Research
A SCIENCE PARTNER JOURNAL

RESEARCH ARTICLE

Realization of Quantum Secure Direct Communication with Continuous Variable

Zhengwen Cao, Yuan Lu, Geng Chai*, Hao Yu, Kexin Liang, and Lei Wang

School of Information Science and Technology, Northwest University, Xi'an710127, China.

*Address correspondence to: chai.geng@nwu.edu.cn

Citation: Cao Z, Lu Y, Chai G, Yu H, Liang K, Wang L. Realization of Quantum Secure Direct Communication with Continuous Variable. *Research* 2023;6:Article 0193. https://doi.org/10.34133/research.0193

Submitted 3 April 2023
Accepted 21 June 2023
Published 14 July 2023

Copyright © 2023 Zhengwen Cao et al. Exclusive licensee Science and Technology Review Publishing House. No claim to original U.S. Government Works. Distributed under a Creative Commons Attribution License 4.0 (CC BY 4.0).

With the progress of theoretical and applied technologies, the communication system based on the classical encryption is seriously threatened by quantum computing and distributed computing. A communication method that directly loads confidential information on the quantum state, quantum secure direct communication (QSDC), came into being for resisting security threats. Here, we report the first continuous-variable QSDC (CV-QSDC) experimental demonstration for verifying the feasibility and effectiveness of the CV-QSDC protocol based on Gaussian mapping and propose a parameter estimation for signal classification under the actual channels. In our experiment, we provided 4×10^2 blocks, where each block contains 10^5 data for direct information transmission. For the transmission distance of 5 km in our experiment, the excess noise is 0.0035 SNU, where SNU represents the unit of shot-noise units. The 4.08×10^5 bit per second experimental results firmly demonstrated the feasibility of CV-QSDC under the fiber channel. The proposed grading judgment method based on parameter estimation provides a practical and available message processing scheme for CV-QSDC in a practical fiber channel and lays the groundwork for the grading reconciliation.

Introduction

In an era of highly developed network technology, there are still some insecure factors in the transmission of confidential information. One-time pad is a mechanism of communication that theoretically guarantees the absolute security of encrypted information [1]. Its security is guaranteed by the security of the key. However, with the progress of theoretical and applied technologies, the communication system based on the classical encryption is seriously threatened by quantum computing and distributed computing [2–4].

In order to resist security threats that are caused by brute-force cracking of key by increasing computational complexity, a way of communication based on fundamental principles of quantum mechanics came into being. Different from quantum key distribution (QKD) [5–8], quantum secure direct communication (QSDC) is the true sense of secure communication, and its secret message is loaded on the quantum state and transmitted directly in the channel [9]. Quantum principles such as no-cloning theorem [10], Heisenberg's uncertainty principle [11], and the correlation of entangled particles [12] guarantee its security. Moreover, this mode retains the function of perceiving eavesdropping while making it impossible for Eve to eavesdrop any secret message, that is, to achieve the role of anti-eavesdropping. Therefore, the development of this technology is conducive to the conversion of classical communication to quantum communication.

Generally, discrete-variable (DV) scheme and continuous-variable (CV) scheme are 2 important technologies to realize quantum communication. Since the first DV protocol was proposed, DV-QSDC was well developed in recent years in both theory and experiment [13–18]. For instance, device-independent (DI) QSDC and measurement device-independent (MDI) QSDC protocols have been proposed [19–27]. Additionally, one-step QSDC protocols and their DI and MDI versions, which enable the transmission of photons in a single round, have also been introduced [28–30]. Focusing on the experimental demonstration, in the original scheme proposed by Long and colleagues [31,32], optical delay, a mature and experimentally feasible technique that can be used to replace quantum memory, makes full use of the 2-qubit in an Einstein-Podolsky-Rosen (EPR) pair to implement 2-step DV-QSDC experiments. On this basis, many experimental schemes have been further proposed. In 2016, Long and colleagues [33] reported the first experimental demonstration of DV-QSDC based on the DL04 protocol, and the feasibility was firmly demonstrated in the presence of noise and loss. Zhang et al. [34] first reported the experimental demonstration with atomic quantum memory for the first time in principle in 2017, demonstrating the potential application of long-distance quantum communication in quantum networks. In 2018, Sun et al. [35] proposed an implementation scheme without quantum memory, taking advantage of the wiretap channel theory and classical coding theory, and made great progress in the practical application of QSDC. In 2019, Long and colleagues [36] implemented a practical DV-QSDC system based on the DL04 protocol that operates at a repetition rate of 1 MHz under a realistic channel of 1.5 km with high noise and high loss characteristics. The secure communication rate achieves 50 bps, sufficient to effectively send text messages and reasonably sized files of images and sounds. In 2020, Sun et al. [37] proposed a quantum-memory-free DL04 QSDC protocol inches closer to the quantum channel's capacity and importantly

improved the original DL04 QSDC's robustness. Pan et al. [38], also in 2020, reported an experimental implementation of free-space DV-QSDC, which shows that QSDC is feasible in free space. In 2021, Liu et al. [39] designed a 2-decoy-state protocol that only requires 2 decoy states and performed full parameter optimization for a real-life QSDC system by introducing a genetic algorithm. In 2022, Liu et al. [40] presented a fiber-based QSDC system without active polarization compensation. Long and colleagues [41] successfully experimentally implemented DV-QSDC of over 100 km fiber with time-bin and phase quantum states also in 2022, demonstrating that intercity QSDC through fiber is feasible with present-day technology.

Compared with DV scheme, CV quantum communication can be well compatible with the existing optical fiber communication, which has been extensively studied recently. Moreover, its advantages of simple light source preparation, convenient detection, and low equipment cost are conducive to the construction of quantum communication network. Therefore, in order to accelerate the development of the entire QSDC field, it is necessary to explore CV-QSDC technology.

The principles of quantum mechanics impose an upper bound on the information in CV-QSDC that has possibly leaked to a potential eavesdropper, which is done by the legitimate parties through estimating the parameters of quantum channels [42–44]. In the preliminary development of QSDC, parameter estimation, a crucial aspect connecting quantum information processing stage and message extracting stage, has attracted the attention of many researchers. In addition, parameter estimation can also be combined with other methods that suppress excess noise, such as adaptive optics [45], to improve system performance. However, numerous schemes that have been proposed so far are only for CVQKD [46–51]. Different from QKD, QSDC that directly transmits information has more elaborate requirements for parameter estimation, where the complete extraction of subsequent information cannot be effectively guaranteed by those existing schemes. Therefore, it is necessary to research on parameter estimation scheme suitable for system based on experiments.

In this context, we established an experimental CV-QSDC platform based on Gaussian mapping scheme [52] and experimentally demonstrated it. We introduced a new parameter estimation scheme under the actual channels with complexity and fluctuation. Specifically, the main contributions of this work are as follows: (a) We reported the first CV-QSDC experimental demonstration for verifying the feasibility and effectiveness of the protocol based on Gaussian mapping. Experimental results show that the proposed scheme successfully implements under the actual channel that is complex and volatile. (b) We performed the parameter estimation that came closer to the actual situation through the experimental demonstration and simulated the influence of whether the channel fluctuation is taken into account on the transmission distance. The results obtained from parameter estimation also more realistically and accurately reflect the fluctuation and instability of the actual channel, which may have a great impact on the efficiency of subsequent message extraction. Moreover, it can be obtained experimentally that the system performance can be improved if the channel fluctuation characteristics are taken into account. (c) We proposed a scheme for quality classification of information blocks based on parameter estimation results, which further optimizes the process of sequential postprocessing to improve the security and integrity of message. Furthermore, this scheme facilitates the extraction of secret messages from continuous variables and lays the technical foundation for the complete construction of the system and future engineering applications.

