


# Continuous-variable quantum secure direct communication with one-time pad

Yi-Yu Mao(毛宜钰), Chang-Hua Hu(胡昌华), Wen-Ti Huang(黄文体), Wei Zhao(赵微), and Lei Chen(陈磊)
**Citation:**Chin. Phys. B, 2026, 35 (**4**): 040302. DOI: 10.1088/1674-1056/ae181a
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

---

## 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)
Chin. Phys. B, 2025, 34 (**3**): 030303. DOI: 10.1088/1674-1056/ada549

## 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

---

**SPECIAL TOPIC — Quantum communication and quantum network**

# Continuous-variable quantum secure direct communication with one-time pad

Yi-Yu Mao(毛宜钰)[1], Chang-Hua Hu(胡昌华)[2], Wen-Ti Huang(黄文体)[3], Wei Zhao(赵微)[4], and Lei Chen(陈磊)[5,†]

[1] *School of Physics and Electronic Science, Changsha University of Science and Technology, Changsha* 410114, *China*
[2] *School of Computer Science and Technology, Changsha University of Science and Technology, Changsha* 410114, *China*
[3] *School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan* 411201, *China*
[4] *Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan* 250316, *China*
[5] *PT. Sinotrans CSC Indonesia, Jakarta* 12940, *Indonesia*

(Received 12 August 2025; revised manuscript received 27 October 2025; accepted manuscript online 28 October 2025)

Quantum secure direct communication (QSDC) enables the direct transmission of secret messages over a quantum channel without prior key sharing. QSDC implemented in the continuous-variable (CV) regime allows high-capacity information transmission using simple optical communication technologies. In this work, we propose a novel CV-QSDC protocol with a quantum one-time pad, which achieves secure message transmission based on coherent states and unitary operations, and the receiver can directly obtain the secret messages after measuring the coherent states. The security of this protocol is jointly guaranteed by one-time pad encryption and a CV quantum key distribution (QKD) protocol. Performance analysis shows that the proposed scheme can achieve a quantum bit error rate (QBER) lower than 1% by adjusting the modulation variance and unitary operation parameters. With the optimal modulation variance, the secure transmission distance of the proposed protocol can exceed 150 km.

**Keywords:** quantum secure direct communication, quantum-one-time pad, continuous-variable

**PACS:** 03.67.Hk, 03.67.Dd

**DOI:** 10.1088/1674-1056/ae181a **CSTR:** 32038.14.CPB.ae181a

## 1. Introduction

As an emerging branch of quantum communication, quantum secure direct communication (QSDC) enables the direct transmission of secret messages from Alice to Bob without prior key sharing, offering a novel approach to quantum secure communication distinct from quantum key distribution (QKD). Only protocols that meet the following two requirements can be called QSDC. First, after the transmission of qubits, the receiver Bob should read out the secret messages directly without additional classical information. Second, even in the presence of an eavesdropper, the encoded secret messages should not be leaked.

The concept of QSDC was first proposed by Long *et al.*[1] in 2000. It enables the transmission of deterministic keys based on Einstein–Podolsky–Rosen (EPR) pairs in QKD, and these deterministic keys can be regarded as the secret messages. On this basis, in 2003, Deng *et al.*[2] proposed a two-step QSDC protocol with blocks of EPR pairs, in which the set of ordered EPR pairs is divided into a checking sequence and a message-coding sequence. The two-step QSDC protocol is secure since no eavesdropper can obtain both sequences simultaneously. The following year, a quantum one-time pad QSDC protocol based on a sequence of polarized single photons was proposed,[3] which employs single photons as a one-time pad to directly encode secret information. Building upon these foundational protocols, the early stage of QSDC research witnessed a wave of theoretical diversification. Various improved protocols were proposed to explore new dimensions and capabilities, such as those based on multipartite entanglement,[4] high-dimensional entanglement,[5] hyper-entanglement,[6] controlled QSDC[7] and so on. These works significantly expanded the theoretical landscape of QSDC.

In recent years, the field of QSDC has matured rapidly, yielding both deeper theoretical insights and groundbreaking experimental demonstrations. On the theoretical front, this progress is exemplified by the development of measurement-device-independent QSDC (MDI-QSDC) to close critical detection loopholes,[8,9] the proposal of a one-step protocol to streamline the communication process,[10] and the introduction of passive-source QSDC to eliminate the side-channel risks associated with the source encoder.[11,12] Furthermore, the integration of quantum error correction codes has been explored to improve robustness against noise,[13] and the security framework has been advanced with the proposal of device-independent QSDC (DI-QSDC).[14,15] Novel communication

†Corresponding author. E-mail: chenlei2025@foxmail.com

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

resources, such as hybrid entanglement, have also been utilized to design new QSDC schemes.[16] In parallel, the experimental realization of QSDC has seen remarkable milestones, firmly establishing its practicality. This progress was initiated by the first proof-of-principle experiments using single photons[17] and entanglement,[18] which spurred a series of subsequent experimental verifications and refinements.[19–21] In addition, the experimental implementation of QSDC networks has been successfully demonstrated, showcasing a crucial step towards future quantum internet applications.[22,23]

