC — Quantum communication and quantum network

Continuous-variable quantum secure direct communication based on N-APSK with Boltzmann–Maxwell distribution

Zheng-Wen Cao(曹正文), Yu-Jie Zhang(张昱洁), Geng Chai(柴庚)†, Zhang-Tao Liang(梁章韬), Xin-Lei Chen(陈欣蕾), Lei Wang(王磊), and Yu-Jie Wang(王禹杰)

Laboratory of Quantum Information and Technology, School of Information Science and Technology, Northwest University, Xi'an 710127, *China*

(Received 29 September 2024; revised manuscript received 20 December 2024; accepted manuscript online 3 January 2025)

Continuous-variable quantum secure direct communication (CVQSDC) with Gaussian modulation (GM) demands a considerable quantity of random numbers during the preparation process and encodes them separately on the quadrature components of the quantum states. Hence, high-speed random number generators are required to satisfy this demand, which is difficult to implement in practical applications. CVQSDC with discrete modulation (DM), correspondingly, employs a finite number of quantum states to achieve encoding, which can circumvent the shortcomings of the GM scheme. Based on the advantages of DM, the issue of attaining the most optimal secrecy capacity and communication distance remains to be resolved. Here, we propose a CVQSDC protocol based on N-symbol amplitude phase shift keying (N-APSK), which exploits the Boltzmann–Maxwell distribution assisted probability shaping technique. In comparison with the uniform distribution, according to 32-APSK CVQSDC, the proposed scheme extends the communication distance by about 38%, while obtaining a higher secrecy capacity at the same communication distance. Furthermore, increasing the value of N will concurrently increase the quantity of rings in the constellation, thereby facilitating enhancements of communication distance. This work incorporates the modulation approaches prevalently employed in classical communication into the realm of quantum communication, attaining gratifying advancements in communication distance and secrecy capacity, and concurrently facilitating the integrated development of quantum communication and classical communication.

Keywords: quantum secure direct communication, discrete-modulation, amplitude phase shift keying, Boltzmann–Maxwell distribution

PACS: 03.67.–a, 03.67.Hk, 03.67.Dd, 42.50.Ex

DOI: 10.1088/1674-1056/ada549 **CSTR:** 32038.14.CPB.ada549

1. Introduction

Quantum secure communication mainly includes quantum key distribution (QKD), quantum secure direct communication (QSDC), quantum teleportation (QT) and so on.[1] Different from the secure key-based communication mode of QKD, QSDC adopts a single-channel structure to directly transmit secret messages and has been widely studied as a mature secure communication scheme. The original QSDC protocol was proposed by Long and Liu *et al.* in 2002,[2] in which a method of quantum block transmission was proposed that can detect the presence of an eavesdropper during transmission, making it impossible for the eavesdropper to obtain the information. In 2002, Boström and Felbinger proposed a secure communication scheme based on dense coding, called the ping–pong protocol;[3] this protocol clarified the definition of QSDC for the first time, which has certain theoretical value, but there is still the risk of information leakage. Subsequently, Deng *et al.* proposed a two-step QSDC scheme based on the Einstein–Podolsky–Rosen (EPR) concept in 2003,[4] which verifies the security under an ideal noiseless channel and gives the conditions for secure transmission under a noisy channel. In 2004, Deng and Long proposed the DL04 QSDC scheme based on single-photon sequences.[5] In 2005, Wang *et al.* proposed a QSDC scheme using high-dimensional entangled states,[6] which improves the security and channel capacity of communication by combining block transmission and superdense coding. In 2006, Jin *et al.* first proposed a three-party QSDC scheme based on the Greenberger–Horne–Zeilinger (GHZ) state, which was shown to be secure against not only intercept-and-resend attacks but also disturbance attacks.[7]

In recent years, research on QSDC has developed further. In 2021, Cao *et al.* proposed a QSDC protocol based on Gaussian mapping, which effectively solves the offset problem caused by the non-uniformity of the secret-message bit-stream and is applicable to different modulation variances.[8] In 2022, Sheng *et al.* proposed a one-step QSDC protocol to reduce the number of photon transmissions in the channel from two to one, which greatly simplified the experimental operation of QSDC and improved the performance of information transmission.[9] Cao *et al.* demonstrated the first continuous-variable quantum secure direct communication (CVQSDC) experiment in 2023, which verified the feasibility and effectiveness of a CVQSDC protocol based on Gaussian mapping, and proposed an estimation method for signal classification

†Corresponding author. E-mail: chai.geng@nwu.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

under practical channels.[10] In the same year, Liang *et al.* proposed a QSDC scheme based on an intermediate basis, which reduced the probability of the eavesdropping party selecting the correct measurement basis through intermediate-basis EPR pairs, thus improving the security of the system.[11] Zhao *et al.* in 2024 proposed a hybrid entanglement-based QSDC protocol, which has higher communication efficiency due to near-deterministic Bell state measurements, as well as higher fidelity, and provides a new approach to realizing secure QSDC.[12] In the same year, Zhang *et al.* proposed a single-photon-based three-party QSDC protocol, which encodes the information by adopting a hypercoding technique after passing identity authentication.[13] The protocol guarantees the security of the transmitted information and the legal identity of each sender and has important application prospects in the field of quantum networks. Furthermore, Wang *et al.* introduced a purification scheme for CVQSDC based on coherent states to mitigate the decoherence effects of quantum states. By effectively suppressing excess noise, this scheme significantly enhanced the secrecy capacity of the communication system. Experimental results demonstrated that the excess noise was reduced to 58% of its original level, leading to a 43.6% improvement in secrecy capacity.[14] These advancements provide robust theoretical and experimental foundations for the development of high-security and low-loss quantum communication networks.

At the same time, in order to solve the impact of the defects of the detection equipment in practical experiments, the measurement-device-independent (MDI) QSDC protocol has been successively proposed.[15,16] In 2020, Sheng *et al.* proposed device-independent (DI) and measurement-device-independent parameter (MDI) QSDC schemes, which enhance the practical security of QSDC and effectively improve the quality of communication.[17,18] In 2022, Ying *et al.* put forward a one-step MDI-QSDC protocol that made use of nonlinear-optical complete hyperentanglement Bell state measurement (HBSM) and linear-optical partial HBSM, and the experimental results showed that the one-step MDI QSDC protocol with complete HBSM achieved a maximum communication distance of approximately 354 km.[19] In 2023, Zhou *et al.* proposed a DI-QSDC protocol based on a single-photon source, which improved the secure communication distance of the protocol sixfold compared with the current DI-QSDC protocol. Meanwhile, an entanglement channel constructed by combining entanglement purification avoids information leakage and has broad prospects.[20] In the same year, Zeng *et al.* proposed a high-capacity DI-QSDC protocol based on the superconding technique, which provides numerical simulation of the change of secrecy capacity with the communication distance and improves the secrecy capacity of DI-QSDC.[21] Due to the advantages of QSDC, its development will further promote the development and application of secure communications.