Results

System implementation

The experimental setup for the proposed CV-QSDC system is shown in Fig. 1. The necessary conditions for CV-QSDC experiment include the coherent light sources (CW) for generating entangled light, the modulators (AM2 and PM) for information modulation, the homodyne detectors (Hom3 and Hom4) for Bell detection, and pilot signal for synchronization. Utilization of polarization multiplexing and time-division multiplexing ensures the transmission of local oscillator light, detection light, and signal light without mutual interference. Concretely, to verify the feasibility of the proposed CV-QSDC protocol based on Gaussian mapping scheme, coherent light source CW for generating coherent light, nondegenerate optical parametric amplifier NOPA, and amplitude modulator AM1 are used in experiments to generate entangled light pulses at a repetition rate of 10 MHz, where the resulting signal light is retained at Alice for information modulation and the detection light is sent to Bob for channel secure detection. The beam splitter BS3 and homodyne detector Hom1 at Alice's end and BS6 and Hom2 at Bob's end are adopted for channel secure detection. Meanwhile, signal light passes through the fiber delay line DL2 and then completes the modulation of the secret message under the joint action of the amplitude modulator AM2 and the phase modulator PM, and then passes through the polarization beam splitter PBS1 and fiber channel to Bob.

The entire communication process consists of 2 steps. The security detection is conducted first, and information transmission occurs only under the premise of the security of channel. As shown in Fig. 2, the local oscillator, the detection light, and the signal light are transmitted using polarization multiplexing and time-division multiplexing techniques through Faraday mirror and fiber delay lines. Specifically, during the secure detection phase, Alice and Bob perform measurements on their respective entangled light beams in the selected corresponding time slots. So, here, taking fiber delay line into account,

$$\Delta t = \frac{n\Delta L}{c}, \tag{1}$$

where ΔL is the length of fiber delay line, n is the refractive index of optical fiber, and c is the speed of light in vacuum [53]. Due to the repetition frequency of 10 MHz, the interval between identical pulses is 100 ns. Therefore, the 30-ns fiber delay is used in the experiment (shown in Fig. 2).

When Bob receives the modulated signal light, depolarization demultiplexing and time-division demultiplexing are performed to separate the detection light and the signal light for performing Bell measurements (employing BS8, Hom3, and Hom4). The quantum memory is not required in this experimental platform, mainly because the CV-QSDC protocol based on Gaussian mapping is actually a secure coding protocol based on Wyner's wiretap channel theory. The plaintext to be transmitted is mapped into ciphertext in groups using shared Gaussian random sequence, and generated ciphertext is then transmitted through a quantum channel using error correction codes and detection codes.

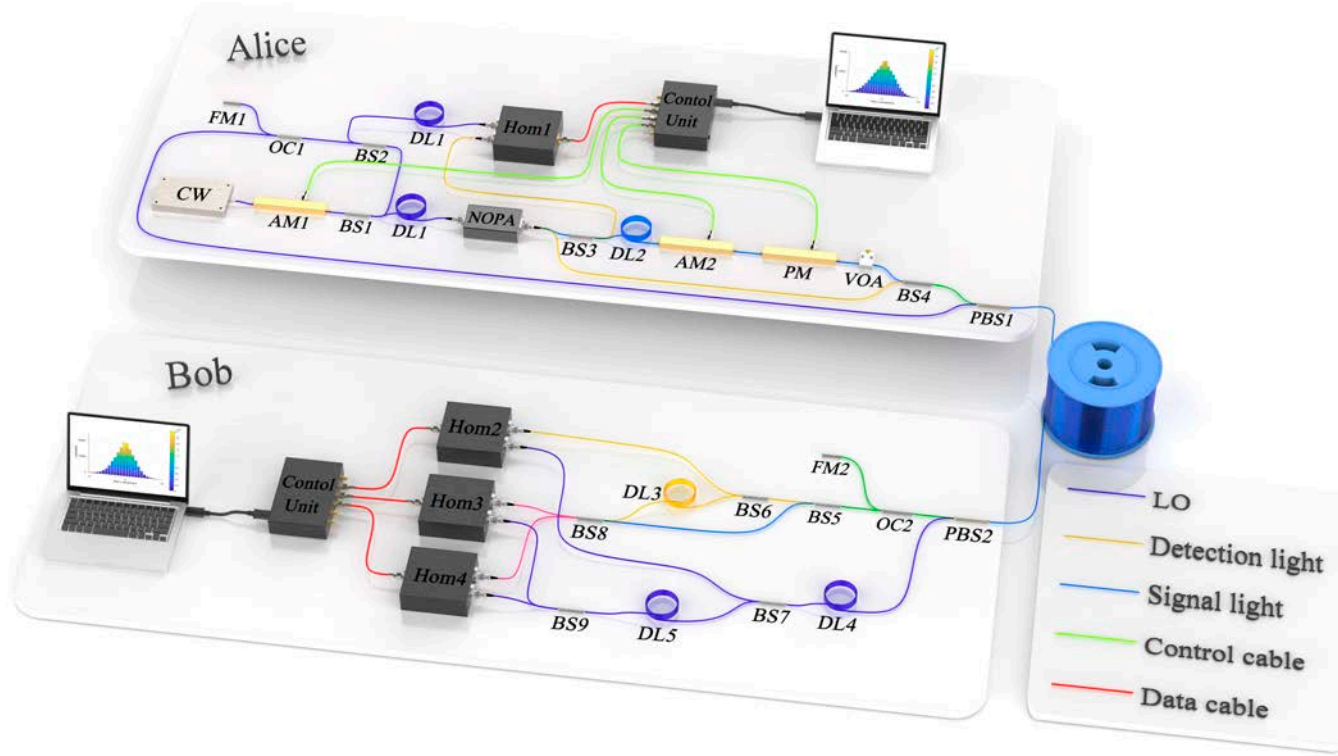


Fig. 1. Experiment setup. CW, 1550-nm continuous-wave light source; NOPA, nondegenerate optical parametric amplifier; BS, beam splitter; OC, optical circulator; DL, fiber delay line; AM, amplitude modulator; PM, phase modulator; VOA, variable optical attenuator; Hom, homodyne detector with over 50% detection efficiency; PBS, polarization beam splitter; FM, faraday mirror.

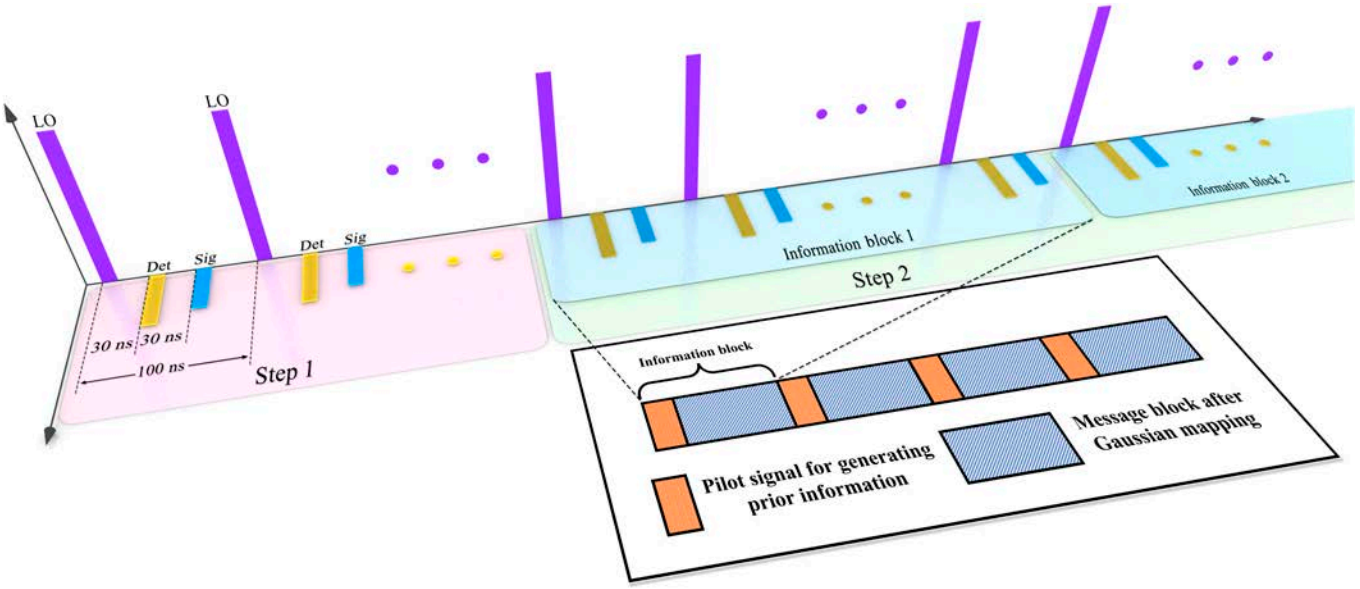


Fig. 2. Schematic diagram of signal transmission during communication. Step 1 represents the security detection phase, while step 2 represents the information transmission phase. Specifically, polarization multiplexing and time-division multiplexing are employed to differentiate the local oscillator (LO), detection light (Det), and signal light (Sig), and the time interval for time-division multiplexing is set to 30 ns. During the information transmission phase, each information block consists of pilot signal and secret message. The pilot signal consists of quantum light [54] and undergoes the same channel as the transmitted signal light. Therefore, the a priori information obtained from these pilot signals and the X component can be used for synchronization and calculating the secrecy capacity.