The QSDC protocols mentioned above are all based on the discrete-variable (DV) regime,[24–26] however, perfect single photons are hard to generate and detect. As an alternative, the continuous-variable (CV) mechanism offers simpler signal generation and measurement technologies, exhibiting enhanced compatibility with standard telecommunication systems.[27–29] The exploration of QSDC within the CV framework was pioneered by Pirandola *et al.*,[30] who established the foundational theory for CV-QSDC based on coherent states. Subsequent research has made significant progress, leading to more robust and practical CV-QSDC schemes.[31–37] Recently, successful experimental demonstrations of CV-QSDC have been reported, showcasing its high-speed capability and compatibility with conventional telecom components.[38,39]

In this paper, we propose a CV-QSDC protocol with a quantum one-time pad, which employs coherent states and unitary operations to encode secret messages. Specifically, Bob prepares coherent states and transmits them to Alice, followed by channel detection to verify the security of the transmission process. If the channel is secure, the coherent states are sent back to Bob after being encoded with secret messages by two different unitary operations. Bob can directly infer the secret messages based on the results of homodyne detection. We derive the quantum bit error rate (QBER) for different secret messages, and the results show that the QBER of the proposed protocol can be controlled below 1% by adjusting the modulation variance and unitary operation parameters. The security of the proposed protocol is analyzed systematically, which shows that the protocol can achieve a secure transmission distance exceeding 150 km by selecting an appropriate modulation variance. The security of this protocol is jointly guaranteed by one-time pad encryption and the CV-QKD protocol.

The rest of this paper is organized as follows. In Section 2, a brief introduction to the DV quantum one-time pad QSDC protocol is presented, followed by a description of binary bit modulation. Section 3 describes the detailed process of the proposed CV-QSDC protocol with a quantum one-time pad, and derives the QBER corresponding to different secret messages. In Section 4, the security of the proposed protocol is analyzed systematically. Finally, the conclusion is given in Section 5.

## 2. Basic knowledge

In this section, we introduce the essential knowledge relevant to the proposed protocol, including the DV quantum one-time pad QSDC protocol and binary bit modulation, which can help to better understand the subsequent content.

### 2.1. DV quantum-one-time pad QSDC protocol

Figure 1 shows the schematic diagram of the DV quantum one-time pad QSDC protocol, which comprises two steps. In the first step, the receiver Bob prepares a batch of single photons and sends them to the sender, Alice. Each photon is randomly prepared in one of the four polarization states: $|H\rangle = |0\rangle$, $|V\rangle = |1\rangle$, $|u\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$, $|d\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. For notational convenience, we refer to this batch of single photons as the A-batch. After receiving the photons in the A-batch, Alice randomly selects a subset of photons of appropriate size from the A-batch, referred to as the S-batch, and measures each photon in the S-batch randomly using either the rectilinear basis or the diagonal basis. To enable Bob to estimate the error rate, Alice discloses the positions, measurement bases, and measurement results of the photons in the S-batch. If the error rate exceeds the security boundary, Bob concludes that the channel is insecure and terminates the protocol. Conversely, if the error rate remains within acceptable limits, the protocol proceeds to the next step. The role of this step is that Bob sends a batch of photons to Alice to carry the messages back and to verify the security of the channel.

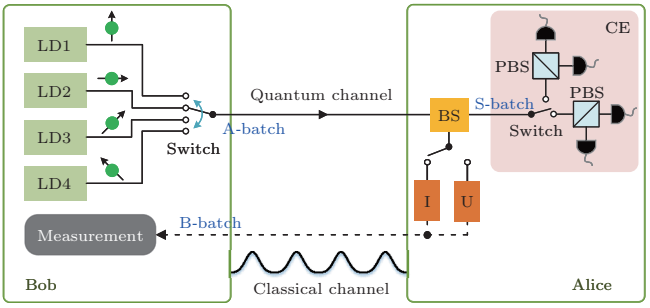



**Fig. 1.** Schematic of the DV quantum one-time pad QSDC protocol. $I$ and $U$ denote the two unitary operations performed by Alice. LD: laser source; BS: beam splitter; PBS: polarization beam splitter; CE: eavesdropping check.

The second step serves for message encoding and transmission. For the remaining photons in the A-batch after excluding the S-batch, which are referred to as the B-batch, Alice encodes them using one of the two unitary operations, $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $U = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, respectively, according to the secret messages. If the secret message is 0, the unitary operation $I$ is performed, and if the secret message is 1, the unitary operation $U$ is performed. The encoded

photons are transmitted back to Bob. Since the photons in the A-batch are prepared by Bob, he measures them using the same measurement basis as that used when preparing the photons, thereby obtaining correct measurement results and reading out the secret information. After message transmission, Alice randomly selects a subset of photons from the B-batch and publicly announces their positions and encoded bit values, which enables Alice and Bob to estimate whether there is an eavesdropper, Eve, intercepting information in the channel.

In the above process, the first step is similar to the BB84 QKD protocol,[24] except that no measurement is performed on the photons in the B-batch. The second step is identical to one-time pad encryption, that is, the secret messages are encrypted based on photons with completely random states in the B-batch. Therefore, the security of the DV quantum one-time pad QSDC protocol is jointly guaranteed by the one-time pad and the BB84 QKD protocol.[3]

