Continuous-Variable Quantum Secure Direct Communication Based on Gaussian Mapping

Zhengwen Cao, Lei Wang, Kexin Liang, Geng Chai,* and Jinye Peng

Laboratory of Quantum Information & Technology (QIT), School of Information Science and Technology, Northwest University, Xi'an 710127, China

(Received 29 January 2021; revised 7 May 2021; accepted 16 July 2021; published 6 August 2021)

Quantum secure direct communication (QSDC) realizes the transmission of secret messages directly in a quantum channel. A continuous-variable- (CV) based quantum-communication system allows high-speed, large-capacity information transmission in optical telecommunication systems. In this work, we propose a QSDC protocol based on Gaussian mapping. As for Gaussian modulation, the designed Gaussian-mapping scheme effectively solves the problem, which results from the nonuniformity of the secret-message bit-stream, and is applicable to different modulation variances. The system performance analysis shows that the proposed scheme can realize inerrant Gaussian modulation of secret messages, and secure transmission of messages under information theory. Moreover, our work hopes to stimulate discussion on experimental realization and practical advance of CV-QSDC protocol.

DOI: 10.1103/PhysRevApplied.16.024012

I. INTRODUCTION

Quantum secure direct communication (QSDC) [1], which realizes the transmission of secret messages directly in a quantum channel, provides a quantum secure communication different from quantum key distribution (QKD) [2,3]. Thus, it reduces not only the system complexity, but also the risk of information leakage [4].

In the preliminary development of QSDC, some classic protocols construct possible modes of QSDC [5–7], in which the two-step protocol [6] and the one-time pad protocol [7] are proved to be theoretically secure. Both protocols provided the conditions that the QSDC protocol needs to meet and the criterion to judge its security, laying the foundation for the future development of quantum communication. Since the presentation of a high-dimensional scheme based on quantum dense coding [8], the QSDC mode has aroused the interest of researchers and has rapidly developed into a research hotspot in the field of quantum communication. This has been extended to various protocols, such as the multiple-particle protocol [9,10] and the controlled protocol [11,12]. These protocols guarantee security through ensuring that the eavesdropper is unable to obtain two or more entangled particles simultaneously [6,8–13] or by using quantum states to encrypt private messages [7,14,15]. With the enrichment and advancement of QSDC technology, more theoretical researches have paved the way for practical applications. Through the proposal of the measurement-device-independent (MDI) QSDC scheme, including single photons [16] and entangled photons [17], the security loopholes in measurement equipment can be eliminated, resulting in the increase of communication distance. On the other hand, the problems in photon transmission loss and decoherence can be solved through the device-independent (DI) QSDC scheme [18], which guarantees absolute safety in a practical noisy quantum channel. These schemes provided theoretical guidance for the subsequent device design of practical QSDC systems. Besides, a practical encoding method called quantum-channel compression can be employed to improve transmission distance and informational efficiency [19]. Recently, aside from plentiful achievements in theoretical research, experimental researches have also been advancing gradually. Certain developments in QSDC have occurred, such as quantum low-probability interception [20], a practical communication prototype [21], and an experiment in free space [22].

The research progress just described is based on discrete variables. In addition to easy implementation from state preparation to measurement, it is noteworthy that continuous-variable (CV) quantum-communication systems can integrate with existing optical communication systems and speed up its experimental realization and practical promotion process, comparing with the needs to meet conditions like single-photon detection in the discrete variable. Significantly, Pirandola *et al.* initially put forward a secure quantum direct communication (SQDC) scheme with coherent states and gave a brief discussion about

*chai.geng@nwu.edu.cn

the security [23]. Furthermore, a higher security was realized through modifying spin coherent states [24]. Since the noise properties of a squeezed-state light field is better than that of a coherent-state light field, which is more conducive to the detection and extraction of weak signals, some QSDC schemes based on squeezed states were born [25–28]. The development of entanglement purification and entanglement distribution promotes the protocol based on two-mode squeezed states to the specific application stage [29,30], so the research in this field becomes more meaningful. Most of the existing CV-QSDC schemes consider the introduction of a continuous-variable pattern but do not systematically solve performance analysis issues. In order to promote the cooperative development of quantum-communication system with continuous variables, including QKD and QSDC, a CV-QSDC scheme based on Gaussian mapping is proposed, relying on the more mature Gaussian-modulation-based CV QKD.

In this work, we propose a CV-QSDC scheme based on Gaussian mapping using two-mode squeezed states, which employs a Gaussian source and Gaussian modulation to realize the secure transmission of quantum signals carrying secret messages. Concretely, the offset problem is caused by the nonuniformity of the secret-information bitstream directly encoded as a Gaussian random number, so that a Gaussian-mapping scheme is designed to effectively solve this problem, and the stable realization of Gaussian modulation can be ensured under diverse variances. Finally, the security of the proposed protocol based on Gaussian mapping is analyzed systematically. The analysis shows that the proposed scheme can realize inerrant Gaussian modulation of secret messages, and secure transmission of messages under the information theory. Moreover, our work hopes to stimulate discussion on the experimental realization and practical advance of the CV-QSDC protocol.

The rest of this paper is organized as follows. In Sec. II, we describe the protocol based on Gaussian mapping, including the data postprocessing stage. We further depict the impact of the offset problem, and introduce the specific implementation method of Gaussian-mapping operation, and then analyze its results under different variances. In Sec. III, we analyze the system performance of the protocol under collective attacks and compare the system performance with and without Gaussian mapping. Finally, our summary is in Sec. IV.

II. CV QSDC BASED ON THE GAUSSIAN-MAPPING PROTOCOL

Next, the proposed protocol is introduced, and its Gaussian mapping is also analyzed. Specifically, we introduce the designed CV QSDC based on the Gaussian-mapping protocol in detail in Sec. II A. The protocol contains two main phases: quantum-information processing phase and information postprocessing phase. For the message modulation in the quantum-information processing phase, we propose a Gaussian-mapping scheme and introduce it clearly in Sec. II B.