The complete CV-QSDC system functions mainly include the entanglement judgment function during the first safety inspection and the information transfer function based on entangled state. The experimental results verified the correlation of data in the CV-QSDC protocol based on Gaussian mapping under 5-km channel and effectiveness of the parameter estimation. The rendering of partial variables acquired from the quadrature component X obtained experimentally is shown in

Fig. 3. In particular, correlation of variables between Alice and Bob is shown in Fig. 3A. The experimental results prove that most of the variable points are linear correlation, which verifies the feasibility of the implementation for the proposed scheme. The statistical characteristics of Alice and Bob variables are shown in Fig. 3B. The experimental results show that the variables at both ends are in line with the Gaussian distribution, indicating that the experimental variables can meet the necessary conditions for carrying out subsequent steps. Therefore, the above experiment shows the rationality of variable acquisition and provides data support for the message extracting stage.

Parameter estimation scheme

The secret message on the basis of obtaining quadrature components is extracted by Alice and Bob during the message extracting stage. The processing operations mainly include the following 3 stages: parameter estimation, data reconciliation, and message extraction. Among them, parameter estimation plays a critical role in connecting the quantum information processing and message extracting in the CV quantum communication system. The results of parameter estimation can provide a reference for achieving the consistency of the data of both parties. Most studies in the past have assumed that the relevant parameters are theoretically invariant when analyzing the system performance [42,55–58], but this assumption is not in line with the actual situation. Next, a appropriate parameter estimation scheme is described.

In the CV-QSDC system, the message is transmitted in chunks rather than in whole. For each information block, secrecy capacity ΔI_i of the i-th information block is calculated based on the estimated value of the parameters. After the measure by Bob, Alice and Bob possess 2 sets of related variables, namely, $X = \left\{\left(x_i^{\mathrm{A}}, x_i^{\mathrm{B}}\right)\right\}_{i=1,2,\ldots,M}$ and $P = \left\{\left(p_i^{\mathrm{A}}, p_i^{\mathrm{B}}\right)\right\}_{i=1,2,\ldots,M}$ (superscripts A and B represent the variables obtained by Alice and Bob, respectively, subscript *i represents the i-th information block, M* represents the total number of information block). One set of variables carries secret message, and the other set of variables carries Gaussian random numbers without secret message, which is the set of data samples of parameter estimation. It is assumed here that the secret message is modulated on the P component, while the X component is used for parameter estimation. Generally speaking, all the blocks on the X component are employed to estimate the relevant channel parameters. Among them, the transmittance T and excess noise ε of quantum channel can be used to describe the influence of the transmission on the quantum signal [59].

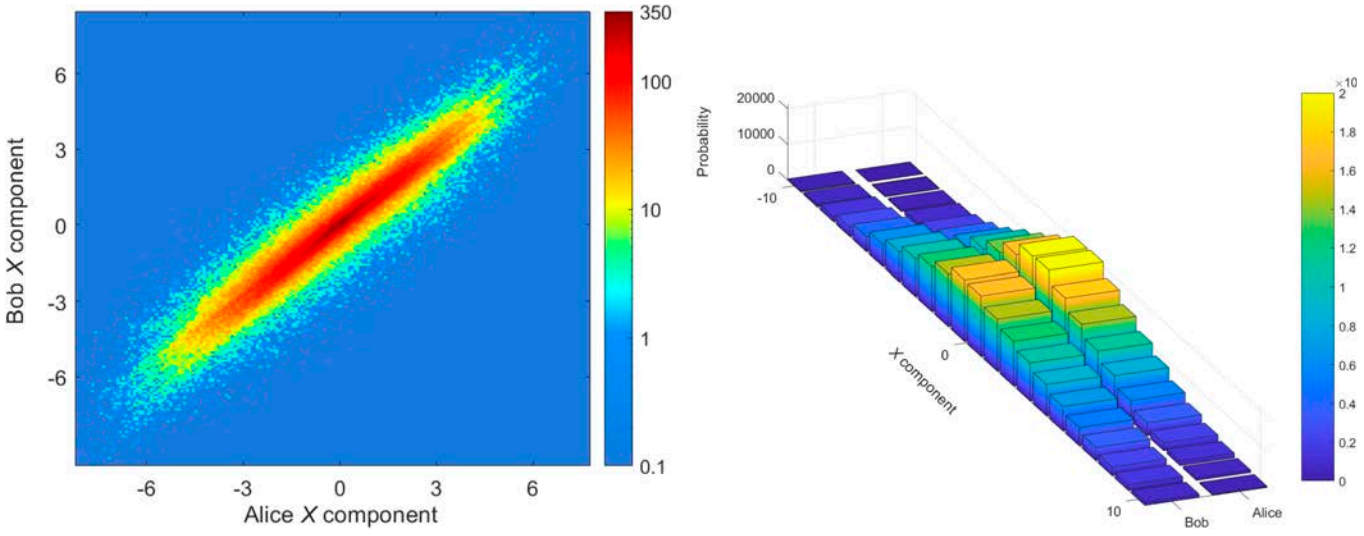
The quantum channel is described through linear models [60] in actual phenomenon. So, here, taking the correlation of variables of the i-th information block between Alice and Bob into account,

$$x_i^{\mathrm{B}} = x_i^{\mathrm{A}} t_i + z_i, \tag{2}$$

where $t_i = \sqrt{\eta T_i}$, and z_i is Gaussian noise with variance $\sigma_i^2 = \eta T_i \varepsilon_i + N_{0i} + v_{el}$ and mean zero, and N_{0i} is the shot noise. T_i and ε_i are the transmittance and excess noise of the i-th information block, respectively. Detecting efficiency η and the electrical noise v_{el} induced by the detector can be obtained by precalibration. The variance and quantum communication system parameters meet the following relationships:

$$\begin{aligned} \langle x_i^{\mathrm{A}^2} \rangle &= V_{\mathrm{A}}, \quad \langle x_i^{\mathrm{A}} x_i^{\mathrm{B}} \rangle = \sqrt{\eta T_i} V_{\mathrm{A}}, \\ \langle x_i^{\mathrm{B}^2} \rangle &= \eta T_i V_{\mathrm{A}} + N_{0i} + \eta T_i \varepsilon_i + v_{el}, \end{aligned} \tag{3}$$

where T_i, V_A, N_{0i}, ε_i, and v_{el} all expressed in their respective units rather than in shot noise units. Since detecting efficiency η and electrical noise v_{el} are calibrated in advance, Bob can obtain $\left\{{}_j x_0^{\mathrm{B}}\right\}_{j=1,2,\ldots,N'}$ (N' represents the total number of quantum signals required to transmit an information block over quantum channel) by forcing a quantum channel not to transmit



A Correlation **B** Alice's and Bob's variables

Fig. 3. Experimental data renderings. (A) Correlation between Alice and Bob variables. The solid red line indicates that the data satisfy the linear relationship of $y = tx + z$. (B) Statistical properties of the X component of Alice and Bob. The horizontal axis represents the variables, while the vertical axis represents the frequency.

any signals. So the set of Bob's variables $\left\{ {}_j x_0^{\mathrm{B}} \right\}_{j=1,2,\ldots,N'}$ can be employed to calibrate the noise of the i-th information block,

$$\left\langle \left({}_j x_{0i}^{\mathrm{B}} \right)^2 \right\rangle = N_{0i} + v_{el}. \tag{4}$$