### 2.2. Binary bit modulation

Binary bit modulation is a fundamental information encoding technique in quantum communication, which represents classical bits (0 or 1) through two distinguishable quantum states.[40] In particular, for an arbitrary quantum state $|\alpha\rangle = X + \mathrm{i}P$, where the quadratures $X, P \sim \mathcal{N}(\mu, \sigma^2)$, if one wants to encode bit 0, a displacement $A$ can be introduced to $|\alpha\rangle$, making its quadratures become $X = X + A$ and $P = P + A$, where $A$ is a positive constant. Similarly, if one wants to encode bit 1, a displacement $A + B$ can be introduced to $|\alpha\rangle$, so that the quadratures become $X = X + A + B$ and $P = P + A + B$. When demodulating the signal, under the ideal condition $\sigma^2 = 0$, only two results, $\mu + A$ and $\mu + A + B$, can be obtained, corresponding to bit 0 and bit 1, respectively. However, due to quantum uncertainty, the variance $\sigma^2$ of quantum states cannot be zero, which means that the measurement results fluctuate around the ideal values. Therefore, a judgment threshold $\mathcal{H} = \mu + A + B/2$ can be chosen. If the measurement result $X'(P') < \mathcal{H}$, it is considered that bit 0 has been modulated; otherwise, it is considered that bit 1 has been modulated. It is worth noting that if a result $X'(P') > \mathcal{H}$ is obtained when bit 0 is modulated, it causes an error, and vice versa. To achieve effective transmission, the probability of demodulation errors must be guaranteed to be below a certain threshold. In this paper, QBER is selected to evaluate the reliability of the protocol for secret message transmission, which will be elaborated on in the next section.

## 3. CV-QSDC protocol with quantum-one-time pad

In this section, we first elaborate on the proposed CV-QSDC protocol with a quantum one-time pad, then derive the QBER of the protocol, and discuss the impact of different parameters on the QBER.

### 3.1. Protocol description

Due to the advantages of CV-QSDC over DV-QSDC in terms of signal generation and detection, in this paper, we extend the DV quantum one-time pad QSDC protocol to the continuous-variable domain and propose a CV-QSDC protocol with a quantum one-time pad. This protocol consists of five steps: state preparation, channel detection, message encoding, measurement and demodulation, and postprocessing, which are specified as follows.

**Step 1 (State preparation)** As shown in Fig. 2, Bob prepares a batch of coherent states $|X_\mathrm{B} + \mathrm{i}P_\mathrm{B}\rangle$ and modulates them using an amplitude modulator (AM) and a phase modulator (PM), such that the quadratures $X_\mathrm{B}$ and $P_\mathrm{B}$ follow a Gaussian distribution $\mathcal{N}(0, V_\mathrm{B})$, where $V_\mathrm{B}$ is the modulation variance. The modulated coherent states are transmitted to Alice through a public channel, which is characterized by a transmission efficiency $T$ and excess noise $\varepsilon$. For simplicity, we denote this batch of coherent states as the A-batch.

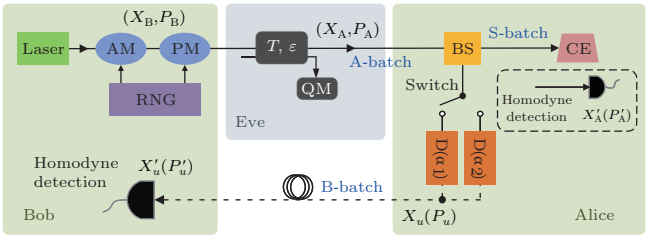



**Fig. 2.** Schematic of the CV-QSDC protocol with a quantum one-time pad. AM: amplitude modulator; PM: phase modulator; RNG: random number generator; QM: quantum memory; BS: beam splitter; CE: eavesdropping check.

**Step 2 (Channel detection)** After being transmitted through the channel, the coherent states in the A-batch arrive at Alice's station, and their quadratures are expressed as

$$\begin{aligned} X_\mathrm{A} &= \sqrt{T}X_\mathrm{B} + \sqrt{T}\delta X_\mathrm{ex} + \delta X_\mathrm{sn}, \\ P_\mathrm{A} &= \sqrt{T}P_\mathrm{B} + \sqrt{T}\delta P_\mathrm{ex} + \delta P_\mathrm{sn}, \end{aligned} \tag{1}$$

where $\delta X_\mathrm{ex}(\delta P_\mathrm{ex})$ arises from channel excess noise satisfying $\langle \delta X_\mathrm{ex}^2 \rangle = \langle \delta P_\mathrm{ex}^2 \rangle = \varepsilon$ in shot noise units, and $\delta X_\mathrm{sn}(\delta P_\mathrm{sn})$ arises from shot noise satisfying $\langle \delta X_\mathrm{sn}^2 \rangle = \langle \delta P_\mathrm{sn}^2 \rangle = 1$. Therefore, the variance of the quadratures can be expressed as

$$\langle X_\mathrm{A}^2 \rangle = \langle P_\mathrm{A}^2 \rangle = TV_\mathrm{B} + T\varepsilon + 1. \tag{2}$$

If we define the channel-added noise as $\chi_\mathrm{line} = 1/T + \varepsilon - 1$, then Eq. (2) can be simplified to

$$\langle X_\mathrm{A}^2 \rangle = \langle P_\mathrm{A}^2 \rangle = T(V + \chi_\mathrm{line}), \tag{3}$$

where $V = V_\mathrm{B} + 1$.