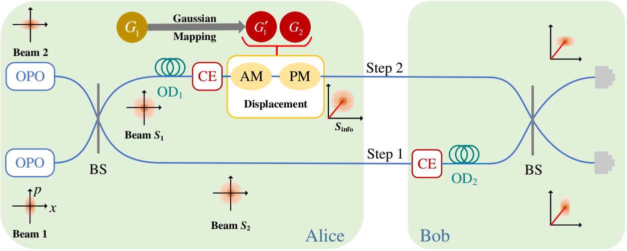

FIG. 1. System diagram of QSDC based on two-mode squeezed states. OPO, optical parametric oscillator; BS, 50:50 beam splitter; AM, amplitude modulation; PM, phase modulation; CE, checking eavesdropping, includes two stages: channel detection and identity authentication; G_1, a Gaussian sequence; G_1', a Gaussian sequence after the Gaussian mapping; G_2, another Gaussian sequence; both OD$_1$ and OD$_2$ are optical delays. The former represents the time that beam S_2 is transmitted to Bob, and the latter represents the sum of the time that beam S_1 is modulated and transmitted to Bob.

A. Protocol steps

In this section, we describe each step of the protocol as shown in Fig. 1, which is divided into two parts: security detection and message transmission. Furthermore, the protocol description is as follows.

(a) **Step 1 (Preparation stage):** the squeezed vacuum state is produced by the optical parametric oscillator. In phase space, the quadrature position (x) or quadrature momentum (p) of the vacuum state is compressed to generate different squeezed vacuum states. Specifically, beam 1 and beam 2 are represented as

$$x_1 = \exp(-r)\,|0\rangle_{x_1}, p_1 = \exp(r)\,|0\rangle_{p_1} \tag{1}$$

and

$$x_2 = \exp(r)\,|0\rangle_{x_2}, p_2 = \exp(-r)\,|0\rangle_{p_2}, \tag{2}$$

where $r\,(> 0)$ is the compression coefficient. As the input state, the vacuum state with a subscript denotes its one of quadrature components.

Two-mode squeezed lights S_1 (signal light) and S_2 (detection light) are generated by beam 1 and beam 2 passing through a 50:50 beam splitter. They are described by

$$X_1 = \frac{1}{\sqrt{2}}(x_1 + x_2), P_1 = \frac{1}{\sqrt{2}}(p_1 + p_2) \tag{3}$$

and

$$X_2 = \frac{1}{\sqrt{2}}\left(x_2 - x_1\right), P_2 = \frac{1}{\sqrt{2}}\left(p_2 - p_1\right). \tag{4}$$

Alice then retains one of the beams S_1, and sends the other beam S_2 to Bob.

(b) **Step 2 (Channel detection stage):** Alice selects a group of random positions on the pair of entangled beams and measures x and p components of her beam S_1 at these positions. She then publishes the selected positions and her measurement results. Bob chooses the same positions as Alice to measure two components simultaneously, and combines his measurement results with Alice's for entanglement judgment, using the inseparability criterion [31], which is expressed as

$$\left\langle (\Delta X_m)^2 \right\rangle + \left\langle (\Delta P_m)^2 \right\rangle < 2, \tag{5}$$

where X_m and P_m represent the measurement results of x and p components, and "1" means the Einstein-Podolsky-Rosen (EPR) noise, which is observed when each EPR pair is detected separately.

For a selected position, if their results satisfy the above inequality, the information of the position is secure. After tallying the combination results of all selected locations, if the error rate is lower than the threshold, they will continue to step 3. Otherwise, the communication has to be terminated.

(c) **Step 3 (Authentication stage):** similarly, after the measurement, Bob tells Alice the information of measurement positions and measurement results. After that, they choose whether to proceed to the next step according to the combination results. Moreover, the purpose of this stage is to verify Bob's identity, because only legitimate communication parties can use the classical channel to publish information.

(d) **Step 4 (Gaussian-mapping stage):** after the secret messages are divided into m information blocks, with the help of a Gaussian random sequence G_1 with mean zero and variance V_A, the Gaussian-mapping operation is performed on each information block to obtain a corresponding set of Gaussian random variables. Finally, the secret messages are mapped to a string of Gaussian random sequence $G_1'(\subseteq G_1)$.

(e) **Step 5 (Gaussian modulation stage):** the sequence G_1' is used to modulate the quadrature position X or the quadrature momentum P of S_1 and anther Gaussian random sequence $G_2(\neq G_1')$ is adopted to modulate another quadrature component of S_1. The so-called modulation refers to the operation on the position of phase space through the action of displacement operator $\hat{D}(\alpha)$. The concrete realization is the joint action of amplitude modulator and phase modulator. After modulation, the beam S_1 evolves into the signal beam S_{info} that is sent to Bob.

(f) **Step 6 (Measurement stage):** after receiving S_{info}' experienced through the quantum channel, Bob employs a heterodyne detector to measure the two quadrature components of S_{info}' with the assistance of detection light S_2' (after channel transmission) and obtains the measurement results, which can be described as follows:

$$\begin{aligned} X_m &= \frac{1}{\sqrt{2}}\left(X_{\text{info}}' - X_2'\right), \\ P_m &= \frac{1}{\sqrt{2}}\left(P_{\text{info}}' + P_2'\right). \end{aligned} \tag{6}$$

(g) **Step 7 (Postprocessing stage):** the transmission and measurement of the quantum state are inevitably influenced by the unknown characteristics of quantum channel and the imperfections of practical commercial devices [32], which will ulteriorly cause the deterioration of system performance. Thereby, information postprocessing ought to be implemented before Gaussian inverse mapping. Generally speaking, the postprocessing stage mainly includes parameter estimation, reverse reconciliation, and privacy amplification.

(i) In the parameter estimation part: Bob measures the component on which the sequence G_2 is modulated and gets the results. Alice then sends the sequence G_2 to Bob over a publicly authenticated secure channel. Traditionally, Bob utilizes the measuring results and the results received from Alice as a set of associated data to complete the parameter estimation.