So the maximum likelihood estimate for the corresponding parameters based on Eq. 2 and the variables possessed by both communication parties can be obtained:

$$\begin{aligned} \hat{\sigma}_{0i}^2 &= \frac{1}{N'} \sum_{j=1}^{N'} \left({}_j x_{0i}^{\mathrm{B}} \right)^2, \quad \hat{V}_{\mathrm{A}} = \frac{1}{N} \sum_{j=1}^{N} \left({}_j x_{0i}^{\mathrm{A}} \right)^2, \\ \hat{t}_i &= \frac{\sum_{j=1}^{N} {}_j x_i^{\mathrm{A}} {}_j x_i^{\mathrm{B}}}{\sum_{j=1}^{N} \left({}_j x_i^{\mathrm{A}} \right)^2}, \quad \hat{\sigma}_i^2 = \frac{1}{N} \sum_{j=1}^{N} \left({}_j x_i^{\mathrm{B}} - {}_j x_i^{\mathrm{A}} \hat{t} \right)^2, \end{aligned} \tag{5}$$

where N represents the total number of quantum signals required to transmit in each information block, $\hat{\sigma}_0^2$, $\hat{V}_{\mathrm{A}}$, $\hat{t}_i$, and $\hat{\sigma}_i{}^2$ are independent estimates of each other and are subordinated to the following distributions:

$$\begin{aligned} \hat{t}_i &\sim \mathrm{N}\left(t_i, \frac{\sigma_i^2}{\sum_{j=1}^{N} \left({}_j x_i^{\mathrm{A}} \right)^2} \right), \\ \frac{N\hat{\sigma}_i^2}{\sigma_i^2}, \frac{N'\hat{\sigma}_{0i}^2}{\sigma_{0i}^2}, \frac{N\hat{V}_{\mathrm{A}}}{V_{\mathrm{A}}} &\sim \chi^2(N-1), \end{aligned} \tag{6}$$

where σ_0^2, V_{A}, t_i, and σ_i^2 are the truth values of the corresponding parameters [42,61]. The estimation following the χ^2 distribution can be approximated by the Gaussian distribution when the sample size is sufficient, and the corresponding confidence interval can be expressed as:

$$\begin{aligned} t_i &\in \left[\hat{t}_i - \Delta t_i, \hat{t}_i + \Delta t_i \right], \\ \sigma_i^2 &\in \left[\hat{\sigma}_i^2, -\Delta\sigma_i^2, \hat{\sigma}_i^2 + \Delta\sigma_i^2 \right], \\ \mathrm{V_A} &\in \left[\hat{\mathrm{V}}_{\mathrm{A}} - \Delta \mathrm{V_A}, \hat{\mathrm{V}}_{\mathrm{A}} + \Delta \mathrm{V_A} \right], \\ \sigma_0^2 &\in \left[\hat{\sigma}_0^2, -\Delta\sigma_0^2, \hat{\sigma}_0^2 + \Delta\sigma_0^2 \right], \end{aligned} \tag{7}$$

where Δt_i, $\Delta\sigma_i^2$, ΔV_{A}, and $\Delta\sigma_0^2$ are given by

$$\begin{aligned} \Delta t_i &= z_{\varepsilon_{\mathrm{PE}}/2} \sqrt{\frac{\hat{\sigma}_i^2}{N V_{\mathrm{A}}}}, \quad \Delta\sigma_i^2 = z_{\varepsilon_{\mathrm{PE}}/2} \frac{\hat{\sigma}_i^2 \sqrt{2}}{\sqrt{N}}, \\ \Delta V_{\mathrm{A}} &= z_{\varepsilon_{\mathrm{PE}}/2} \frac{\hat{V}_{\mathrm{A}}^2 \sqrt{2}}{\sqrt{N}}, \quad \Delta\sigma_0^2 = z_{\varepsilon_{\mathrm{PE}}/2} \frac{\hat{\sigma}_0^2 \sqrt{2}}{\sqrt{N'}}. \end{aligned} \tag{8}$$

In addition, $z_{\varepsilon \mathrm{PE}/2}$ satisfies the equations:

$$\begin{cases} 1 - \mathrm{erf}\left(\dfrac{Z_{\varepsilon_{\mathrm{PE}}/2}}{\sqrt{2}} \right) = \dfrac{\varepsilon_{\mathrm{PE}}}{2}, \\ \mathrm{erf}(x) = \dfrac{2}{\sqrt{\pi}} \displaystyle\int_0^x \exp\left(-\tau^2 \right) d\tau, \end{cases} \tag{9}$$

where $\varepsilon_{\mathrm{PE}}$ is the probability that the parameter estimate is outside the confidence interval calculated during the parameter estimation phase. Finally, the estimated values of parameters can be obtained:

$$\hat{T}_i = \frac{\hat{t}_i^2}{\eta}, \quad \hat{\varepsilon}_i = \frac{\hat{\sigma}_i^2 - \hat{\sigma}_{0i}^2}{\hat{t}_i^2}. \tag{10}$$

In the process of parameter estimation, the estimation of modulation variance $\hat{V}_{\mathrm{A}}$, transmittance $\hat{T}$, and excess noise $\hat{\varepsilon}$ has the most obvious effect on the calculation of the secrecy capacity. However, the modulation variance of an information block is a set fixed value, estimation of which is close to the original modulation variance. Therefore, the effect on the estimation of secrecy capacity is mainly determined by the transmittance and excess noise in the channel.

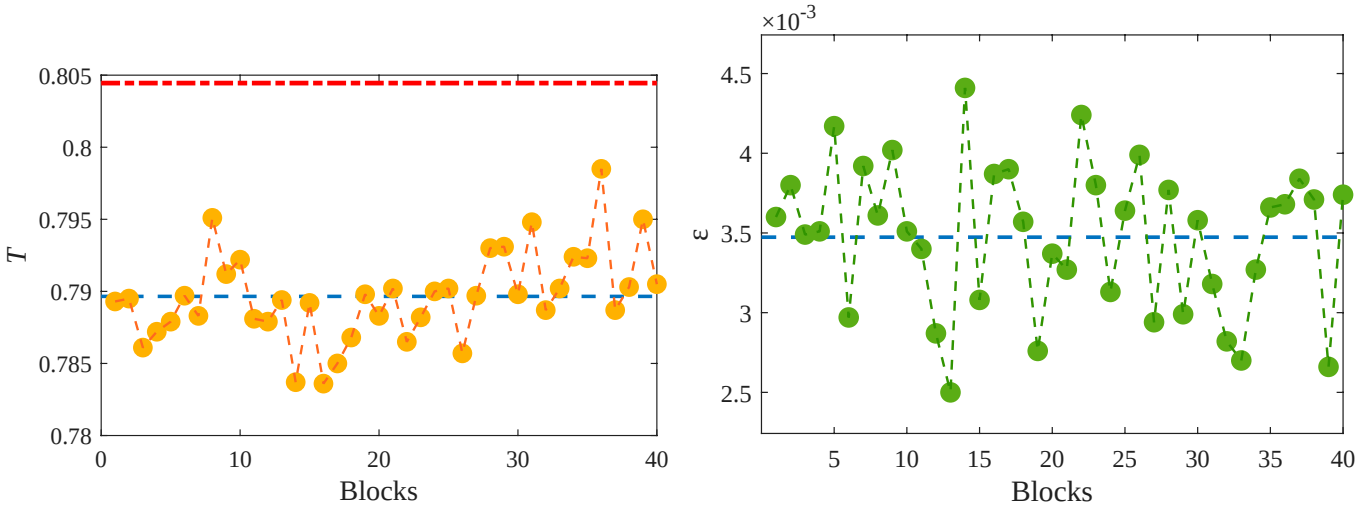
To perform the parameter estimation, the experiment sets the total information to 4×10^2 blocks, and each block contains 10^5 variables. The overview of experimental parameters and performance is shown in Table.