Discrete modulation (DM)[24–28] employs a finite number of quantum states for coding, circumventing the requirement for precise hardware and high-speed true random number generators in Gaussian modulation (GM),[22,23] thereby lowering the complexity of practical applications. Consequently, in the domain of quantum communication, N-PSK and N-APSK discrete modulation techniques are extensively employed in continuous-variable quantum key distribution (CVQKD). In 2009, Leverrier and Grangier proposed a four-state modulation CVQKD protocol and gave a security proof under a linear channel assumption.[26] It proved the security of the N-PSK universal protocol in lossy but noise-free quantum channels,[29] and concluded that the most suitable scheme is $N = 8$ by analyzing the performance of the protocol at $N = 4$, $N = 8$, and $N = 16$.[30] Almeida *et al.* in 2021 proposed a DM-CVQKD based on N-APSK, which demonstrated that it can more closely approximate the true GM results compared to N-PSK,[31] and proposed the use of binomial probabilistic shaping to optimize the N-APSK. Meanwhile, in DM, the use of non-uniform probability-shaping techniques to optimize N-APSK constellations leads to higher performance and efficiency. It was shown that the results can gradually approach those of GM, such as binomial distribution and Boltzmann–Maxwell distribution.[32] For the CVQSDC protocol, information can be directly transmitted through the quantum channel without the requirement of any secret key exchange between the communication parties. This eliminates the necessity of generating and sharing the secret key as in the CVQKD protocol and utilizes the secret key to encrypt and decrypt the subsequent classical communication. Consequently, we contemplated applying N-APSK modulation technology to the CVQSDC protocol to attain enhanced performance.

In this paper, an N-APSK QSDC protocol with Boltzmann–Maxwell distribution is proposed. This protocol has achieved satisfactory enhancements of both secrecy capacity and communication distance. Compared with uniform and binomial distributions, the Boltzmann–Maxwell distribution for describing the probability of constellations can maximize the capacity of the channel, thereby obtaining a higher secrecy capacity and a longer communication distance. Meanwhile, we also explored the secrecy capacity and communication distance of N under different values; an increase in the value of N in accordance with a certain pattern will lead to an increase in the number of rings in the APSK constellation. When $N = 32$, 64, 128, 256, the communication distance will be enhanced as the value of N rises, concurrently obtaining a comparatively favorable secrecy capacity. Nevertheless, as the ring increases, the enhancements become smaller.

The rest of the paper is organized as follows. In Section 2, we propose a CVQSDC protocol based on N-APSK with Boltzmann–Maxwell distribution and verify the superi-

ority of the proposed protocol in terms of secrecy capacity and communication distance. In Section 3, we analyze the performance of 32-APSK as an example, and ultimately present the communication distance of N-APSK with Boltzmann–Maxwell (BM) distribution as a function of secrecy capacity. Our conclusions are given in Section 4.

2. *N*-APSK CVQSDC with Boltzmann–Maxwell distribution

Based on the two-step QSDC protocol, the CVQSDC based on N-APSK with Boltzmann–Maxwell distribution is put forward and the steps of the proposed protocol are devised. The system model diagram of this protocol is shown in Fig. 1. The orange dashed box diagram presents a schematic illustration of APSK modulation employing two sequences of random numbers. In the case of 32-APSK, for instance, the rings are initially selected based on the Boltzmann–Maxwell distribution probability. Subsequently, it selects the positions within the ring for modulation with uniform distribution probability. The figure on the right is an illustration of the probability density of the ring when the probability of the ring has uniform distribution, binomial distribution and Boltzmann–Maxwell distribution. Here, the probabilities of the rings are all selected to the left of the black dashed line.

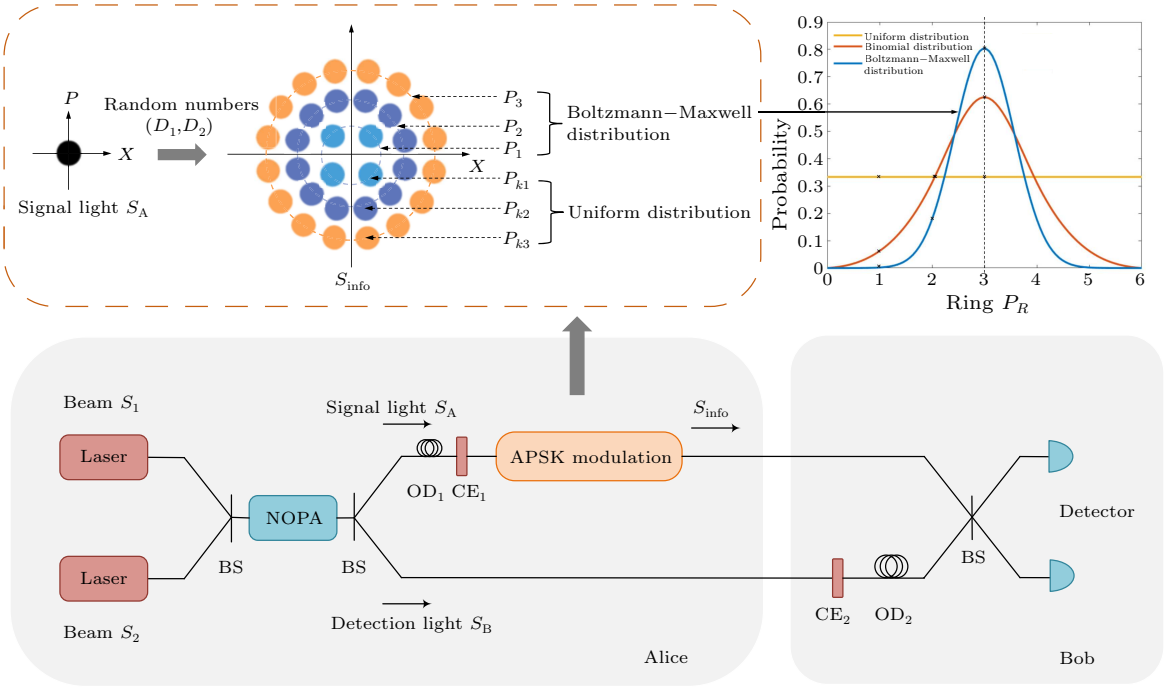


Fig. 1. The system model diagram of the N-APSK CVQSDC (Laser indicates the laser source, NOPA represents the nondegenerate optical parametric amplifier, BS represents the beam splitter, OD_1 and OD_2 represents the fiber optic delay lines, CE_1 and CE_2 represents the process of security detection and authentication in Step 2, P_1, P_2 and P_3 represent the probabilities of the first ring, second ring and third ring, P_{k_1}, P_{k_2} and P_{k_3} represent the probabilities of each state on the three rings, and D_1, D_2 denotes the sequences of random numbers used for APSK modulation).