(ii) In the reverse reconciliation part: following the parameter estimation, Alice and Bob correct the sequences G_1' and G_1'' (G_1' after experiencing the quantum channel) through applying a reconciliation strategy and an error-correcting scheme in order to obtain a set of identical reconciliatory sequence.

(iii) In the privacy amplification part: before the secret-information block is restored, the communication parties employ privacy amplification to eliminate redundant information introduced by the Gaussian-mapping process and the information that the transmission process may leak to the eavesdropper Eve. Eventually, the secure transmission of secret messages is realized.

B. Gaussian-mapping scheme

In CV-QKD, the original Gaussian random number G_1 is modulated directly on the quadrature component of light field, and the mean and variance of the modulated coherent states obtained are consistent with those of random number. However, in the proposed protocol, the correspondence between the secret-message block and Gaussian random number G_1 is realized through random sampling, so as to obtain the Gaussian random number G_1' for Gaussian modulation. When the probability of "0" and "1" in the secret messages, P_0 and P_1, is not uniform, the direct

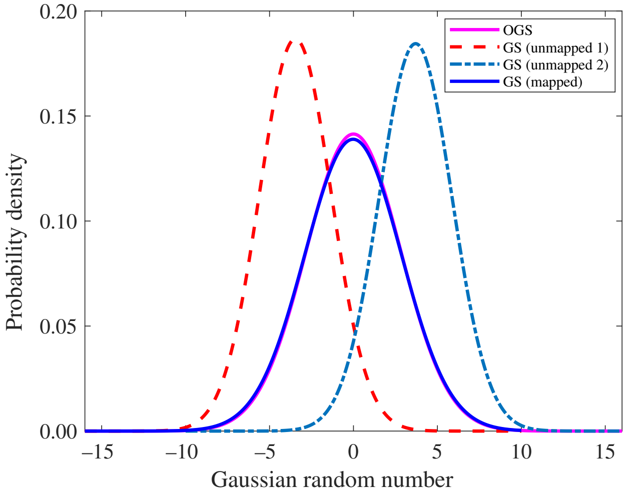

FIG. 2. Probability density-function diagram of Gaussian sequences. The red dashed line expresses the Gaussian sequence without Gaussian mapping and “0” occurrences are more in secret messages. The blue dashed line expresses the Gaussian sequence without Gaussian mapping and “1” occurrences are more in secret messages. The Gaussian sequence with Gaussian mapping is in the blue gray line. OGS, original Gaussian sequence with mean zero and variance $V_A = 8$.

coding of secret messages will lead to an offset of the mean and variance of Gaussian sequence G'_1 compared with sequence G_1. As shown in Fig. 2, the red and blue dotted lines, respectively, represent the distribution of G'_1 when $P_0 > P_1$ and $P_0 < P_1$. It can be seen that the left or right shift of the mean is determined by the probability of “0” and “1” in the secret messages. No matter what the probability distribution is, the variance is always reduced. The modulation variance is critical to the system performance analysis and affects subsequent postprocessing, thus posing a threat to the practical security of the system. Therefore, the Gaussian-mapping scheme is the core of the proposed protocol.

The offset issue that results from the nonuniformity of secret messages can be solved through the designed Gaussian-mapping scheme, which is briefly described as follows: first of all, the probability of “0” and “1” in the secret messages can be uniform through code conversion. Following that, all bits in each information block are randomly replaced by 2-bit code elements (for example, one code element in $\{00, 01\}$ is randomly selected to replace the “0” code element and vice versa). Then continuing to chunk each information block, detection bits and error-correction codes are randomly inserted for each data block. Finally, different data blocks correspond to arbitrary Gaussian random number in different regions under the mapping rules.

The simulation analysis is demonstrated in Fig. 2, the purple-red solid line and the blue solid line individually represent the distribution of the original Gaussian sequence G_1 and that of G'_1, which is generated with Gaussian mapping. The analysis shows that two curves are almost coincident, which means that the offset issue results from the nonuniformity of secret messages is treated. Obviously, the Gaussian-mapping scheme introduces redundant information while solving the offset issue, which not only increases the randomness of the secret messages, but also provides the operation space for the subsequent postprocessing phase.

The process diagram of Gauss mapping is shown in Fig. 3. After secret messages of length k is divided into n blocks, the following operations are performed on each block of messages.

(a) **Uniformization of messages:** the probability of “0” and “1” in the secret messages can be uniform through code conversion. For example, one code element in $\{01, 10\}$ is alternately selected to replace the “0” code element, and another code element in $\{00, 11\}$ is alternately selected to replace the “0” code element.

(b) **Uniformization of blocks:** all bits in each information block are randomly replaced by 2-bit code elements. Concretely, one code element in $\{00, 01\}$ is randomly selected to replace the “0” code element, and another code element in $\{10, 11\}$ is randomly selected to replace the “1” code element.

(c) **Detection bits:** continuing to divide the information block into m boxes, d detection bits are inserted randomly into each boxes. Its purpose is to realize security detection in the process of information transmission.

(d) **Error correction:** an appropriate error-correction code is randomly placed in a fixed position for each box. The purpose is to correct the error code caused by channel transmission or eavesdropping interference.

(e) **Mapping:** the sequence G_1 with zero mean and variance V_A is divided into $2^{[(4k/nm)+d]}$ intervals according to the rule of equal probability. The box corresponding to the interval is mapped to the arbitrary Gaussian random number belonging to this interval.