For the coherent states in the A-batch, Alice randomly selects a set of states to perform homodyne detection, which we

designate as the S-batch. The measurement results are given by

$$\begin{aligned} X'_{\rm A} &= \sqrt{\eta T}X_{\rm B} + \sqrt{\eta T}\delta X_{\rm ex} + \delta X_{\rm sn} + \delta X_{\rm el}, \\ P'_{\rm A} &= \sqrt{\eta T}P_{\rm B} + \sqrt{\eta T}\delta P_{\rm ex} + \delta P_{\rm sn} + \delta P_{\rm el}, \end{aligned} \tag{4}$$

where $\eta$ represents the detection efficiency for homodyne detection, and $\delta X_{\rm el}(\delta P_{\rm el})$ denotes the electronic noise satisfying $\langle \delta X_{\rm el}^2 \rangle = \langle \delta P_{\rm el}^2 \rangle = v_{\rm el}$ in shot noise units. The variances of $X'_{\rm A}$ and $P'_{\rm A}$ can be calculated as

$$\langle X_{\rm A}'^2 \rangle = \langle P_{\rm A}'^2 \rangle = \eta T V_{\rm B} + \eta T \varepsilon + 1 + v_{\rm el}. \tag{5}$$

If we define the detection-added noise as $\chi_{\rm hom} = [(1-\eta) + v_{\rm el}]/\eta$, then the total noise related to the channel input is represented as $\chi_{\rm tot} = \chi_{\rm line} + \chi_{\rm hom}/T$. Therefore, Eq. (5) can be simplified to

$$\langle X_{\rm A}'^2 \rangle = \langle P_{\rm A}'^2 \rangle = \eta T (V + \chi_{\rm tot}). \tag{6}$$

Alice announces the positions, measured quadratures, and the corresponding measurement results of the coherent states in the S-batch. Bob compares the quadrature values announced by Alice with those at the same positions in the A-batch, and determines the communication efficiency of the transmission, which is evaluated by the effective information $\Delta I$ detailed in Section 4. If the effective information exceeds the security threshold, it is considered that there is an eavesdropper, and the protocol is terminated. Otherwise, the subsequent steps proceed.

**Step 3 (Messages encoding)** For the remaining coherent states in the A-batch after channel detection, which we refer to as the B-batch, Alice encodes each state using one of the two unitary operations, $\mathcal{D}(\alpha_1)$ or $\mathcal{D}(\alpha_2)$, based on the secret messages. In this protocol, we assume that Alice uses the binary bit modulation described in Subsection 2.2. Figure 3 shows the message encoding process represented in phase space. For the secret message bit 0, Alice performs $\mathcal{D}(\alpha_1)$, and the coherent state becomes

$$X_u = X_{\rm A} + \rho, \quad P_u = P_{\rm A} + \rho. \tag{7}$$

Apparently, $X_u$ $(P_u)$ is a Gaussian variable satisfying $X_u(P_u) \sim \mathcal{N}(\rho, \sigma_u^2)$, with $\sigma_u^2 = T(V + \chi_{\rm line})$. For the secret message bit 1, Alice performs $\mathcal{D}(\alpha_2)$, and the coherent state becomes

$$X_u = X_{\rm A} + \rho + \varsigma, \quad P_u = P_{\rm A} + \rho + \varsigma. \tag{8}$$

In this case, $X_u$ $(P_u)$ satisfies $\mathcal{N}(\rho + \varsigma, \sigma_u^2)$, where $\rho$ and $\varsigma$ are two constants. After being encoded with the secret messages, the coherent states in the B-batch are transmitted back to Bob.

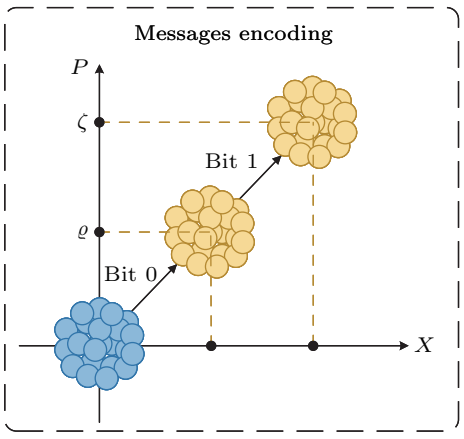



**Fig. 3.** Message encoding process represented in phase space.

**Step 4 (Measurement and demodulation)** Bob receives the encoded coherent states in the B-batch and measures one of the two quadratures randomly using a homodyne detector. The measurement results are given by

$$\begin{aligned} X'_u &= \sqrt{\eta T}X_u + \sqrt{\eta T}\delta X_{\rm ex} + \delta X_{\rm sn} + \delta X_{\rm el}, \\ P'_u &= \sqrt{\eta T}P_u + \sqrt{\eta T}\delta P_{\rm ex} + \delta P_{\rm sn} + \delta P_{\rm el}. \end{aligned} \tag{9}$$

For simplicity, we assume that the homodyne detector used by Bob is identical to that used by Alice, with the same detection efficiency $\eta$ and electronic noise $v_{\rm el}$. As the coherent states in the B-batch are prepared by Bob, he can infer which unitary operation Alice has chosen according to the modulated quadratures $X_{\rm B}$ $(P_{\rm B})$ and the measurement results $X'_u$ $(P'_u)$. Due to the symmetry between the two quadratures $X'_u$ and $P'_u$ in the quantum state, we analyze only the case where Bob measures $X'_u$ for simplicity. The result of measuring $P'_u$ is identical to that of measuring $X'_u$.