Step 1 (Preparation stage) Alice, the sender, utilizes a squeezed operator $S(r) = \mathrm{e}^{\left[r\left(s_1^{\dagger}s_2^{\dagger}-s_1s_2\right)\right]}$ to prepare two-mode squeezed beams S_A and S_B. Here s_1 and s_2 denote the input beams used to prepare the two-mode squeezed beams, $s_1^{\dagger}$ and $s_2^{\dagger}$ denote the Hermite conjugation of the input beams, and r denotes the squeezed factor.[33] Thus the two-mode squeezed beams can be expressed as

$$\begin{aligned} S_A &= S^{\dagger}(r)s_1S(r) = s_1\cosh(r) \pm s_2\sinh(r), \\ S_B &= S^{\dagger}(r)s_2S(r) = s_2\cosh(r) \pm s_1\sinh(r), \end{aligned} \tag{1}$$

where $\sinh(\cdot)$ is the hyperbolic sine function, $\cosh(\cdot)$ is the hyperbolic cosine function. Correspondingly, the relation between the quadrature components of the beams s_1 and s_2, and the two-mode squeezed beams S_A and S_B, can be expressed by

$$\begin{aligned} X_A &= x_{s_1}\cosh(r) \pm x_{s_2}\sinh(r), \\ X_B &= x_{s_2}\cosh(r) \pm x_{s_1}\sinh(r), \\ P_A &= p_{s_1}\cosh(r) \mp p_{s_2}\sinh(r), \\ P_B &= p_{s_2}\cosh(r) \mp p_{s_1}\sinh(r), \end{aligned} \tag{2}$$

where $x_{s_{1,2}}$ and $p_{s_{1,2}}$ denote the quadrature components of the beams s_1 and s_2, $X_{A,B}$ and $P_{A,B}$ represent the quadrature components of two-mode squeezed beams S_A and S_B. Afterwards, Alice retains beam S_A as the signal light and sends beam S_B as the detection light through the quantum channel to the receiver Bob.

Step 2 (Security detection and authentication stage) Alice chooses a set of random positions on the signal light S_A, measures their X_A and P_A and announces the chosen positions and measurement results. Bob chooses the same positions on the beam S_B' as Alice and measures the two quadrature compo-

nents. After the measurements obtained by Bob, using these measurements and Alice's measurements for judgment, which is based on the inseparability criterion[34]

$$\left\langle \left[\Delta(X_{\mathrm{A}}+X'_{\mathrm{B}})\right]^2\right\rangle + \left\langle \left[\Delta(P_{\mathrm{A}}-P'_{\mathrm{B}})\right]^2\right\rangle \leq 2, \tag{3}$$

where $\Delta(\cdot)$ represents the standard deviation of the measurement result and $\langle\cdot\rangle$ represents the average of the results in these symbols.

If the measurement result of the selected position violates the inequality, the channel is secure. Otherwise, the communication is ended. Subsequently, Bob selects another set of random positions on the detection light S'_{B} and measures the two quadrature components, and announces the chosen positions and measurement results. Alice selects the same measurement position as Bob on the signal light S_{A} and measures the two quadrature components, judging by the inseparability criterion whether to continue the communication or not.

Step 3 (Encoding stage) Two sequences of random numbers (D_1, D_2) are selected to modulate the signal light S_{A} according to the secret information required to be encoded. The N-APSK constellation is initially introduced, which gives rise to the representation of the distribution of quantum states in phase space in the form of the N-APSK constellation. The N-APSK constellation is composed of multiple concentric N-PSK constellations and the number of states in each ring is

$$N_R = \begin{cases} 4, & R=1, \\ 12, & R=2, \\ 2^{(R+1)}, & R\geq 3, \end{cases} \tag{4}$$

where R denotes the number of rings, $R=\{1,2,\ldots,M\}$, M represents the total number of rings and N_R is the number of states in the R-th ring, so the number of states increases from the first ring to the M-th ring, which is 4, 12, 16, 32, 64, 128, 256,..., respectively.

The set of constellations composed of N-APSK can be expressed as

$$\chi = \begin{cases} r_1 \mathrm{e}^{\mathrm{j}\left(\frac{2\pi}{N_1}i+\theta_1\right)} & \text{for } i=0,\ldots,N_1-1,\ (R=1), \\ r_2 \mathrm{e}^{\mathrm{j}\left(\frac{2\pi}{N_2}i+\theta_2\right)} & \text{for } i=0,\ldots,N_2-1,\ (R=2), \\ \vdots & \\ r_R \mathrm{e}^{\mathrm{j}\left(\frac{2\pi}{N_R}i+\theta_R\right)} & \text{for } i=0,\ldots,N_R-1,\ (R=M), \end{cases} \tag{5}$$

where r_R denotes the radius of the ring and θ_R represents the phase of the states in the R-th ring.[35] Thus, according to the representation of the set of constellations, the set of states in the R-th ring can be represented as

$$|\alpha_{k_R}\rangle_{(R)} = \left|\frac{R}{M}\alpha\,\mathrm{e}^{\mathrm{i}(k_R-\frac{1}{2})\theta_R}\right\rangle,\quad k_R=\{1,\ldots,N_R\}, \tag{6}$$

by employing probability-shaping techniques to modify the probability distribution of the N-APSK constellation, an enhancement in communication performance can be achieved. Figure 2 presents the distribution and probability information of the 32-APSK constellation under uniform, binomial and Boltzmann–Maxwell distribution; the key difference among which lies in the probability of each ring. In Fig. 2, the probability of each ring is $P_{R(\mathrm{unif.})}=1/M$, while the probability of each state within a ring is $P_{k_R}=1/N_R$ (For 32-APSK, $R=\{1,2,3\}$, $M=3$). A uniform distribution evenly distributes energy among the constellation points, which might lead to the low energy efficiency of the signal and limited communication capacity in non-ideal propagation environments. Due to the incapability of effectively utilizing the channel characteristics, the signal undergoes more attenuation during transmission, thereby affecting the communication distance. A non-uniform distribution is capable of optimizing the layout of the constellation in accordance with the channel characteristics, possessing a superior anti-interference capability and reducing the error rate. For Figs. 2(b) and 2(c), the ring probability is

$$P_{R(\mathrm{binom.})} = \frac{2}{2^{(2M-1)}}\binom{2M-1}{R-1},$$

$$P_{R(\mathrm{BM})} = \frac{\mathrm{e}^{-\nu\left(\frac{\mathrm{Ring}}{M}\right)^2}}{\sum_{j=1}^{\mathrm{Ring}} P_j},\quad \mathrm{Ring}=M-R+1,$$

in contrast to the binomial distribution, the Boltzmann–Maxwell distribution gradually enhances the probability of the outer ring, enabling states with larger amplitudes to maintain a relatively higher energy over longer distances. This effectively mitigates signal loss and augments the effective transmission distance of the system in the presence of attenuation caused by the increase in propagation distance.