As an instance, a Gaussian-mapping scheme in detail is demonstrated in Fig. 3. The information block “10” is transformed into an codeword “0001” through code conversion, and then is converted into uniformly distributed four boxes $\{01, 01, 00, 10\}$ through random operation. Then, a detection bit is randomly inserted into each four boxes to obtain $\{010, 101, 000, 100\}$, and then an odd parity bit is placed at the end of the boxes to obtain $\{0100, 1011, 0001, 1000\}$. Since there exists only one uniquely identified odd parity bit in a box, it will not affect the division of Gaussian-mapping interval, so the division of Gaussian sequence is completed according to the box with detection bits. Eventually, the Gaussian random number is divided into eight intervals according

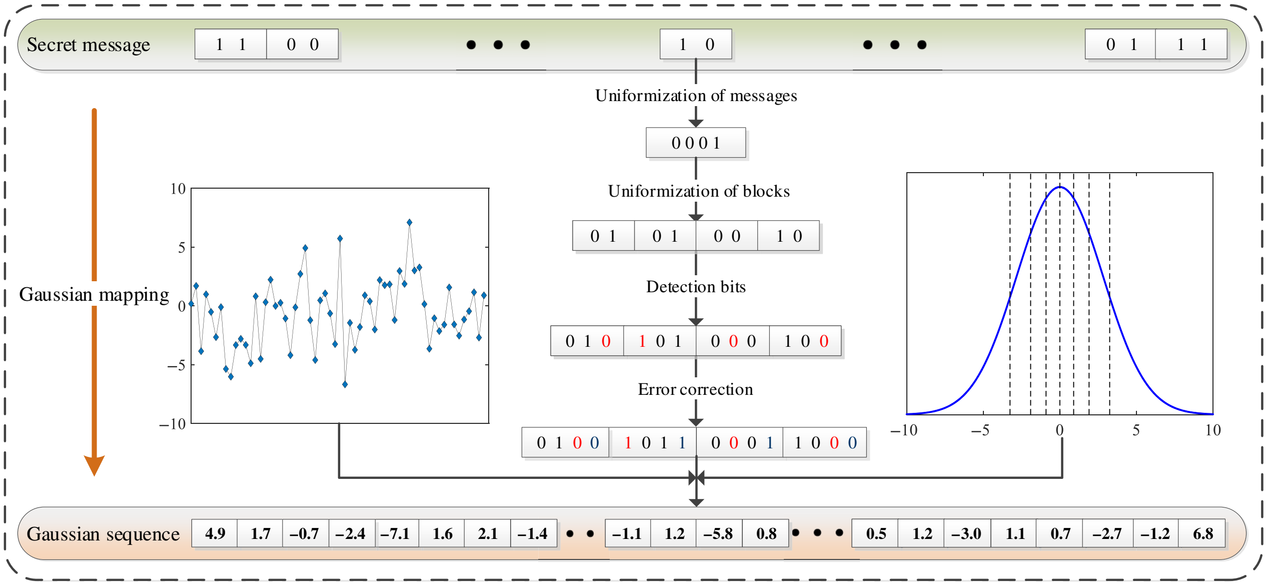

FIG. 3. Process diagram of Gaussian mapping. The small figure on the left represents the randomly generated original Gaussian sequence with the variance 8, and its probability density-function diagram is in the small picture on the right. The mapping operation is showed in the small picture on the right as well. The abscissa axis is divided into eight intervals under the rule of equal probability: $(-\infty, -3.2537]$, $(-3.2537, -1.9077]$, $(-1.9077, -0.9012]$, $(-0.9012, 0]$, $\cdots$, $(1.9077, 3.2537]$, $(3.2537, +\infty)$. These intervals, respectively, represent the binary numbers 000, 001, 010, 011, 100, 101, 110, 111.

to the principle of equal probability, which correspond to eight code elements $\{000, 001, \cdots, 111\}$ as illustrated in Table I. For the box of $\{010, 101, 000, 100\}$, arbitrary Gaussian random number in the corresponding interval is selected, hence the Gaussian-mapping variable is $\{-1.1, 1.2, -5.8, 0.8\}$.

The above analysis for Gaussian mapping is carried out in the case of the variance 8 of the original Gaussian sequence. In order to test that Gaussian mapping is still applicable in other situations, we conduct verification under different variances. It is worth noting that as the variance changes, the interval division in the mapping mechanism should be adjusted according to the principle of equal probability. Otherwise, there exists large differences between the variance of the original sequence and the sequence with Gaussian mapping. Through comparing the probability density function under different variances, it can be seen that the Gaussian mapping still has an obvious effect on correcting alterant variance as shown in Fig. 4. In addition, it is obvious that in order to satisfy the requirements of Gaussian mapping, the number of random numbers in the original sequence G_1 is greater than that in the sequence G_1' after Gaussian mapping. Although the numbers of these two sequences are different, there is almost no difference in their variances. Therefore, no matter how the variance changes, the Gaussian-mapping scheme can solve the offset problem.

TABLE I. Mapping mechanisms.

000 $(-\infty, -3.25]$	001 $(-3.25, -1.91]$	010 $(-1.91, -0.90]$	011 $(-0.90, 0]$
100 $(0, 0.90]$	101 $(0.90, 1.91]$	110 $(1.91, 3.25]$	111 $(3.25, +\infty)$

III. SYSTEM PERFORMANCE ANALYSIS

In Sec. II A, channel detection and identity authentication, as two stages of checking eavesdropping, jointly complete the security detection of the channel. Both results are within the security threshold, meaning that the channel is secure. Only when the channel is secure, can secret-message transmission be carried out. That is to say, the detection light and the signal light are transmitted to Bob successively through the same channel.