Specifically, when the secret message is bit 0, Bob can obtain a value $\varpi_0$ as

$$\begin{aligned} \varpi_0 &= X'_u - T\sqrt{\eta}X_{\rm B} \\ &= \sqrt{\eta T}\rho + \sqrt{\eta T}(\sqrt{T}+1)\delta X_{\rm ex} \\ &\quad + (\sqrt{\eta T}+1)\delta X_{\rm sn} + \delta X_{\rm el}. \end{aligned} \tag{10}$$

Obviously, $\varpi_0$ is a Gaussian variable satisfying $\varpi_0 \sim \mathcal{N}(\sqrt{\eta T}\rho, \sigma_\rho^2)$, with $\sigma_\rho^2 = \eta T(\sqrt{T}+1)^2\varepsilon + (\sqrt{\eta T}+1)^2 + v_{\rm el}$. When the secret message is bit 1, Bob can obtain a value $\varpi_1$ as

$$\begin{aligned} \varpi_1 &= X'_u - T\sqrt{\eta}X_{\rm B} \\ &= \sqrt{\eta T}(\rho+\varsigma) + \sqrt{\eta T}(\sqrt{T}+1)\delta X_{\rm ex} \\ &\quad + (\sqrt{\eta T}+1)\delta X_{\rm sn} + \delta X_{\rm el}. \end{aligned} \tag{11}$$

Similarly, $\varpi_1$ is a Gaussian variable satisfying $\varpi_1 \sim \mathcal{N}(\sqrt{\eta T}(\rho+\varsigma), \sigma_\rho^2)$. Since the values of $\delta X_{\rm ex}$, $\delta X_{\rm sn}$, and $\delta X_{\rm el}$ are random and hard to determine in practice, Bob cannot obtain the exact values of $\rho$ and $\varsigma$. Therefore, we choose a judgment threshold $\mathcal{H} = \sqrt{\eta T}(\rho + \varsigma/2)$.[40] When $\varpi_0 < \mathcal{H}$, Bob

demodulates the correct message bit 0; otherwise, he obtains the incorrect message bit 1. When $\varpi_1 > \mathcal{H}$, Bob demodulates the correct message bit 1; otherwise, he obtains the incorrect message bit 0.

**Step 5 (Post-processing)** To verify the security of the secret message transmission process, Alice randomly selects a portion of the coherent states in the B-batch and publishes the corresponding unitary operations ($\mathcal{D}(\alpha_1)$ or $\mathcal{D}(\alpha_2)$). Based on the modulated values in the preparation stage, the results from homodyne detection, and the values published by Alice, Bob can estimate the effective information $\Delta I$ of the transmission process. If the effective information exceeds the security threshold, the transmission process is deemed unsafe and the protocol is terminated. Otherwise, it is considered that secure transmission of the secret information has been achieved.

### 3.2. QBER of the protocol

In this section, we separately analyze the QBER of the proposed protocol when the secret message is bit 0 and bit 1. Since Alice employs binary bit modulation, the QBER of message 0 can be expressed as[40]

$$P_{0\mathrm{err}} = \int_{\mathcal{H}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_u} \exp\left[-\frac{(x-\sqrt{\eta T}\rho)^2}{2\sigma_u^2}\right] \mathrm{d}x, \tag{12}$$

and the QBER of message 1 can be expressed as

$$P_{1\mathrm{err}} = \int_{-\infty}^{\mathcal{H}} \frac{1}{\sqrt{2\pi}\sigma_u} \exp\left[-\frac{(x-\sqrt{\eta T}(\rho+\varsigma))^2}{2\sigma_u^2}\right] \mathrm{d}x. \tag{13}$$

Note that the obtained QBER is the same regardless of whether the quadrature $X$ or $P$ is measured in homodyne detection, as the operations applied to the two quadratures are identical. Therefore, the QBER for message 1 and message 0 is identical, and Eqs. (12) and (13) can be further simplified to

$$P_{0\mathrm{err}} = P_{1\mathrm{err}} = \frac{1}{2}\mathrm{erfc}\left(\frac{\varsigma}{2}\sqrt{\frac{\eta T}{2\sigma_u^2}}\right). \tag{14}$$

As shown in Eq. (14), the expression of the QBER is independent of the parameter $\rho$, indicating that the difference between the two unitary operations is the key factor affecting the QBER.

Figure 4(a) illustrates the QBER with respect to the channel transmission efficiency $T$ under different values of $\varsigma$. We observe that the QBER decreases monotonically as the transmission efficiency increases for all values of $\varsigma$, because an increase in transmission efficiency implies an improvement in the signal-to-noise ratio (SNR), thereby causing the probability of error to decrease. In addition, the QBER for $\varsigma = 10$ and $\varsigma = 15$ is much lower than that for $\varsigma = 5$, indicating that better performance can be achieved by choosing two unitary operations $\mathcal{D}(\alpha_1)$ and $\mathcal{D}(\alpha_2)$ with a large difference. However, it is worth noting that the value of $\varsigma$ cannot be increased indefinitely. The quantum states encoded by Alice are ultimately measured by Bob using homodyne detection, and an excessively large value of $\varsigma$ may cause the measurement results $X_u'(P_u')$ to exceed the linear response region of the homodyne detector, thereby compromising the security of the protocol. Therefore, the value of $\varsigma$ should be set according to the linear threshold $\alpha$ of the homodyne detector, such that Bob's measurement results satisfy $\varsigma \ll \alpha$ with high probability.[41,42]

Figure 4(b) shows the QBER with respect to the transmission distance $L$ under different values of modulation variance $V_{\mathrm{B}}$. The transmission distance is related to the channel transmission efficiency $T$ by the standard loss model $T = 10^{-\alpha L/10}$, where $\alpha = 0.2$ dB/km is the loss coefficient of the optical fiber.[43] We find that choosing a smaller modulation variance can effectively suppress the QBER of the protocol, and this suppression effect is more pronounced at shorter distances. As the transmission distance increases, the QBER increases significantly for all modulation variances, and even a smaller value of $V_{\mathrm{B}}$ does not lead to a substantial reduction in the QBER. This is because long-distance transmission aggravates signal attenuation and amplifies the channel-added noise, resulting in a reduced SNR and an increased QBER.