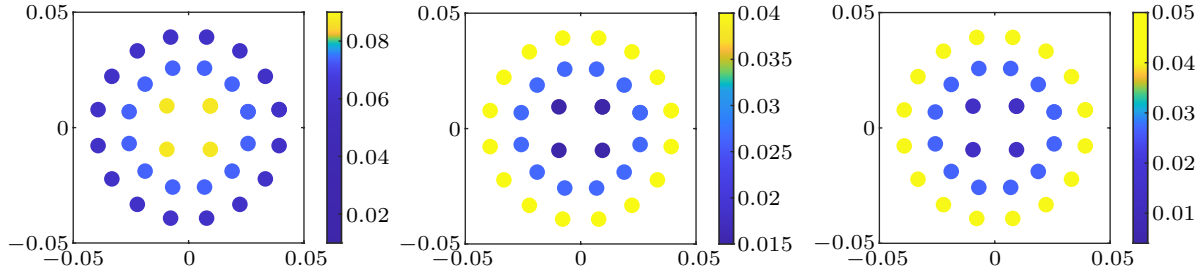


Fig. 2. Illustrations of 32-APSK constellation under uniform distribution, binomial distribution and Boltzmann–Maxwell distribution.

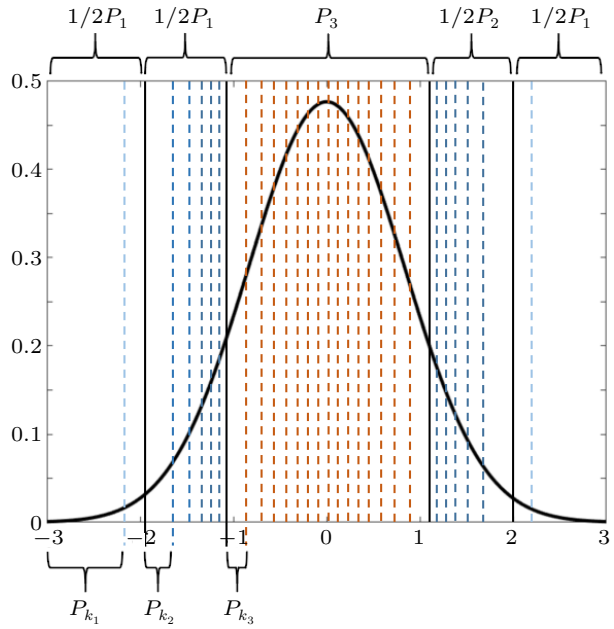


Fig. 3. Schematic diagram of interval division in Gaussian distribution ($P_1 = 0.0195$, $P_2 = 0.1771$, $P_3 = 0.8034$, $P_{k_1} = 1/4$, $P_{k_2} = 1/12$, $P_{k_3} = 1/16$).

Table 1. Gaussian mapping and reflecting intervals.

Secret messages	Alice's mapping intervals	Bob's reflecting intervals	Quantum states
00000	$[-3,-1.83)$	$[-3,-2.16)$	$\|\alpha_1\rangle_{(1)}$
00001	$[-1.83,-1.65)$	$[-2.16,-1.96)$	$\|\alpha_2\rangle_{(1)}$
00010	$[1.65,1.83)$	$[1.96,2.16)$	$\|\alpha_3\rangle_{(1)}$
00011	$[1.83,3)$	$[2.16,3)$	$\|\alpha_4\rangle_{(1)}$
00100	$[-1.65,-1.39)$	$[-1.96,-1.65)$	$\|\alpha_1\rangle_{(2)}$
00101	$[-1.39,-1.24)$	$[-1.65,-1.47)$	$\|\alpha_2\rangle_{(2)}$
00110	$[-1.24,-1.14)$	$[-1.47,-1.34)$	$\|\alpha_3\rangle_{(2)}$
00111	$[-1.14,-1.05)$	$[-1.34,-1.24)$	$\|\alpha_4\rangle_{(2)}$
01000	$[-1.05,-0.98)$	$[-1.24,-1.16)$	$\|\alpha_5\rangle_{(2)}$
01001	$[-0.98,-0.91)$	$[-1.16,-1.08)$	$\|\alpha_6\rangle_{(2)}$
01010	$[0.91,0.98)$	$[1.08,1.16)$	$\|\alpha_7\rangle_{(2)}$
01011	$[0.98,1.05)$	$[1.16,1.24)$	$\|\alpha_8\rangle_{(2)}$
01100	$[1.05,1.14)$	$[1.24,1.34)$	$\|\alpha_9\rangle_{(2)}$
11101	$[1.14,1.24)$	$[1.34,1.47)$	$\|\alpha_{10}\rangle_{(2)}$
01110	$[1.24,1.39)$	$[1.47,1.65)$	$\|\alpha_{11}\rangle_{(2)}$
01111	$[1.39,1.65)$	$[1.65,1.96)$	$\|\alpha_{12}\rangle_{(2)}$
10000	$[-0.91,-0.74)$	$[-1.08,-0.87)$	$\|\alpha_1\rangle_{(3)}$
10001	$[-0.74,-0.60)$	$[-0.87,-0.71)$	$\|\alpha_2\rangle_{(3)}$
10010	$[-0.60,-0.48)$	$[-0.71,-0.57)$	$\|\alpha_3\rangle_{(3)}$
10011	$[-0.48,-0.37)$	$[-0.57,-0.44)$	$\|\alpha_4\rangle_{(3)}$
10100	$[-0.37,-0.27)$	$[-0.44,-0.32)$	$\|\alpha_5\rangle_{(3)}$
10101	$[-0.27,-0.18)$	$[-0.32,-0.21)$	$\|\alpha_6\rangle_{(3)}$
10110	$[-0.18,-0.09)$	$[-0.21,-0.11)$	$\|\alpha_7\rangle_{(3)}$
10111	$[-0.09,0)$	$[-0.11,0)$	$\|\alpha_8\rangle_{(3)}$
11000	$[0,0.09)$	$[0,0.11)$	$\|\alpha_9\rangle_{(3)}$
11001	$[0.09,0.18)$	$[0.11,0.21)$	$\|\alpha_{10}\rangle_{(3)}$
11010	$[0.18,0.27)$	$[0.21,0.32)$	$\|\alpha_{11}\rangle_{(3)}$
11011	$[0.27,0.37)$	$[0.32,0.44)$	$\|\alpha_{12}\rangle_{(3)}$
11100	$[0.37,0.48)$	$[0.44,0.57)$	$\|\alpha_{13}\rangle_{(3)}$
11101	$[0.48,0.60)$	$[0.57,0.71)$	$\|\alpha_{14}\rangle_{(3)}$
11110	$[0.60,0.74)$	$[0.71,0.87)$	$\|\alpha_{15}\rangle_{(3)}$
11111	$[0.74,0.91)$	$[0.87,1.08)$	$\|\alpha_{16}\rangle_{(3)}$