When only one of the entangled pairs is stolen, the valuable information cannot be read. Considering that the detection light is secure, the eavesdropper Eve cannot recover the secret information, even if she intercepted the signal light. Thus, as long as the security of the detection light is guaranteed, the protocol is secure. However, if both sides of the communication did not detect the eavesdropper, the eavesdropper can easily obtain two entangled beam pairs, and measure them to obtain the secret information. In fact, even if Eve intercepts the information block, it is just a string of Gaussian random numbers to her. Even so, in order to further ensure the security of the protocol, we can judge whether the encrypted information is leaked through parameter estimation, analyzing the relevance of

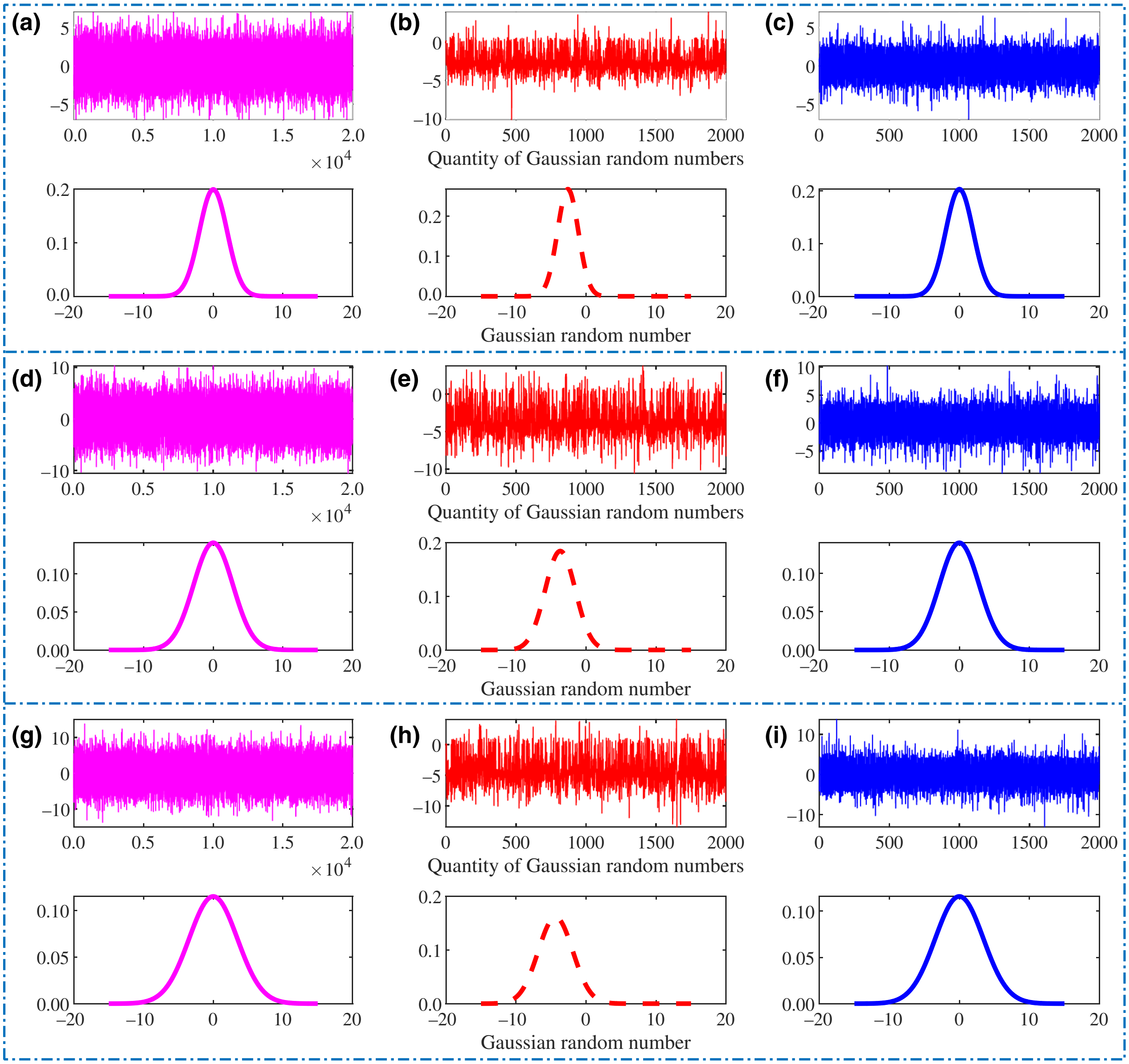

FIG. 4. The data diagram of Gaussian mapping. Left to right corresponds to the original Gaussian sequence, the sequence without Gaussian mapping, the sequence with Gaussian mapping. From top to bottom, the first two rows, the middle two rows, and the last two rows represent the variances of 4, 8, and 12, respectively. Each unit contains two subgraphs: the sequence itself and its probability density function. In the subgraph describing the sequence, the horizontal and vertical coordinates represent data points and values, respectively.

information between the two communication parties. In particular, only one of Bob and Eve can accurately measure the quadrature components of light field. Hence, if the relevance between Eve and Alice is higher, it means that Bob can discover Eve by comparing with Alice. And the communication will be aborted, so it will not be carried out for the process of restoring the secret information, which ensures the security of the secret information.

As the detection light is secure, the eavesdropper cannot have both entangled beams, actually. Therefore, our security analysis is based on the secure transmission of detection light, which is similar to the two-step QSDC protocol [6]. As shown in Fig. 5, in order to analyze the maximum of information that the eavesdropper can obtain, we assume that Alice prepares a pair of entangled lights, and sends the detection light to Bob after measuring the signal light. Since the detection light itself does not carry any information, we add the modulation process to the detection stage to quantitatively analyze the amount of information. Moreover, the process of information modulation is equivalent to the change of quantum state “*B*” caused by Alice’s measurement. It is consistent with the

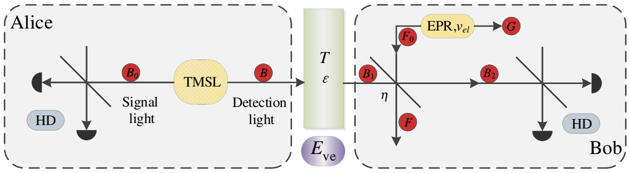

FIG. 5. Entanglement-based scheme of the Gaussian-modulation CV-QSDC protocol with heterodyne detection. TMSL, two-mode squeezed-state light source; HD, heterodyne detection; T, transmittance; ε, excess noise; the imperfection of the detector is described by the detection efficiency η and the electronic noise ν_{el} contained in variance ν.

entanglement-based (EB) model in CV QKD [33], so the security analysis is based on this model.