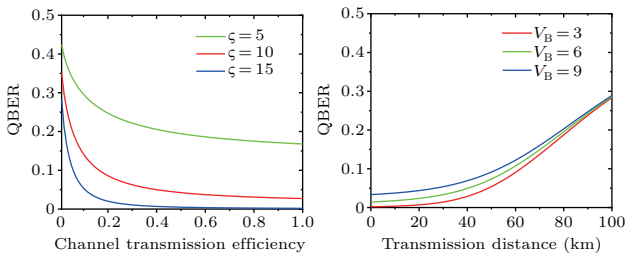



**Fig. 4.** (a) QBER with respect to the channel transmission efficiency $T$ under different values of $\varsigma$. Curves from top to bottom correspond to $\varsigma = 5$, $\varsigma = 10$, and $\varsigma = 15$, respectively. The modulation variance $V_{\mathrm{B}}$ is set to 3. (b) QBER with respect to the transmission distance $L$ under different values of modulation variance $V_{\mathrm{B}}$. Curves from top to bottom correspond to $V_{\mathrm{B}} = 9$, $V_{\mathrm{B}} = 6$, and $V_{\mathrm{B}} = 3$, respectively. The parameter $\varsigma$ is set to 15.

## 4. Security analysis

In this section, we analyze the security of the proposed CV-QSDC protocol with quantum-one-time pad. From the detailed steps of the protocol described in Section 3, it can be seen that the security of the protocol is jointly guaranteed by CV-QKD and the one-time pad. Firstly, the quantum state preparation and transmission processes are completely consistent with those of the CV-QKD protocol, which ensures the security of the quantum states carrying secret messages during transmission. Secondly, the secret messages are encoded on the quadratures of the coherent states in B-batch. This process is equivalent to one-time pad encryption, because the coherent states used to encode secret messages are completely random. Even if Eve measures these states, she cannot recover the secret messages due to ignorance of the values modulated by Bob during state preparation.

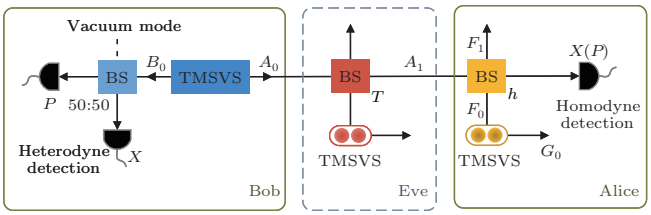



**Fig. 5.** The equivalent entanglement-based (EB) scheme of the quantum-one-time pad CV-QSDC protocol with homodyne detection. BS: beam splitter; TMSVS: two-mode squeezed vacuum state.

Next, we demonstrate the security of the quantum states transmission process, which is equivalent to that of the CV-QKD protocol. To simplify the security analysis, we convert the prepare-and-measure (PM) description presented in Section 3 into the entanglement-based (EB) scheme, which is equivalent to the PM scheme.[44,45] As illustrated in Fig. 5, Bob generates a two-mode squeezed vacuum state (TMSVS) with variance $V = V_{\rm A} + 1$ in shot-noise units, and retains the mode $B_0$ while sending the other mode $A_0$ to Alice. During transmission through the quantum channel, mode $A_0$ may be subjected to attacks by Eve. Typically, Eve's attacks primarily fall into three categories: individual attacks, collective attacks, and coherent attacks. Since coherent attacks and collective attacks pose significantly greater threats to CV-QKD systems than individual attacks, and the security proof against collective attacks is sufficient to obtain security against coherent attacks,[46] we explore the security of the proposed protocol against collective attacks. Bob's detection is modelled by a beam splitter (BS) with transmittance $\eta$, and the electronic noise $v_{\rm el}$ of the detector is modelled by a TMSVS state with variance $v$, one half of which enters the second input port of the BS. The effective information (bits/pulse) between Alice and Bob can be represented as

$$\Delta I = \beta I_{\rm AB} - \chi_{\rm AE}, \tag{15}$$

where $\beta$ denotes the reverse reconciliation efficiency, and $I_{\rm AB}$ and $\chi_{\rm AE}$ are the mutual informations. Specifically, $I_{\rm AB}$ is the Shannon mutual information between Alice and Bob, which can be calculated as

$$I_{\rm AB} = \frac{1}{2}\log_2 \frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}}. \tag{16}$$