Consequently, for the N-APSK modulation under the Boltzmann–Maxwell distribution, the probability of each state can be expressed as

$$P_{R|k_R(\mathrm{BM})} = \frac{1}{N_R} \cdot \frac{\mathrm{e}^{-v\left(\frac{\mathrm{Ring}}{M}\right)^2}}{\sum_{j=1}^{\mathrm{Ring}} P_j}, \tag{7}$$

where the parameter v is a probabilistic shaping factor, which is used to determine the value of the probabilities; therefore, it can be chosen to take the values when the probabilities sum is 1. Thus the total number of states on the constellation is the sum of the number of states in each ring, which can be expressed as

$$\begin{aligned} |\alpha_N\rangle \;=\; & P_{1|1}\cdot|\alpha_1\rangle_{(1)} + \cdots + P_{1|4}\cdot|\alpha_4\rangle_{(1)} + P_{2|1}\cdot|\alpha_1\rangle_{(2)} \\ & + \cdots + P_{2|12}\cdot|\alpha_{12}\rangle_{(2)} + \cdots + P_{M|1}\cdot|\alpha_1\rangle_{(M)} \\ & + \cdots + P_{M|N_M}\cdot|\alpha_{N_M}\rangle_{(M)}. \end{aligned} \tag{8}$$

Next, we will describe in detail the process of generating the sequences of random numbers. The secret messages are firstly homogenized so that the probabilities of occurrence of 0 and 1 in the secret messages are equal. Then the secret messages are divided into a number of information blocks, and check bits and detection bits are inserted. Subsequently, a sequence of Gaussian random numbers (D_1, D_2) is prepared with mean 0 and variance V_A. Each information block corresponds to the Gaussian distribution interval and the information blocks are mapped to Gaussian random variables. Eventually, the secret messages are mapped into a sequence of Gaussian random number sequence D_1' to modulate the signal light S_A, where $D_1' \subseteq D_1$. Taking 32-APSK as an example, the probability of each ring is the Boltzmann–Maxwell distribution probability and the probability of the state in the ring is the uniform distribution probability. The random numbers with Gaussian distribution are divided into 32 intervals according to the probabilities. It is first divided into three intervals according to the Boltzmann–Maxwell distribution probabilities, which represent the probabilities of each of the three rings. Then, according to the number of states on the ring, continue to divide the intervals according to the uniform distribution. The interval division schematic is shown in Fig. 3. Finally, the 32 intervals are mapped one-to-one with the binary numbers to complete the Gaussian mapping. The table of mapped intervals is shown in Table 1.

Step 4 (Modulation stage) Alice prepares the corresponding quantum states $|\alpha_{k_R}\rangle_{(R)}$ based on the Gaussian random number sequences (D_1', D_2) obtained in Step 3 and modulates the quadrature components of the signal light S_A. The correspondence between quantum states and Gaussian random number intervals is shown in Table 1. The sequence D_1' modulates the component of the quadrature $X_{k_{R(R)}}$ components and the sequence D_2 modulates the $P_{k_{R(R)}}$ component. At this time, the signal light S_A is modulated into the beam S_info containing

information and is finally sent to Bob through the quantum channel. Taking into account the channel loss, S_{info} evolves into S'_{info} after passing through the channel.

Step 5 (Measurement and demodulation stage) After Bob receives the beam S'_{info}, the quadrature components of the beam S'_{info} are measured through CV Bell detection. The measurement results are obtained with the assistance of the beam S'_{B}, which can be expressed as follows:

$$X_{\text{m}} = \frac{1}{\sqrt{2}}(X'_{\text{info}} - X'_{\text{B}}), \quad P_{\text{m}} = \frac{1}{\sqrt{2}}(P'_{\text{info}} + P'_{\text{B}}), \tag{9}$$

where X_{m} and P_{m} denote the quadrature components of the measurement result, X'_{info} and P'_{info} denote the quadrature components of the beam S'_{info}, X'_{B} and P'_{B} denote the quadrature components of the beam S'_{B}.

Security detection is performed by the additional random detection bits added in Step 3. Bob compares the measurements of the random detection bits with the results announced by Alice and calculates the error rate, which is used to determine the safety threshold. When the error rate is below the safety threshold, it means that the information transmission is considered safe and can be continued to the next step, and vice versa, in which case the communication is stopped. Then Bob confirms that the quantum state transmission is secure, based on the quadrature components of the measurements, thus obtaining the original information. Due to the influence of noise in the channel, there are certain differences between the reflecting intervals and mapping intervals corresponding to secret messages and Gaussian random numbers, as shown in Table 1. The inserted check bits are used to detect and correct errors generated in the transmission of information and are implemented by using suitable error correction codes randomly inserted into the information blocks. Finally, Bob demodulates the measurements (X_{m}, P_{m}) and corresponds the obtained results with Gaussian random numbers to obtain the original secret messages.

3. Performance analysis

In Step 2 of the communication protocol, we verify the security of the channel by measuring the signal light held by Alice and the detection light held by Bob, based on the characteristic of quantum entanglement. A second eavesdropping check is also conducted using the inserted random detection bits, which is analogous to the two-step QSDC protocol.[36] Then, we mainly discuss the security of N-APSK CVQSDC under collective attack. For the three attacks used by the eavesdropper Eve, namely, individual attack, collective attack and coherent attack, the study shows that the collective attack and coherent attack are more threatening to the CV quantum communication system compared to the individual attack and that the coherent attack cannot obtain more information compared to the collective attack.[37] The security of this protocol is analyzed through Wyner's wiretap channel theory by the channel between Alice and Bob as the main channel and the channel where Eve eavesdrops as the wiretap channel;[38] the channel model is shown in Fig. 4.