Two quantum lights generated by the two-mode squeezed-state source are essentially entangled continuous-variable quantum signals. The eavesdropper Eve can mainly use three attack methods against the continuous-variable quantum system of Gaussian source: individual attacks, collective attacks, and coherent attacks. The current research shows that in contrast to individual attacks, collective attacks and coherent attacks are more threatening to CV systems, and coherent attacks can not obtain more information than collective attacks under reverse reconciliation [34]. Therefore, this work primarily discusses the security of the CV-QSDC protocol under collective attacks.

In the case of collective attacks and reverse reconciliation, secure and effective information (*bits*/*pulse*) between Alice and Bob is defined as [35]

$$\Delta I = \beta I_{AB} - \chi_{BE}, \tag{7}$$

where $\beta \in (0,1)$ is the efficiency of reverse reconciliation, χ_{BE} stands for the maximum information that Eve can access from Bob by the constraints of the Holevo bound [36,37].

The mutual information I_{AB}, between Alice and Bob, is expressed as [38]

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{V_B}{V_{B|A}}\right) = \frac{1}{2}\log_2\left(\frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}\right), \tag{8}$$

and the total noise is $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{het}}/T$, the linear noise in channel is $\chi_{\text{line}} = 1/T - 1 + \varepsilon$, and the detection noise is $\chi_{\text{het}} = 2\,(1+\nu_{\text{el}})/\eta - 1$.

As for heterodyne detection, Bob's measured value is $m_B = x_B, p_B\ (dm_B = dx_B dp_B)$, thus the maximum information listened by Eve is given by

$$\chi_{BE} = S(\rho_E) - \int dm_B p\,(m_B)\, S\left(\rho_E^{m_B}\right), \tag{9}$$

where $p\,(m_B)$ indicates the probability density of measured value, $\rho_E^{m_B}$ represents the eavesdropper's states after Bob's measurement, and $S(\rho)$ is the von Neumann entropy of the quantum state. Eve's eavesdropping purifies the system to $\rho_{B_0B_1}$, and after Bob's measurement, $S\left(\rho_E^{m_B}\right) = S\left(\rho_{B_0FG}^{m_B}\right)$, in which $S\left(\rho_{B_0FG}^{m_B}\right)$ and Bob's measurement results are mutually independent, so χ_{BE} is as follows [39]:

$$\chi_{BE} = S\left(\rho_{B_0B_1}\right) - S\left(\rho_{B_0FG}^{m_B}\right). \tag{10}$$

For the Gaussian state, Eq. (10) can be simplified to

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{11}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2}$ are the symplectic eigenvalues corresponding to the covariance matrix $\gamma_{B_0B_1}$ of the quantum state $\rho_{B_0B_1}$, and $\lambda_{3,4,5}$ are the symplectic eigenvalues of $\gamma_{B_0FG}^{m_B}$.

Regardless of the measuring method, the covariance matrix $\gamma_{B_0B_1}$ is directly written as

$$\begin{aligned}\gamma_{B_0B_1} &= \begin{pmatrix} \gamma_{B_0} & \sigma_{B_0B_1}^T \\ \sigma_{B_0B_1} & \gamma_{B_1} \end{pmatrix} \\ &= \begin{pmatrix} V\cdot I_2 & \sqrt{T\left(V^2-1\right)}\cdot\sigma_Z \\ \sqrt{T\left(V^2-1\right)}\cdot\sigma_Z & T\,(V+\chi_{\text{line}})\cdot I_2 \end{pmatrix},\end{aligned} \tag{12}$$

where I_2 is the identity matrix of two order, and $\sigma_Z = \text{diag}\{1,-1\}$. The symplectic eigenvalues, $\lambda_{1,2}(\geq 1)$, are as follows:

$$\lambda_{1,2}^2 = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right), \tag{13}$$

and

$$\begin{aligned} A &= V^2\,(1-2T) + 2T + T^2(V+\chi_{\text{line}})^2, \\ B &= T^2(V\chi_{\text{line}} + 1)^2. \end{aligned} \tag{14}$$

The covariance matrix $\gamma_{B_0FG}^{m_B}$ related to the measuring method is expressed by

$$\gamma_{B_0FG}^{m_B} = \gamma_{B_0FG} - \sigma_{B_0FGB_2}^T H_{\text{het}} \sigma_{B_0FGB_2}. \tag{15}$$

Since heterodyne detection measures two quadrature components simultaneously, an additional vacuum noise is introduced, and $H_{\text{het}} = \left(\gamma_{B_2} + I_2\right)^{-1}$. The covariance matrix $\gamma_{B_0FGB_2}$, which can be derived from the transformation of the rows and columns corresponding to the subscripts of the matrix $\gamma_{B_0B_2FG}$, is decomposed into blocks to know the matrixes γ_{B_0FG}, γ_{B_2} , $\sigma_{B_0FGB_2}$ as follows:

$$\gamma_{B_0B_2FG} = \left(Y^{\mathrm{BS}}\right)^T\left(\gamma_{B_0B_1} \oplus \gamma_{F_0G}\right)\left(Y^{\mathrm{BS}}\right),$$
$$\gamma_{B_0FGB_2} = \begin{pmatrix} \gamma_{B_0FG} & \sigma^T_{B_0FGB_2} \\ \sigma_{B_0FGB_2} & \gamma_{B_2} \end{pmatrix}, \tag{16}$$

where the matrices γ_{F_0G} and Y^{BS}, respectively, represent the covariance matrix of equivalent EPR source and the transmission matrix of beam splitter BS, which are as follows:

$$\gamma_{F_0G} = \begin{pmatrix} \nu.I_2 & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & \nu.I_2 \end{pmatrix},$$
$$Y^{\mathrm{BS}} = I_{B_0} \oplus \begin{pmatrix} \sqrt{\eta}\cdot I_2 & \sqrt{1-\eta}\cdot I_2 \\ -\sqrt{1-\eta}\cdot I_2 & \sqrt{\eta}\cdot I_2 \end{pmatrix} \oplus I_G, \tag{17}$$