The result estimates of channel transmittance and excess noise are shown in Fig. 4. According to the distribution of small solid circles in Figs. 4A and B, the experimental results demonstrate the feasibility of the existing parameter estimation scheme in estimating the channel transmittance and excess noise, and lay the foundation for the design and implementation of subsequent grading scheme. In addition, the volatility nature of the data is obviously shown. Low-quality information blocks are more severely affected by channel interference and eavesdropping interference, making it more challenging to extract secure messages from them compared to high-quality information blocks. When using the same reconciliation scheme, the reconciliation efficiency of low-quality information blocks is lower than that of high-quality information blocks. Therefore, the grading processing based on different quality information blocks is highly necessary. By employing a more efficient reconciliation scheme for low-quality information blocks, the aim is to enhance their reconciliation efficiency and ultimately achieve high reconciliation efficiency for different quality information blocks.

The relationship between the transmission distance and the secrecy capacity under different conditions is shown in Fig. 5. The transmission performance of the result based on the

Table. Overview of experimental parameters and performance. *SNR*, signal-to-noise ratio; β, reconciliation efficiency; *FER*, frame error rate of the reconciliation; V_A, modulation variance; ξ, excess noise at the channel input; v_{el}, electronic noise; η, efficiency of the homodyne detector; P, error rate of information block; *SC*, secrecy capacity; bps, bit per second.

Parameter	*Length* (km)	*SNR* (dB)	β	*FER*	V_A (SNU)
Value	5	1.895	0.89	10^{-3}	7
Parameter	ξ (SNU)	v_{el} (SNU)	η (SNU)	P	*SC* (bps)
Value	0.0035	0.0042	0.6	10^{-5}	4.08×10^5



A estimates of channel transmittance T **B** estimates of excess noise ε

Fig. 4. (A and B) Parameter estimates of channel transmittance and excess noise. The small solid circles in subgraphs represent the result of estimation of 40 information blocks selected as observation objects. The blue dotted line represents the average of the parameter estimates of all information blocks. The volatility of the data is represented by the dotted lines connecting points to points. The red dotted line in (A) represents the theoretical upper bound of channel transmittance.The optical fiber model used in our experimental platform is G652D, with an actual attenuation coefficient α of approximately 0.19 dB/km. Therefore, the theoretically calculated upper limit of the channel transmittance is approximately 0.804.

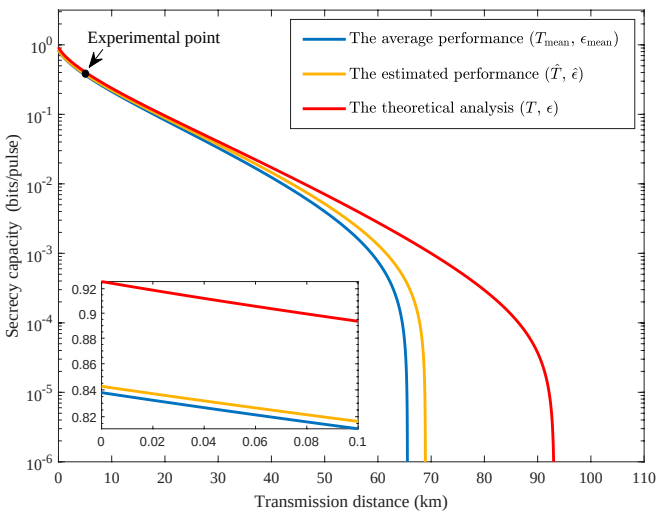


Fig. 5. The relationship between the transmission distance and the secrecy capacity, which is based on the calibrated parameters in Table 1 using a standard expression. From left to right: Average performance result of the system, performance of a system that takes into account channel volatility, and theoretical performance of the system.

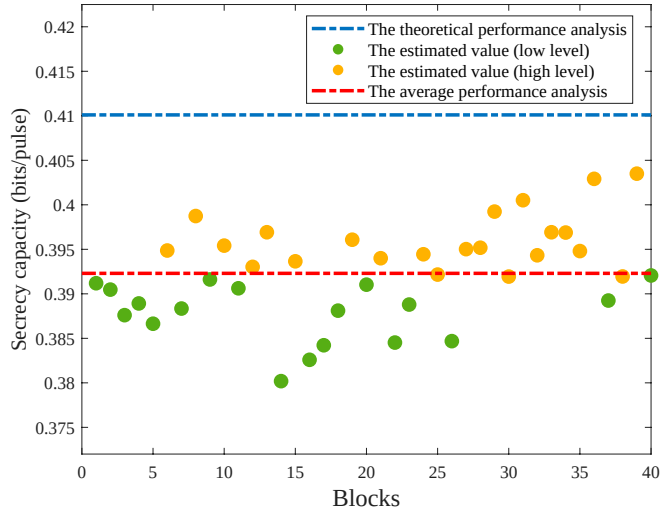


Fig. 6. The estimate of secrecy capacity. The data points represent 40 information blocks selected as grading objects. The blue dotted line indicates the secrecy capacity in theoretical case when the transmission length of the fiber channel is set to 5 km. The red dotted line indicates the average of secrecy capacity, which is obtained by calculating the secrecy capacity for multiple segments of pilot signals and then taking the mean. The information blocks that satisfy criterion 2 are represented by the yellow data point. The information blocks that do not meet criterion 2 are represented by the green data point.

parameter estimate under conditions that take channel volatility into account is represented by the second curve from left to right. For a transmission distance of 5 km in our experiment, the excess noise is 0.0035 SNU, where SNU represents the unit of shot-noise units. The secrecy capacity has reached 4.08×10^5 bit per second (bps), which demonstrates the effectiveness of the experimental platform. Obviously, compared to the average performance (the blue curve), the safe transmission distance is increased and the system performance is improved when parameter estimation under conditions that take volatility into account (the yellow curve).

Based on the above analysis, a grading processing operation explained in detail in the "Grading processing method based on parameter estimation" section is adopted to classify the quality of the information blocks, so as to perform the corresponding reconciliation strategies on the information blocks of different quality to improve the reconciliation efficiency of information blocks and speed up the extraction rate of secret message. The calculation results of grading all information blocks are shown in Fig. 6, which shows that the

experimental communication process is secure and explains that the proposed grading processing scheme is feasible and effective.

Discussion

In this work, an experimental platform is established for the Gaussian mapping-based CV-QSDC. The experiment completes the process of CV-QSDC on the platform basis well, and the experimental data from both parties have a strong correlation. According to Fig. 6, the curve fitted from the data suggests that the secrecy capacity of this system can reach 10 bps at 100 km. Compared to the currently achievable DV-QSDC experimental system with the longest communication distance in the world, this experimental system has a much higher communication rate than its rate of 0.54 bps at 100 km [41]. This comparison highlights the advantage of the established experimental platform in terms of communication rate. However, one limitation of the continuous-variable experimental system is the high signal loss and limited transmission distance in the channel, making it suitable only for short- to medium-distance communication. Therefore, the future development goal for continuous-variable experimental system is to enhance the communication distance as much as possible. The results of the experiment also show that the platform has the advantages of systematization, extensiveness, and comprehensiveness and has certain reference value and guidance significance to the study of parameter estimation and secret message grading processing part of CV-QSDC. With the help of the proposed parameter estimation scheme and the analysis of beam propagation in the fiber channel based on the established platform, the transmittance and the excess noise of system have been studied for in-depth analysis of the actual performance of the system. The experimental results show that the proposed parameter estimation scheme has effectiveness in estimating the channel transmittance and excess noise. The estimation of secrecy capacity and grading criteria of information in this protocol are also effective. Moreover, the experimental results show the rationality of data acquisition and provide data support for the message extracting stage.

Consequently, the experimental result based on this experimental platform coincides with the relevance characteristics of the message before and after the transmission for CV-QSDC, which proves the availability and rationality of this platform and provides a feasible method for experiment of CV-QSDC. Furthermore, by incorporating coding processes, employing transmission, and receiving antennas at the communication endpoints, this system has the potential for future development in CV-QSDC communication in free space. Moreover, the experimental result based on the parameter estimation including grading judgment provides a practical and available post-processing method for CV-QSDC in a practical fiber channel. Finally, based on the analysis mentioned above, the established platform can acquire data appropriately and efficiently provide data support for the message extracting stage. The proposed parameter estimation method can effectively improve the grading processing performance and lay the groundwork for the grading processing reconciliation scheme. All in all, future work will therefore focus on solving the problem of adaptation between information grading reconciliation schemes and different transmission quality information blocks under actual experimental systems.