Moreover, $\chi_{\rm AE}$ is the Holevo bound of the mutual information between Alice and Eve, calculated as

$$\chi_{\rm AE} = S(\rho_{B_0A_1}) - S(\rho^{m_{\rm A}}_{B_0FG_0}). \tag{17}$$

Under the collective attack, Eq. (17) can be rewritten as

$$\chi_{\rm AE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{18}$$

with the notation $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, where $\lambda_{1,2}$ and $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrices, corresponding to $\gamma_{B_0A_1}$ of the quantum state $\rho_{B_0A_1}$ and $\gamma^{m_{\rm A}}_{B_0FG_0}$ of the quantum state $\rho^{m_{\rm A}}_{B_0FG_0}$, respectively. The covariance matrix $\gamma_{B_0A_1}$ is written as

$$\gamma_{B_0A_1} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T(V^2-1)}\mathbb{Z} \\ \sqrt{T(V^2-1)}\mathbb{Z} & T(V+\chi_{\rm line})\mathbb{I}_2 \end{bmatrix}, \tag{19}$$

with the notations $\mathbb{I}_2 = {\rm diag}(1,1)$ and $\mathbb{Z} = {\rm diag}(1,-1)$. Therefore, the symplectic eigenvalues $\lambda_{1,2}$ satisfy

$$\lambda^2_{1,2} = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right), \tag{20}$$

where

$$\begin{aligned} A &= V^2 + T^2(V+\chi_{\rm line})^2 - 2T(V^2-1), \\ B &= T^2(\chi_{\rm line}+1)^2. \end{aligned} \tag{21}$$

Similarly, the symplectic eigenvalues $\lambda_{3,4,5}$ can be calculated as

$$\lambda^2_{3,4} = \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right), \tag{22}$$

where

$$\begin{aligned} C &= \frac{A\chi_{\rm hom} + V\sqrt{B} + T(V+\chi_{\rm line})}{T(V+\chi_{\rm tot})}, \\ D &= \sqrt{B}\frac{V+\sqrt{B}\chi_{\rm hom}}{T(V+\chi_{\rm tot})}, \end{aligned} \tag{23}$$

and $\lambda_5 = 1$. Based on the above calculations, we can evaluate the security of the proposed CV-QSDC protocol with quantum-one-time pad. The security evaluation is implemented in Step 2 and Step 5 of the protocol. Once the value of the effective information $\Delta I$ is less than 0, we consider the communication process to be insecure and terminate the protocol. In the simulation, the fixed parameters are set as $\varepsilon = 0.05$, $\beta = 0.95$, $v_{\rm el} = 0.01$ and $\eta = 0.6$. All of these values are standard, realistic assumptions based on typical implementations of CV-QKD.[47,48]

To demonstrate the impact of modulation variance and transmission distance on the effective information, Fig. 6 shows the three-dimensional diagram of the effective information $\Delta I$, modulation variance $V_{\rm B}$ and transmission distance $L$. The red solid curve represents the modulation variance at each distance when the maximum effective information is reached, and the green (yellow) dashed line represents the upper (lower) bound of $V_{\rm B}$ when the effective information reaches 80% of its maximum value. We can see that the maximum transmission distance of the protocol can exceed 150 km by optimizing the modulation variance. In addition, it is well-known that if the effective information changes rapidly with $V_{\rm B}$ around its optimal value, it is difficult for Bob to accurately estimate the optimal modulation variance. In Fig. 6, we find that around the red solid curve (maximal effective information), the effective information is insensitive to changes of $V_{\rm B}$, indicating that

the protocol is robust against small fluctuations in modulation variance. When the estimated $V_B$ falls within the range defined by the upper and lower dashed curves, the effective information can exceed 80% of its optimal value $\Delta I_{\max}$.

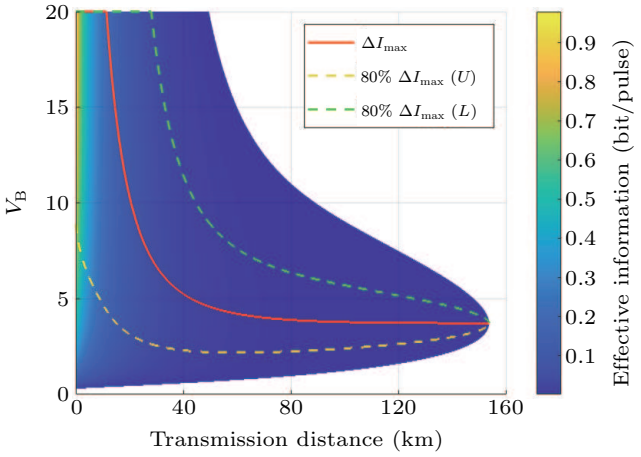



**Fig. 6.** Effective information as a function of modulation variance $V_B$ and transmission distance $L$. The red solid line represents the maximum effective information $\Delta I_{\max}$ at each distance, and the two dashed curves indicate the range where the effective information reaches 80% of its maximum.

## 5. Conclusion

In this paper, we proposed a CV-QSDC protocol with quantum-one-time pad, which employs coherent states and unitary operations to encode secret messages. The process of this protocol is largely consistent with that of the CVQKD protocol and the one-time pad encryption, ensuring the security of secret message encoding and transmission. The QBER of the protocol can be controlled below 1% by adjusting the modulation variance and unitary operation parameters, demonstrating the practicability of the protocol. The security analysis shows that the proposed protocol is secure against collective attacks and can achieve a transmission distance exceeding 150 km.

Despite these promising results, this work has certain limitations that point to valuable directions for future research. Firstly, although the security of the proposed protocol against collective attacks has been analyzed in the asymptotic limit, a comprehensive finite-size security analysis remains an important and non-trivial extension for assessing practical performance. Secondly, our current security analysis does not consider potential security loopholes in practical CV-QSDC systems that could be exploited by Eve, such as the finite linear range of detectors and fluctuations in shot noise. Future research will focus on addressing challenges related to practical implementation, aiming to advance the real-world applicability of CV-QSDC.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 62402178 and 62501084), the Shandong Provincial Natural Science Foundation (Grant No. ZR2024QF285), and the Qilu University of Technology (Shandong Academy of Sciences) Major Project (Grant No. 2025ZDZX02).