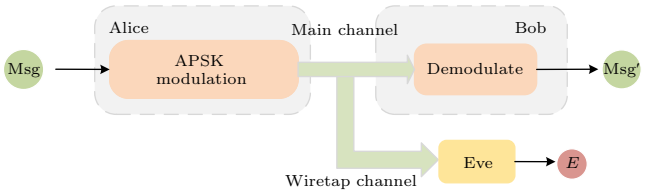


Fig. 4. Wyner's wiretap channel model (Msg denotes the transmitted secret messages, which are modulated at Alice and sent over the main channel to Bob, who demodulates it to get the secret messages Msg′. Eve eavesdrops through the wiretap channel and gets messages E).

The modulation scheme of the protocol is done by a set of quantum states $|\alpha_{k_R}\rangle_{(R)}$ with probability $P_{R|k_R}$. For the density matrix, τ of the Boltzmann–Maxwell distribution can be represented as

$$\tau_{\text{BM}} = \sum_{R=1}^{M}\sum_{k_R=1}^{N_R} P_{R|k_R\,(\text{BM})}|\alpha_{k_R}\rangle_{(R)}\langle\alpha_{k_R}|_{(R)}. \tag{10}$$

In the case of a uniform distribution and binomial distribution, given that the probability of each state is $P_{R|k_R\,(\text{unif.})} = \frac{1}{N_R}\cdot\frac{1}{M}$ and $P_{R|k_R\,(\text{binom.})} = \frac{1}{N_R}\cdot\frac{2}{2^{(2M-1)}}\binom{2M-1}{R-1}$ respectively, the density matrix is likewise distinct and can be presented as

$$\tau_{\text{unif.}} = \sum_{R=1}^{M}\sum_{k_R=1}^{N_R} P_{R|k_R\,(\text{unif.})}|\alpha_{k_R}\rangle_{(R)}\langle\alpha_{k_R}|_{(R)},$$

$$\tau_{\text{binom.}} = \sum_{R=1}^{M}\sum_{k_R=1}^{N_R} P_{R|k_R\,(\text{binom.})}|\alpha_{k_R}\rangle_{(R)}\langle\alpha_{k_R}|_{(R)}. \tag{11}$$

The covariance matrix between Alice and Bob is associated with the parameter Z^* and the parameter Z^* of the Boltzmann–Maxwell distribution can be presented as[39]

$$Z^*_{\text{BM}}(T,\xi) = 2\sqrt{T}\,\text{tr}(\tau^{1/2}a\tau^{1/2}a^\dagger) - \sqrt{2T\xi\omega}, \tag{12}$$

where $\omega = \sum_k P_k\left(\langle\alpha_k|\alpha_\tau^\dagger\alpha_\tau|\alpha_k\rangle - \langle\alpha_k|\alpha_\tau|\alpha_k\rangle^2\right)$, $\alpha_\tau = \tau^{1/2}\alpha\tau^{-1/2}$, $\tau = \tau_{\text{BM}}$. α_τ and $\alpha_\tau^\dagger$ are the annihilation and creation operators, respectively. In the case of uniform and binomial distributions, it is feasible to substitute τ in Eq. (12) with $\tau_{\text{unif.}}$ and $\tau_{\text{binom.}}$ for obtaining $Z^*_{\text{unif.}}$ and $Z^*_{\text{binom.}}$. The covariance matrix of the Boltzmann–Maxwell distribution can be expressed as

$$\boldsymbol{\Gamma}_{\text{BM}} = \begin{pmatrix} aI_2 & c\sigma_Z \\ c\sigma_Z & bI_2 \end{pmatrix} = \begin{pmatrix} VI_2 & Z^*_{\text{BM}}\sigma_Z \\ Z^*_{\text{BM}}\sigma_Z & T^*(V+\xi_{\text{line}})I_2 \end{pmatrix}, \tag{13}$$

where σ_Z is the Pauli matrix, I_2 is the 2×2 identity matrix, $V = V_{\text{A}} + 1 = 2\langle n\rangle + 1$, the average photon number $\langle n\rangle = \sum_{R=1}^{M}\sum_{k_R=1}^{N} P_{R|k_R\,(\text{BM})}|\alpha_{k_R}|^2_{(R)}$ and the modulation variance $V_{\text{A}} = 2\langle n\rangle = 2\sum_{R=1}^{M}\sum_{k_R=1}^{N} P_{R|k_R\,(\text{BM})}|\alpha_{k_R}|^2_{(R)}$.

Figure 5 compares the relationship between the Z^* parameter and the modulation variance V_{A} of 32-APSK under

uniform, binomial, Boltzmann–Maxwell distributions. It can be observed that the Boltzmann–Maxwell distribution can get closer to GM when the modulation variance V_A lies within the range of 0 to 0.5. Additionally, we have compared the relationship between the Z^* parameter and the modulation variance V_A for 32-APSK and 256-APSK under Boltzmann–Maxwell distribution. When the modulation variance V_A is within the range of 0 to 0.5, both 32-APSK and 256-APSK approach GM's Z^* parameter infinitely closely. Meanwhile, 256-APSK is closer to GM than 32-APSK. Therefore, in subsequent research, we will analyze the system performance on the condition that the modulation variance V_A is within the range of 0 to 0.5.

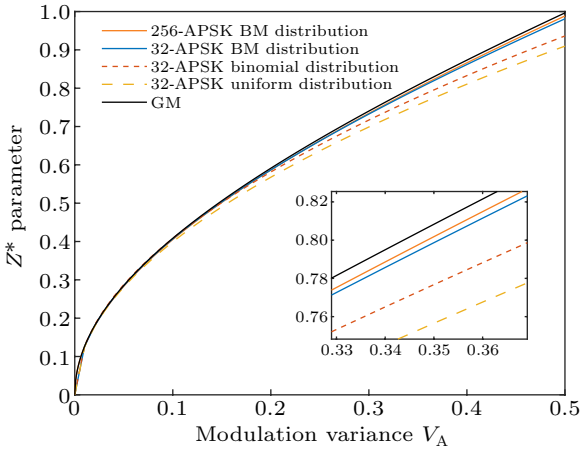


Fig. 5. The Z^* parameter as a function of modulation variance V_A for GM, 32-APSK with uniform distribution, binomial distribution and Boltzmann–Maxwell distribution, and 256-APSK with Boltzmann–Maxwell distribution.