Materials and Methods

The CV-QSDC protocol based on Gaussian mapping

The CV-QSDC protocol based on Gaussian mapping, employing Gaussian source and Gaussian modulation, is proposed to solve the offset problem present in existing CV-QSDC protocol [62]. Specifically, the Gaussian random number sequence, directly encoded by the transmitted secret message, has non-uniform characteristics, which lead to the difference of the mean in the subsequent modulation process. The instability of the mean affects the modulation variance, which is crucial to the quantum communication process. This further impacts the message extraction, resulting in the compromise of the actual security of the system. Through Gaussian mapping, the information in each block is uniformized, which ensures the stability of Gaussian modulation under different variance conditions and facilitates the secure message transmission.

- **Protocol structure**

1. **Preparation**: Optical parameter oscillator is employed to compress the quadrature position (x) or quadrature momentum (p) of the vacuum state in phase space to generate 2 squeezed vacuum light (beam 1 and beam 2). The quadrature position and quadrature momentum corresponding to the squeezed vacuum states can be expressed as:

$$\begin{cases} x_1 = \exp(-r)\,|0\rangle_{x_1}, \\ p_1 = \exp(r)\,|0\rangle_{p_1}, \end{cases} \tag{11}$$

and

$$\begin{cases} x_2 = \exp(-r)\,|0\rangle_{x_2}, \\ p_2 = \exp(r)\,|0\rangle_{p_2}. \end{cases} \tag{12}$$

where $r\ (>0)$ is the compression coefficient, and the vacuum state $|0\rangle$ with the subscript, as the input state, denotes the corresponding quadrature position and quadrature momentum. Then, the 2-mode squeezed states S_1 (signal light) and S_2 (detection light) are generated by these 2 squeezed vacuum states through a 50:50 beam splitter and can be described separately as:

$$\begin{cases} X_1 = \frac{1}{\sqrt{2}}(x_1 + x_2), \\ P_1 = \frac{1}{\sqrt{2}}(p_1 + p_2). \end{cases} \tag{13}$$

and

$$\begin{cases} X_2 = \frac{1}{\sqrt{2}}(x_2 - x_1), \\ P_2 = \frac{1}{\sqrt{2}}(p_2 - p_1). \end{cases} \tag{14}$$

Then, $\boldsymbol{S^1}$, employed as a modulated optical carrier and security detection, is retained by Alice, while $\boldsymbol{S^2}$, employed as a reference for joint measurements and security detection, is sent to Bob.

2. **Security detection**: Alice randomly selects a set of time slots to measure the quadrature components X or P of S_1 and then she publishes the time slots and the measurements. Bob chooses the same time slots as Alice to measure the corresponding components. Then, the inseparability criterion is relied by Bob to combine the measurements and Alice's measurements for entanglement judgments, which can be described as follows:

$$\left\langle (\Delta X_m)^2 \right\rangle + \left\langle (\Delta P_m)^2 \right\rangle < 2, \tag{15}$$

where X_m and P_m represent the measurement results of the corresponding component. The "2" means the sum of the EPR noise that can be observed when each EPR pair is detected separately. If the inseparability criterion is met for the measurement results for all the selected time slot, the information for the location of the time slot is secure. Moreover, the security of the channel is guaranteed when the combined error rate of the measurement results for all selected time slots is below the threshold. Then, the next steps continue; otherwise, the communication is terminated.

3. **Authentication**: Bob publishes measurement results corresponding to the time slot to verify that both parties are legitimate communicating parties for choosing whether to proceed with the next steps, since the classical channel can only be used by legitimate communicators to publish information.
4. **Gaussian mapping**: First, the secret message sequence is divided into multiple information blocks by Alice. Second, the probability of 0 and 1 occurring in each information block is unified using a code conversion method to maintain a mean of 0 for the sequences, thereby reducing the effect on modulation variance. Specifically, 0 in the information block is represented alternately by {01, 10} , while 1 is alternately represented by 00, 11. Third, the information blocks are further divided, and each dividing block is uniformized by randomly replacing all bits with 2-bit code element. Specifically, one of {00, 01} is randomly selected to represent 0, and one of {10, 11} is randomly selected to represent 1. Following that, detection bits are inserted in random positions within each information block. Then, an error correction code is inserted in a fixed position of each information block. Afterward, a Gaussian random sequence G_1 with mean zero and variance V_A is divided into multiple intervals according to the equiprobable rule, where the number of intervals is determined by the number of bits in each information block. Finally, information blocks are mapped to arbitrary Gaussian random numbers that belong to corresponding intervals, resulting in a mapped Gaussian random sequence $\boldsymbol{G^1}'(\subseteq G_1)$.
5. **Gaussian modulation**: The sequence G_1' is adopted to modulate the quadrature position X of S_1, while another Gaussian random sequence $G_2(\neq \boldsymbol{G^1}')$ is adopted to modulate the quadrature momentum P of S_1. After modulation, S_1 evolves into $\boldsymbol{S^{info}}$, which is then transmitted through quantum channel to Bob. The similar modulation scheme [63] is actually based on the one-time pad, in which the X component is regarded as the message needed to be transmitted to Bob, while P acts as the private key shared between Alice and Bob. Compare to it, in the proposed scheme, one component is used for direct information transmission without encryption, while the other component is solely utilized for parameter estimation.
6. **Measurement**: Joint detection is performed by Bob on detection light S_2'(after channel transmission) and signal light S_{info}' for obtaining the corresponding quadrature components, which can be expressed as:

$$\begin{cases} X_m = \dfrac{1}{\sqrt{2}}\left(X'_{\text{info}} - X'_2\right), \\ P_m = \dfrac{1}{\sqrt{2}}\left(P'_{\text{info}} - P'_2\right). \end{cases} \tag{16}$$

7. **Postprocessing**: The secret message on the basis of obtaining quadrature components is extracted by Alice and Bob through parameter estimation, reverse reconciliation, and message extraction.

Grading processing method based on parameter estimation

In this section, we introduce the grading processing scheme based on parameter estimation proposed in response to channel fluctuations. Secure message is less difficult to extract from the high-quality information blocks than from the low-quality one, and the high-quality one experiences a better channel environment with less interference. Existing reconciliation strategies can be used effectively to reconciliate for high-quality information blocks, and guarantee low grading process costs and low error rates. On the contrary, the low-quality information blocks suffered by the channel interference and eavesdropping interference more seriously, which means that using the universal reconciliation schemes for processing different quality information blocks requires a great cost and a lot of error correction information to enhance the reconciliation efficiency of low-quality information blocks and to ensure the security of message extraction. Therefore, for the information blocks marked as high quality or low quality, choosing a matching reconciliation strategy is beneficial to improve the reconciliation efficiency of information blocks and speed up the extraction rate of secret message.

•Scheme structure

Figure 7 details the CV-QSDC parameter estimation scheme, which mainly includes secure judgment and grading processing process. The basic steps of the scheme are as follows:

Step 1: Bell-state measurement: Bob employs Bell-state measurement to measure the information blocks from Alice for obtaining 2 sets of variables modulated onto the X and P components.

Step 2: Parameter estimation: The set of variables X that do not carry secret message is selected as the sample of parameter estimation, and 2 judgment criteria are set as grading criteria based on the results of parameter estimation.

Step 3: Security detection: Since the fiber channel is relatively stable, the estimation of secrecy capacity of i-th information blocks $\Delta\hat{I}_i$ should fluctuate within a relatively narrow band, and there must exist eavesdropping behavior if this estimate is not normal or below zero. Therefore, a relevant criterion is employed for eavesdropping detection.

Step 4: Quality judgment: The mean of secrecy capacity $\Delta\bar{I}_i$ can be used as a measure of signal classification and provides a reliable basis for different reconciliation strategies in the grading processing phase. Therefore, the first criterion is employed to judge the safety of information blocks, and the other criterion is employed to judge the quality of information blocks on the basis of the previous criterion.