where variance ν represents the electronic noise of the detectors. $\lambda_{3,4,5}(\geq 1)$ are derived from calculating eigenvalue equation of matric γ_{B_0FG}, which are as follows:

$$\lambda^2_{3,4} = \frac{1}{2}\left(C \pm \sqrt{C^2-4D}\right), \lambda_5 = 1, \tag{18}$$

and

$$C = \frac{A\chi^2_{\mathrm{het}} + B + 1 + 2\chi_{\mathrm{het}}\left(V\sqrt{B} + T\left(V+\chi_{\mathrm{line}}\right)\right) + 2T\left(V^2-1\right)}{T^2\left(V+\chi_{\mathrm{tot}}\right)^2},$$
$$D = \frac{\left(V+\sqrt{B}\chi_{\mathrm{het}}\right)^2}{T^2\left(V+\chi_{\mathrm{tot}}\right)^2}. \tag{19}$$

Substituting the above equations into Eq. (7), the system performance of the Gaussian modulation CV-QSDC protocol under collective attacks is demonstrated in Fig. 6. The red solid line stands for the system performance with variance $V_A = 8$ under theoretical analysis based on fiber channel. It can be seen that the increase of transmission distance is accompanied by the decrease of channel performance, which restricts the system performance of continuous variables.

Furthermore, the system performance analysis is performed under the influence of the offset problem. Under this circumstance that the mean and variance of the Gaussian sequence change, it leads to the erroneous estimation of the modulation variance, which in turn affects the estimation of channel parameters such as transmittance T and excess noise ε. On the other hand, this also leads to an erroneous postprocessing process of variables, thereby affecting the restoration of secret messages, and bringing about a security threat to practical systems. Ultimately, the correct transmission of messages and the security of systems cannot be guaranteed. As shown in Fig. 6, the purple-red dotted line represents system performance with variance $V_A = 7$ without Gaussian mapping. It shows that the final consequence without Gaussian mapping overestimates system performance. In other words, the security scope of systems without Gaussian mapping is larger than its under theoretical analysis, so the eavesdropper Eve can hide their behaviors in an overestimated range to intercept secret messages without being perceived by two communication partners. The blue dotted line stands

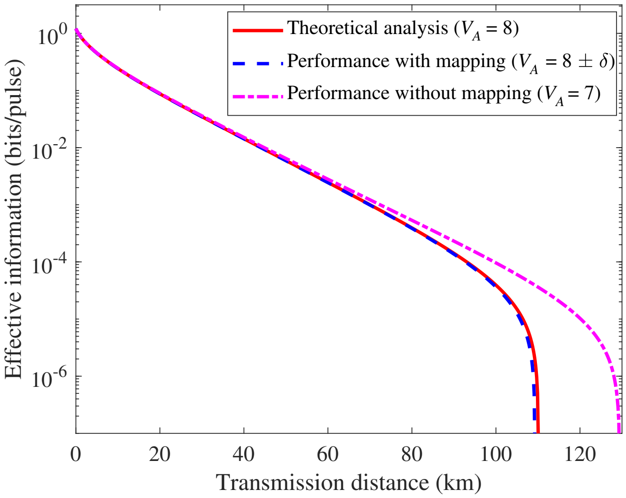

FIG. 6. The relationship between the effective information and the transmission distance with theoretical analysis, Gaussian mapping, and without Gaussian mapping. δ represents the error of the variance with Gaussian mapping, which is a tiny amount.

for system performance with variance $V_A = 8 \pm \delta$ under Gaussian mapping, where δ represents the error of the variance. Whereas, the system performance with Gaussian mapping is nearer to its under theoretical analysis to a greater extent. Therefore, the designed scheme can effectively solve the offset of Gaussian sequence variance and mean, thus ensuring the security of the system.

Finally, comparing with DV system, QSDC based on CV has higher information capacity and transmission rate. It is reasonable to believe that the further coordinated development of CV-QSDC and CV-QKD based on Gaussian modulation will greatly promote the practical process of quantum secure communication. In the security analysis, the security risks caused by the overestimation of system performance, which results from the offset of modulation variance, are compensated through Gaussian mapping. Gaussian mapping lays a theoretical foundation for the practical implementation of CV QSDC in the future.

IV. CONCLUSION

In conclusion, we propose a CV-QSDC protocol based on Gaussian mapping. In the message modulation stage, secret messages are divided into blocks followed by the information blocks being mapped into a set of Gaussian random sequence. And the sequence is modulated to the quadrature component of the signal light via Gaussian modulation. In the communication process, the signal light can only be transmitted when the detection light is deemed secure, and only when the previous data block is securely received can the next data block be transmitted. In addition, we design a Gaussian-mapping scheme for the offset problem and verify its validity on different variances. The analysis shows that the mean and variance of the Gaussian sequence after Gaussian mapping are almost unchanged from the original sequence even though the probabilities “0” and “1” of the secret messages are not uniform. Gaussian mapping lays a theoretical foundation for the practical implementation of CV QSDC in the future. Furthermore, we mainly analyze the system performance of the protocol based on reverse reconciliation under collective attacks. The results show that the proposed scheme can realize inerrant Gaussian modulation of secret messages, and secure transmission of messages under information theory. Moreover, further work will be carried out, such as practical error-correction methods and so on.

We hope that this work will encourage the QSDC scheme based on CV to be further advanced and shorten its practical time. It is reasonable to believe that the further coordinated development of CV QSDC and CV QKD based on Gaussian modulation will greatly promote the practical process of quantum secure communication.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 62071381).

[1] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, Phys. Rev. A **65**, 032302 (2002).

[2] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York, 1984), p. 175.

[3] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[4] G. L. Long, in 2017 IEEE 85th Vehicular Technology Conference (IEEE, Sydney, 2017), p. 1.