## References

[1] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[2] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[3] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[4] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[5] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[6] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[7] Zhang L L, Zhan Y B and Zhang Q Y 2009 *Int. J. Theor. Phys.* **48** 2971
[8] 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
[9] Ying J W , Zhou L , Zhong W and Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[10] Sheng Y B , Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[11] Ying J W, Zhao P, Zhong W, Du M M, Li X Y, Shen S T, Zhang A L, Zhou L and Sheng Y B 2024 *Phys. Rev. Appl.* **22** 024040
[12] Ying J W, Wang J Y, Xiao Y X, Gu S P, Wang X F, Zhong W, Du M M, Li X Y, Shen S T, Zhang A L, Zhou L and Sheng Y B 2025 *Sci. China Phys. Mech. Astron.* **68** 240312
[13] Ding C W, Wang W Y, Zhang W D, Zhou L and Sheng Y B 2025 *Appl. Phys. Lett.* **126** 024002
[14] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[15] Zeng H, Du M M, Zhong W, Zhou L and Sheng Y B 2023 *Fund. Res.* **4** 851
[16] Zhao P, Zhong W, Du M M, Li X Y, Zhou L and Sheng Y B 2024 *Front. Phys.* **19** 51201
[17] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q and Long G L 2016 *Light Sci. Appl.* **5** e16144
[18] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[19] Zhu F, Zhang W, Sheng Y B and Huang Y D 2017 *Sci. Bull.* **62** 1519
[20] Qi R Y, Long G L, Sun Z, Lin Z S, Niu P H, Hao W T, Song L Y, Huang Q, Gao J C and Yin L G 2019 *Light Sci. Appl.* **8** 22
[21] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L and Lu J H 2022 *Light Sci. Appl.* **11** 83
[22] Qi Z T, Li Y H, Huang Y W, Feng J, Zheng Y L and Chen X F 2021 *Light Sci. Appl.* **10** 183
[23] Yang Y L, Li Y H, Li H, Wu C N, Zheng Y L and Chen X F 2025 *Sci. Bull.* **70** 1445
[24] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 1984 Bangalore, India, pp. 175–179
[25] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[26] Chen Y A, Zhang Q, Chen T Y, *et al.* 2021 *Nature* **589** 214
[27] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[28] Huang D, Huang P, Lin D K and Zeng G H 2016 *Sci. Rep.* **6** 19201
[29] Zhang Y C, Chen Z Y, Pirandola S, et al. 2020 *Phys. Rev. Lett.* **125** 010502
[30] Pirandola S, Braunstein S L, Mancini S and Lloyd S 2008 *Europhys. Lett.* **84** 20013
[31] Han L F, Chen Y M and Yuan H 2009 *Commun. Theor. Phys.* **51** 648
[32] Yuan H, Zhou J, Zhang G, Yang H and Xing L L 2012 *Int. J. Theor. Phys.* **51** 3443
[33] Chai G, Cao Z W, Liu W Q, Zhang M H, Liang K X and Peng J Y 2019 *Laser Phys. Lett.* **16** 095207
[34] Cao Z W, Wang L, Liang K X, Chai G and Peng J Y 2021 *Phys. Rev. Appl.* **16** 024012
[35] Wang L, Chai G, Cao Z W, Chen X L and Liang K X 2025 *Quant. Inf. Process.* **24** 214
[36] Cao Z W, Zhang Y J, Chai G, Liang Z T, Chen X L, Wang L and Wang Y J 2025 *Chin. Phys. B* **34** 030303
[37] Cao Z W, Wang Y J, Chai G, Chen X L and Lu Y 2025 *Chin. Phys. B* **34** 020308
[38] Cao Z W, Lu Y, Chai G, Yu H, Liang K X and Wang L 2023 *Research* **6** 0193

[39] Paparella I, Mousavi F, Scazza F, Bassi A, Paris M and Zavatta A 2025 *Opt. Express* **33** 28917
[40] Zhou N R, Song H C and Gong L H 2013 *Int. J. Theor. Phys.* **52** 4174
[41] Qin H, Kumar R and Alléaume R 2016 *Phys. Rev. A* **94** 012325
[42] Qin H, Kumar R, Makarov V and Allé*a*ume R 2018 *Phys. Rev. A* **98** 012312
[43] Pan D, Long G L, Yin L G, Sheng Y B, Ruan D, Ng S X, Lu J H and Hanzo L 2024 *IEEE Commun. Surv. Tutor.* **26** 1898
[44] Marcos C, Maciej L and Norbert L 2004 *Phys. Rev. Lett.* **92** 217903
[45] Jain N, Chin H M, Mani H, Lupo C, Nikolic D S, Kordts A, Pirandola S, Pedersen T B, Kolb M, Ömer B, Pacher C, Gehring T and Andersen U L 2022 *Nat. Commun.* **13** 4740
[46] Anthony L 2017 *Phys. Rev. Lett.* **118** 200501
[47] Huang P, Wang T, Chen R, Wang P, Zhou Y M and Zeng G H 2021 *New J. Phys.* **23** 113028
[48] nag Oruganti A, Derkach I, Filip R and Usenko V C 2025 *Quantum Sci. Technol.* **10** 025023