•Criteria for quality judgment

Generally, the secrecy capacity ΔI between Alice and Bob is given by [64]

$$\Delta I = (1-FER)(1-P)\left(\beta I_{AB} - \chi_{BE}\right), \tag{17}$$

where β is the efficiency of grading reconciliation algorithm, I_{AB} is the mutual information between Alice and Bob, χ_{BE} is the Holevo bound between Eve and Bob, and P is the error rate of information block. *FER* is the frame error rate of the reconciliation, which can be used to evaluate the reliability and efficiency of the reconciliation scheme. The estimation of secrecy capacity $\Delta\hat{I}_i = \left\{\Delta\hat{I}_1, \Delta\hat{I}_2, \ldots, \Delta\hat{I}_M\right\}$ of the i-th information block ($i \in \{1,2,\ldots,M\}$) can be calculated through the estimation of channel transmittance $\hat{T}_i = \left\{\hat{T}_1, \hat{T}_2, \ldots, \hat{T}_i\right\}$ and excess noise $\hat{\varepsilon}_i = \left\{\hat{\varepsilon}_1, \hat{\varepsilon}_2, \ldots, \hat{\varepsilon}_i\right\}$ from Eqs. 5 to 10.

The parameters involved in the grading criterion calculation process are all obtained based on the X component of information block and the pilot signals that are designed with reference to the synchronization frame [54]. The pilot signals consist of quantum light undergoing the same channel as the transmitted signal light. Therefore, the prior information such as reconciliation efficiency obtained from these pilot signals and the X component can be used for synchronization and also for calculating the average secrecy capacity of the blocks and grading the information blocks. After grading the information blocks, the P component of information blocks undergoes different reconciliation processes according to the grading results.

Criterion 1: Determines the security of i-th information block based on whether the secrecy capacity $\Delta\hat{I}_i$ is greater than zero or not,

$$\begin{cases} \Delta\hat{I}_i > 0, & \text{safe block,} \\ \Delta\hat{I}_i \le 0, & \text{unsafe block.} \end{cases} \tag{18}$$

Criterion 2: In the i-th information block, $\Delta\hat{I}_i$ is employed as a basis for judging transmission performance. By comparing it with the average of the previous secrecy capacity $\Delta\bar{I} = \frac{1}{i}\sum_{k=1}^{i}\Delta\hat{I}_k$, the quality of the current information block in broad terms can be divided into high level and low level

$$\begin{cases} \Delta\hat{I}_i \ge \Delta\bar{I}, & \text{high level,} \\ \Delta\bar{I} > \Delta\hat{I}_i, & \text{low level.} \end{cases} \tag{19}$$

In the 2 criteria mentioned above, the secrecy capacity is compared with zero in criterion 1, which is the criterion for appraising whether the information block is interfered by eavesdropping during transmission. The security capacity is compared with the mean value of the security capacity $\Delta\bar{I}$. in criterion 2, which is used to evaluate whether the information block is of low or high quality. The mean value of the secrecy capacity is actually obtained by calculating the secrecy capacity for X component of multiple blocks and then obtaining the $\Delta\bar{I}$.

Under the combined effect of the 2 criteria, the information blocks are divided into 3 types: SIB1, SIB2, and USIB. Both SIB1 and SIB2 meet both 2 criteria. The former is classified as high-level information blocks, while the latter is classified as low-level information blocks. However, the unsafe information blocks that do not meet criterion 1 are represented by USIB and do not perform subsequent information processing.

Based on the above grading criteria, the grading process is designed as follows: After receiving the i-th information block from Alice, Bob first calculates the estimate of the relevant parameter by Eqs. 5 to 10 for obtaining the secrecy capacity $\Delta\hat{I}_i$ of i-th information block ($i \in \{1,2,\ldots,M\}$) by Eq. 17. Then, the secrecy capacity $\Delta\hat{I}_i$ is employed for determining the security

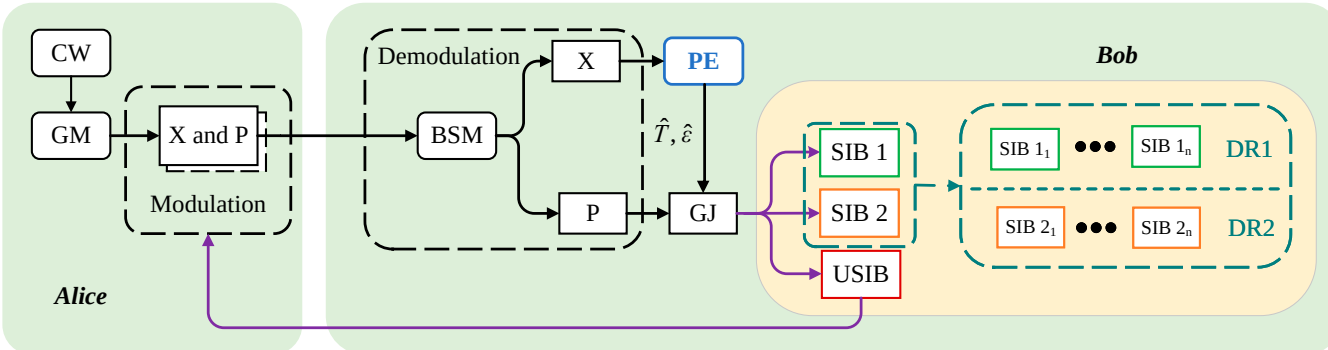


Fig. 7. CV-QSDC parameter estimation scheme. GM, Gaussian modulation; GJ, grading judgement; BSM, Bell-state measurement; SIB1, high-level information blocks; SIB2, low-level information blocks; USIB, unsafe information block; PE, parameter estimation; DR, different reconciliation schemes applying to different quality information blocks.

of the block according to criterion 1. If it is judged to be unsafe, it would be retransmitted until it is judged to be safe. But if it is judged to be secure, Bob would further determine the quality of the information block according to criterion 2. According to the judgment result, the information block is classified as a high-level block or a low-level block, and then we proceed to the next information block. As shown in Fig. 7, DR1 represents a reconciliation scheme applied to high-level information, while DR2 represents a reconciliation scheme applied to low-level information. Since the reconciliation performance is affected by the transmission environment such as the signal-to-noise ratio. According to the classification of transmission quality in this scheme, different reconciliation strategies can be designed for the information blocks of different transmission quality to improve the grading processing performance and lay the groundwork for the grading processing reconciliation scheme. It conduces to maintain the invariant and efficient reconciliation efficiency under fluctuating channel and facilitates the subsequent complete message extraction.

•**Validation**

The calculation result of the estimated secrecy capacity may effectively reflect the transmission quality of the information blocks. Estimates of secrecy capacity for all information blocks are shown in Fig. 6. According to the criteria for quality judgment, criterion 1 for determining the security of an information block is whether the secrecy capacity is greater than zero, while criterion 2 for grading the information block as high level or low level is whether the secrecy capacity is greater than the average secrecy capacity. The experimental results show that all information blocks meet criterion 1, that is, security message in each information block exists, indicating that the communication process is secure. Most of the yellow data points that are judged as high-level blocks according to criterion 2 are located above the green data points, which are judged as low-level blocks according to criterion 2, indicating that the information block is basically divided into 2 categories of high level and low level. Moreover, dividing the information blocks that the secrecy capacity is around the average into data blocks with high or low level has little impact on subsequent data reconciliation, so the impact of grading processing for them can be ignored. These results demonstrate the security of the experimental communication process and the feasibility and effectiveness of the grading processing scheme.

Based on the above analysis, the feasibility of the grading processing scheme based on secrecy capacity is explained. Moreover, according to the analysis in the "Parameter estimation scheme" section, the secrecy capacity in information blocks is determined by the channel transmittance and excess noise. The estimation of the channel transmittance and excess noise is shown to be effective in Fig. 4. Therefore, the estimation of secrecy capacity and the grading criteria of information in this protocol are also effective. The transmission length of the fiber channel is set to 5 km in the experimental scheme. Therefore, the theoretical value of the secrecy capacity of the information block can be calculated by Eq. 17 and represented by a blue dotted line in Fig. 6. Furthermore, all data points are below the blue dotted line, indicating that the optimization of the experimental system is constantly approaching the theoretical analysis. Moreover, the comparison of the performance impact of quality grading on information blocks is shown in Fig. 5 according to experiments and analysis. The performance of the system that does not implement grading is represented by blue lines, while the performance of the system that has implemented grading is represented by yellow lines, which indicates the improvement of classification on system performance.