[5] K. Boström and T. Felbinger, Deterministic Secure Direct Communication Using Entanglement, Phys. Rev. Lett. **89**, 187902 (2002).

[6] F. G. Deng, G. L. Long, and X. S. Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, Phys. Rev. A **68**, 042317 (2003).

[7] F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, Phys. Rev. A **69**, 052319 (2004).

[8] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Quantum secure direct communication with high-dimension quantum superdense coding, Phys. Rev. A **71**, 044305 (2005).

[9] C. Wang, F. G. Deng, and G. L. Long, Multi-step quantum secure direct communication using multi-particle green–horne–zeilinger state, Opt. Commun. **253**, 15 (2005).

[10] H. J. Cao and H. S. Song, Quantum secure direct communication with w state, Chin. Phys. Lett. **23**, 290 (2006).

[11] Y. Xia, S. Zhang, F. Y. Li, K. H. Yeon, F. C. Bo, and C. I. Um, Controlled secure direct communication by using GHZ entangled state, J. Korean Phys. Soc. **47**, 753 (2006).

[12] L. L. Zhang, Y. B. Zhan, and Q. Y. Zhang, Controlled quantum secure direct communication by using four particle cluster states, Int. J. Theor. Phys. **48**, 2971 (2009).

[13] A. M. Marino and C. R. Stroud, Deterministic secure communications using two-mode squeezed states, Phys. Rev. A **74**, 022315 (2006).

[14] S. Pirandola, S. L. Braunstein, S. Lloyd, and S. Mancini, Confidential direct communications: A quantum approach using continuous variables, IEEE J. Sel. Top. Quan. **15**, 1570 (2009).

[15] J. Wang, Q. Zhang, and C. J. Tang, Quantum secure direct communication based on order rearrangement of single photons, Phys. Lett. A **358**, 4 (2006).

[16] Z. R. Zhou, Y. B. Sheng, P. H Niu, L. G. Yin, G. L. Long, and L. Hanzo, Measurement-device-independent quantum secure direct communication, Sci. China Phys. Mech. **63**, 230362 (2020).

[17] P. H. Niu, Z. R. Zhou, Z. S. Lin, Y. B. Sheng, L. G. Yin, and G. L. Long, Measurement-device-independent quantum communication without encryption, Sci. Bull. **63**, 1345 (2018).

[18] L. Zhou, Y. B. Sheng, and G. L. Long, Device-independent quantum secure direct communication against collective attacks, Sci. Bull. **65**, 12 (2020).

[19] G. Bebrov and R. Dimova, Efficient quantum secure direct communication protocol based on quantum channel compression, Int. J. Theor. Phys. **59**, 426 (2020).

[20] J. H. Shapiro, D. M. Boroson, P. B. Dixon, M. E Grein, and S. A. Hamilton, Quantum low probability of intercept, J. Opt. Soc. B **36**, B41 (2019).

[21] R. Y. Qi, Z. Sun, Z. S. Lin, P. H. Niu, W. T. Hao, L. Y. Song, Q. Huang, J. C. Gao, L. G. Yin, and G. L. Long, Implementation and security analysis of practical quantum secure direct communication, Light-Sci. Appl. **8**, 1 (2019).

[22] D. Pan, Z. S. Lin, J. W. Wu, Z. Sun, D. Ruan, L. G. Yin, and G. L. Long, Experimental free-space quantum secure direct communication and its security analysis, Photonics Res. **8**, 09001522 (2020).

[23] S. Pirandola, S. L. Braunstein, S. Mancini, and S. Lloyd, Quantum direct communication with continuous variables, EPL-Europhys. Lett. **84**, 548 (2008).

[24] A. Meslouhi and Y. Hassouni, A quantum secure direct communication protocol using entangled modified spin coherent states, Quantum Inf. Process. **12**, 2603 (2013).

[25] Y. Li, C. L. Ji, S. R. Ji, and M. T. Xu, Continuous variable quantum secure direct communication in non-markovian channel, Int. J. Theor. Phys. **54**, 1968 (2015).

[26] Z. B. Yu, L. H. Gong, and R. H. Wen, Novel multi-party controlled bidirectional quantum secure direct communication based on continuous-variable states, Int. J. Theor. Phys. **55**, 1447 (2016).

[27] G. Chai, Z. W. Cao, W. Q. Liu, M. H. Zhang, K. X. Liang, and J. Y. Peng, Novel continuous-variable quantum secure direct communication and its security analysis, Laser Phys. Lett. **16**, 095207 (2019).

[28] S. Srikara, K. Thapliyal, and A. Pathak, Continuou variable direct secure quantum communication using gaussian states, Quantum Inf. Process. **19**, 1 (2020).

[29] G. Y. Wang, T. Li, Q. Ai, A. Alsaedi, T. Hayat, and F. G. Deng, Faithful Entanglement Purification for High-Capacity Quantum Communication with Two-Photon Four-Qubit Systems, Phys. Rev. Appl. **10**, 054058 (2018).

[30] P. L. Guo, T. Li, Q. Ai, and F. G. Deng, Self-error-rejecting quantum state transmission of entangled photons for faithful quantum communication without calibrated reference frames, EPL-Europhys. Lett. **127**, 60001 (2019).

[31] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Inseparability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2722 (2000).

[32] L. Ruppert, V. C. Usenko, and R. Filip, Long-distance continuous-variable quantum key distribution with efficient channel estimation, Phys. Rev. A **90**, 062310 (2014).

[33] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, Quantum Inf. Comput. **3**, 535 (2003).

[34] R. Renner and J. I. Cirac, de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

[35] B. Kraus, C. Branciard, and R. Renner, Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses, Phys. Rev. A **75**, 012316 (2007).

[36] M. Navascués, F. Grosshans, and A. Acin, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[37] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Peredachi. Inf. **9**, 3 (1973).

[38] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, J. Phys. B **42**, 114014 (2009).

[39] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).