The secrecy capacity can be calculated by

$$C_S = C_M - C_W = I_{AB} - \chi_{AE}, \tag{14}$$

where C_M is the main channel capacity and C_W is the wiretap channel capacity. I_{AB} is the mutual information between Alice and Bob, it can be expressed as

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{V+\xi_{line}}{1+\xi_{line}}\right), \tag{15}$$

where $V = V_A + 1$, the channel linear noise $\xi_{line} = 1/T - 1 + \varepsilon$, T is the channel transmittance and ε is the excess noise. χ_{AE} indicates the information that Eve eavesdrops on Alice; it can be expressed as

$$\chi_{AE} = S(E) - S(E|x_A^M), \tag{16}$$

where $S(E)$ is Eve's von Neumann entropy and $S(E|x_A^M)$ is the conditional entropy of Eve after knowing Alice's measurements. Under the condition that Eve can purify the entire system, χ_{AE} can be calculated as

$$\chi_{AE} = S(\rho_{AB}) - S(\rho_{AB}|x_A^M), \tag{17}$$

where $S(\rho_{AB})$ is the von Neumann entropy of the Alice and Bob systems and $S(\rho_{AB}|x_A^M)$ is the conditional entropy of the Alice and Bob systems after knowing Alice's measurements. $S(\rho_{AB})$ can be obtained from the symplectic eigenvalues λ_1 and λ_2 of the covariance matrix $\boldsymbol{\Gamma}_{BM}$ in Eq. (13),

$$S(\rho_{AB}) = S(\lambda_1) + S(\lambda_2), \tag{18}$$

where

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A - 4B^2}\right)},$$
$$A = V^2 + T^2(V+\xi_{line})^2 - 2TZ_{BM}^{*2},$$
$$B = TV^2 + TV\xi_{line} - Z_{BM}^{*2}.$$

$S(\rho_{AB}|x_A^M)$ can be obtained from the symplectic eigenvalues λ_3 and λ_4 of the covariance matrix $\gamma_{A'B}^{x_A^M}$,

$$\gamma_{A'B}^{x_A^M} = \begin{pmatrix} b - c^2/a & 0 & \sqrt{2}c/(a+1) & 0 \\ 0 & b & 0 & -c/\sqrt{2} \\ \sqrt{2}c/(a+1) & 0 & 2a/(a+1) & 0 \\ 0 & -c/\sqrt{2} & 0 & (a+1)/2 \end{pmatrix}, \tag{19}$$

it can be calculated that the symplectic eigenvalues $\lambda_{3,4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)}$, where

$$C = \frac{V + BT(V+\xi_{line}) + A}{V+1}, \quad D = \frac{BT(V+\xi_{line}) + B^2}{V+1}.$$

Finally, it can be calculated by

$$S(\rho_{AB}|x_A^M) = S(\lambda_3) + S(\lambda_4), \tag{20}$$

where $S(\lambda_i) = \left(\frac{\lambda_i+1}{2}\right)\log_2\left(\frac{\lambda_i+1}{2}\right) - \left(\frac{\lambda_i-1}{2}\right)\log_2\left(\frac{\lambda_i-1}{2}\right)$.

Figure 6 presents the modulation variance V_A of 32-APSK protocols as a function of the secrecy capacity in the cases of uniform, binomial and Boltzmann–Maxwell distributions. It can be observed that when the modulation variance V_A assumes the same value, the secrecy capacity of the 32-APSK protocol with Boltzmann–Maxwell distribution is higher than that of the 32-APSK protocols with binomial and uniform distributions. Regarding the three probability distributions, the modulation variance V_A at which the secrecy capacity attains its optimum value also varies. In the case of the Boltzmann–Maxwell distribution, the optimal value of the modulation variance V_A approximates 0.5; concurrently, for the binomial distribution and the uniform distribution, it approximates 0.3 and 0.1, respectively.

Figure 7 shows the correlation between communication distance and secrecy capacity in the three distributions of 32-APSK. In contrast to the binomial distribution and uniform distribution, the 32-APSK with Boltzmann–Maxwell distribution possesses greater secrecy capacity and longer communication distance. It is capable of extending the communication distance to approximately 20 km, representing an increase

of approximately 38% compared to the uniform distribution. Meanwhile, compared with the other two distributions, the protocol's performance under the Boltzmann–Maxwell distribution can be superior to GM over a larger transmission distance range. When the communication distance is less than 4 km, GM still possesses a high level of secrecy capacity. Nevertheless, when the communication distance is greater than 4 km, the secrecy capacity of N-APSK modulation based on the Boltzmann–Maxwell distribution surpasses that of GM and the gap between them widens as the communication distance increases. Figure 8 illustrates the communication distance as a function of secrecy capacity for N-APSK modulation ($N = 32$, 64, 128, 256) with Boltzmann–Maxwell distribution. At close range, GM continues to exhibit satisfactory communication performance. However, when the communication distance surpasses 4 km, the advantages of the Boltzmann–Maxwell distribution communication protocol become evident. As N increases, the number of rings within the constellation rises, extending the communication distance accordingly. Therefore, by increasing the number of rings, superior performance can be attained. However, when $N = 256$, it is obvious that the improvement diminishes.

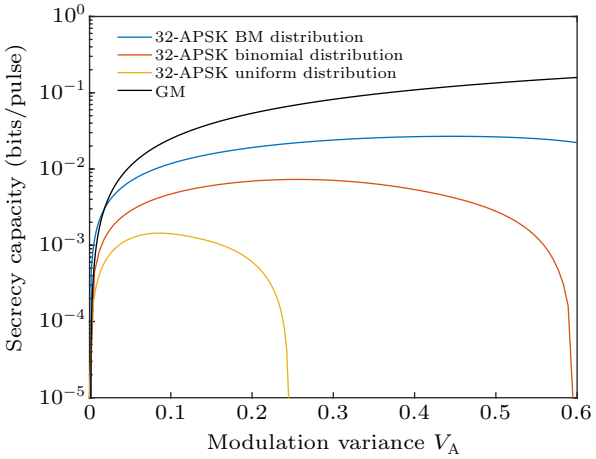


Fig. 6. The modulation variance V_A as a function of the secrecy capacity for GM, uniform, binomial and Boltzmann–Maxwell distribution.

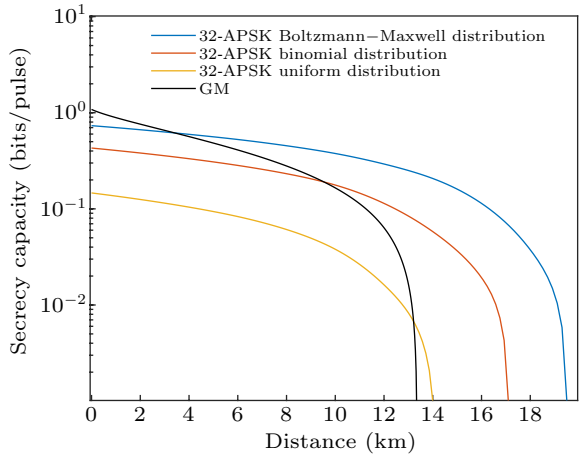


Fig. 7. Communication distance as a function of secrecy capacity for GM, 32-APSK with uniform, binomial and Boltzmann–Maxwell distribution.

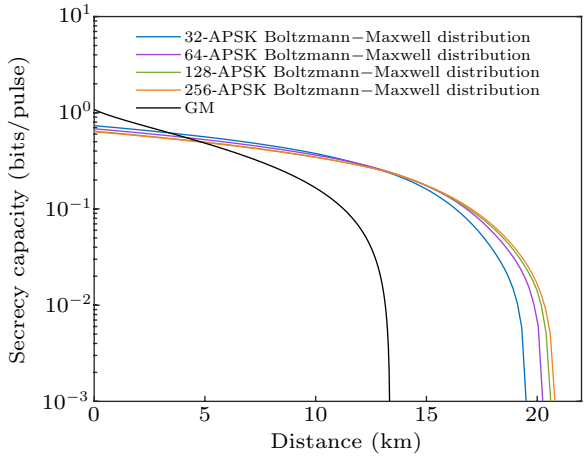


Fig. 8. Communication distance as a function of the secrecy capacity for GM, 32-APSK, 64-APSK, 128-APSK and 256-APSK with Boltzmann–Maxwell distribution.

4. Conclusion

DM-CVQSDC with N-APSK can achieve a longer communication distance than GM-CVQSDC. Meanwhile, N-APSK under Boltzmann–Maxwell distribution possesses a higher secrecy capacity and longer communication distance when compared with binomial distribution and uniform distribution. In this work, by varying the probability distribution of each ring in the APSK constellation, we have designed the N-APSK CVQSDC protocol based on Boltzmann–Maxwell distribution. The performance of CVQSDC was compared among Boltzmann–Maxwell distribution, binomial distribution and uniform distribution with 32-APSK taken as an example. In comparison with uniform distribution, Boltzmann–Maxwell distribution can improve the communication distance by approximately 38%. The communication distance can still be improved as the value of N, i.e., the number of rings increases. However, it is not appropriate to increase the number of rings excessively.

Acknowledgments

Project supported by the National Natural Science Foundation of China (Grant Nos. 62071381 and 62301430), Shaanxi Fundamental Science Research Project for Mathematics and Physics (Grant No. 23JSY014), Scientific Research Plan Project of Shaanxi Education Department (Natural Science Special Project (Grant No. 23JK0680), and Young Talent Fund of Xi'an Association for Science and Technology (Grant No. 959202313011).

References

[1] Pirandola S, Andersen U L, Banchi L, *et al.* 2020 *Adv. Opt. Photonics* **12** 1012
[2] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[3] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[4] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317

[5] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[6] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[7] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 *Phys. Lett. A* **354** 67
[8] Cao Z W, Wang L, Liang K X, Chai G and Peng J Y 2021 *Phys. Rev. Appl.* **16** 024012
[9] Sheng Y B, Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[10] Cao Z W, Lu Y, Chai G, Yu H, Liang K X and Wang L 2023 *Research* **6** 0193
[11] Liang K X, Cao Z W, Chen X L, Wang L, Chai G and Peng J Y 2023 *Front. Phys.* **18** 51301
[12] Zhao P, Zhong W, Du M M, Li X Y, Zhou L and Sheng Y B 2024 *Front. Phys.* **19** 51201
[13] Zhang Q, Du M M, Zhong W, Sheng Y B and Zhou L 2024 *Ann. Phys.* **536** 2300407
[14] Wang L, Chai G, Cao Z W, Chen X L, Liang K X G and Peng J Y 2025 *Sci. China Phys. Mech. Astron.* **68** 220313
[15] Niu P H, Zhou Z R,Lin Z S, Sheng Y B, Yin L G and Long G L 2018 *Sci. Bull.* **63** 1345
[16] Wu X D, Zhou L, Zhong W and Sheng Y B 2020 *Sci. Bull.* **19** 354
[17] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[18] Zhou Z R, Sheng Y B, Niu P H, Yin L G, Long G L and Hanzo L 2020 *Sci. China Phys. Mech. Astron.* **63** 230362
[19] Ying J W, Zhou L, Zhong W and Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[20] Zhou L, Xu B W, Zhong W and Sheng Y B 2023 *Phys. Rev. Appl.* **19** 014036
[21] Zeng H, Du M M, Zhong W, Zhou L and Sheng Y B 2024 *Fundam. Res.* **4** 851
[22] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[23] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier Ph 2003 *Nature* **421** 238
[24] Hirano T, Ichikawa T, Matsubara T, Ono M, Oguri Y, Namiki R, Kasai K, Matsumoto R and Tsurumaru T 2017 *Quantum Sci. Technol.* **2** 024010
[25] Ghorai S,Grangier P, Diamanti E and Leverrier A 2019 *Phys. Rev. X* **9** 021059
[26] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[27] Zhao W, Shi R H, Feng Y T and Huang D 2020 *Phys. Lett. A* **384** 126061
[28] Wang P, Zhang Y, Lu Z G, Wang X Y and Li Y M 2023 *New J. Phys.* **25** 023019
[29] Sych D and Leuchs G 2010 *New J. Phys.* **12** 053019
[30] Becir A, El-Orany F A A and Wahiddin M R B 2012 *Int. J. Quantum Inf.* **10** 1250004
[31] Almeida M, Pereira D, Muga N J, Facão M, Pinto A N and Silva N A 2021 *Opt. Express* **29** 38669
[32] Almeida M, Pereira D, Facão M, Pinto A N and Silva N A 2023 *J. Lightwave Technol.* **41** 6134
[33] Gong L H, Song H C, He C S, Liu Y and Zhou N R 2014 *Phys. Scr.* **89** 035101
[34] Duan L M, Giedke G, Cirac J I and Zoller P 2000 *Phys. Rev. Lett.* **84** 2722
[35] Gaudenzi D R, Fabregas I G A and Martinez A 2006 *IEEE Trans. Wireless Commun.* **5** 2396
[36] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[37] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305
[38] Wu J, Lin Z, Yin L and Long G L 2019 *Quantum Engineering* **1** e26
[39] Denys A, Brown P and Leverrier A 2021 *Quantum* **5** 540