Acknowledgments

Funding: This work is supported by the National Natural Science Foundation of China (62071381), Shaanxi Provincial Key R&D Program General Project (2022GY-023), Qinchuangyuan "Scientist + Engineer" Team Construction Project of Shaanxi Province of China (2022KXJ-009), and Young Talent Fund of Xi'an Association for Science and Technology (959202313011).
Author contributions: Y.L. and H.Y. set up the physical models, performed the experiment and coding, and analyzed the data. Z.C. and G.C. developed ideas for both implementing methods and which physics to study. K.L. and L.W. supervised all work. All authors contributed to deciding the experiment scheme and processing the data, as well as discussed the results and contributed to the manuscript. **Competing interests**: The authors declare that they have no competing interests.

Data Availability

Data sharing is not applicable to the article as no datasets were generated or analyzed during the current study.

References

1. Vernam GS. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *J AIEE*. 1926;45(2):109–115.
2. Knill E, Laflamme R, Milburn GJ. A scheme for efficient quantum computation with linear optics. *Nature*. 2001;409(6816):46–52.
3. Lloyd S. Ultimate physical limits to computation. *Nature*. 2000;406(6799):1047–1054.
4. Taddei MM, Escher BM, Davidovich L, de Matos, Filho. Quantum speed limit for physical processes. *Phys Rev Lett*. 2013;110(5):Article 050402.
5. Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. arXiv:2003.06557 2020.
6. Bennett CH, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Paper presented at: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing; 1984 Dec 10–12; Bangalore, India.
7. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. *Phys Rev Lett*. 2002;88(5):Article 057902.
8. Jin D, Guo Y, Wang Y, Huang D. Parameter estimation of orbital angular momentum based continuous-variable quantum key distribution. *J Appl Phys*. 2020;127(21):Article 213102.
9. Long G-L, Liu X-S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*. 2002;65(3):Article 032302.
10. Wootters WK, Zurek WH. A single quantum cannot be cloned. *Nature*. 1982;299(5886):802–803.
11. Robertson HP. The uncertainty principle. *Phys Rev*. 1929;34(11):163.
12. Hardy L. Nonlocality for two particles without inequalities for almost all entangled states. *Phys Rev Lett*. 1993;71(11):1665.

13. Li T, Long G-L. Quantum secure direct communication based on single-photon bell-state measurement. *New J Phys*. 2020;22(6):Article 063017.
14. Long G-L, Zhang H. Drastic increase of channel capacity in quantum secure direct communication using masking. *Sci Bull*. 2021;66(13):1267–1269.
15. Gao C-Y, Guo P-L, Ren B-C. Efficient quantum secure direct communication with complete bell-state measurement. *Quantum Eng*. 2021;3(4):Article e83.
16. Chen S-S, Zhou L, Zhong W, Sheng Y-B. Three-step three-party quantum secure direct communication. *Sci China Phys Mech Astron*. 2018;61:90312.
17. Yang L, JiaWei W, Lin ZS, Yin LG, Long GL. Quantum secure direct communication with entanglement source and single-photon measurement. *Sci China Phys Mech Astron*. 2020;63(11):Article 110311.
18. Pan D, Song X-T, Long G-L. Free-space quantum secure direct communication: Basics, progress, and outlook. *Adv Devices Instrum*. 2023;4:Article 0004.
19. Zhou L, Sheng Y-B, Long G-L. Device-independent quantum secure direct communication against collective attacks. *Sci Bull*. 2020;65(1):12–20.
20. Zhou L, Bao-Wen X, Zhong W, Sheng Y-B. Device-independent quantum secure direct communication with single-photon sources. *Phys Rev Appl*. 2023;19(1):Article 014036.
21. Zhou ZR, Sheng YB, Niu PH, Yin LG, Long GL, Hanzo L. Measurement-device-independent quantum secure direct communication. *Sci China Phys Mech Astron*. 2020;63(3): Article 230362.
22. Yan Y-F, Zhou L, Zhong W, Sheng Y-B. Measurement-device-independent quantum key distribution of multiple degrees of freedom of a single photon. *Front Phys*. 2021;16: Article 11501.
23. Zou Z-K, Zhou L, Zhong W, Sheng Y-B. Measurement-device–independent quantum secure direct communication of multiple degrees of freedom of a single photon. *Europhys Lett*. 2020;131(4):40005.
24. Liu L, Niu J-L, Fan C-R, Feng X-T, Wang C. High-dimensional measurement-device-independent quantum secure direct communication. *Quantum Inf Process*. 2020;19:404.
25. Hong Y-P, Zhou L, Zhong W, Sheng Y-B. Measurement-device-independent three-party quantum secure direct communication. *Quantum Inf Process*. 2023;22(2):111.
26. Park J, Kim B, Heo J. Statistical fluctuation analysis for decoy-state quantum secure direct communication. *Quantum Inf Process*. 2023;22(2):112.
27. Niu J, Liu X-C. The analysis of efficiency for high-dimensional quantum secure direct communications under atmospheric turbulence. *Europhys Lett*. 2022;139(3):38001.
28. Sheng Y-B, Zhou L, Long G-L. One-step quantum secure direct communication. *Sci Bull*. 2022;67(4):367–374.
29. Zhou L, Sheng Y-B. One-step device-independent quantum secure direct communication. *Sci China Phys Mech Astron*. 2022;65(5):Article 250311.
30. Ying J-W, Zhou L, Zhong W, Sheng Y-B. Measurement-device-independent one-step quantum secure direct communication. *Chin Phys B*. 2022;31(12):Article 120303.
31. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A*. 2003;68(4):Article 042317.
32. Deng FG, Long GL. Secure direct communication with a quantum one-time pad. *Phys Rev A*. 2004;69(5):Article 052319.
33. Jian Yong H, Bo Y, Jing MY, Xiao LT, Jia ST, Qin GQ, Long GL. Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* 2016;5(1):Article e16144.
34. Zhang W, Ding DS, Sheng YB, Zhou L, Shi BS, Guo GC. Quantum secure direct communication with quantum memory. *Phys Rev Lett*. 2017;118(22):Article 220501.
35. Sun Z, Qi R, Lin Z, Yin L, Lu J. Design and implementation of a practical quantum secure direct communication system. Paper presented at: 2018 IEEE Globecom Workshops (GC Wkshps); 2019 Dec 09–13; Abu Dhabi, United Arab Emirates.
36. Qi R, Zhen S, Lin Z, Niu P, Hao W, Song L, Huang Q, Gao J, Yin L, Long GL. Implementation and security analysis of practical quantum secure direct communication. *Light Sci Appl*. 2019;8(1):22.
37. Sun Z, Song L, Huang Q, Yin L, Long G, Jianhua L, Hanzo L. Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design. *IEEE Trans Commun*. 2020;68(9):5778–5792.
38. Pan D, Lin Z, Jiawei W, Zhang H, Sun Z, Ruan D, Yin L, Long GL. Experimental free-space quantum secure direct communication and its security analysis. *Photonics Res*. 2020;8(9):1522–1531.
39. Liu X, Li Z, Luo D, Huang C, Ma D, Geng M, Wang J, Zhang Z, Wei K. Practical decoy-state quantum secure direct communication. *Sci China Phys Mech Astron*. 2021;64(12):Article 120311.
40. Liu X, Luo D, Lin G, Chen Z, Huang C, Li S, Zhang C, Zhang Z, Wei K. Fiber-based quantum secure direct communication without active polarization compensation. *Sci China Phys Mech Astron*. 2022;65(12):Article 120311.
41. Zhang H, Sun Z, Qi R, Yin L, Long GL, Lu J. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light Sci Appl*. 2022;11:83.
42. Jouguet P, Kunz-Jacques S, Diamanti E, Leverrier A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys Rev A*. 2012;86(3):Article 032309.
43. Guo Y, Xie C, Huang P, Li J, Zhang L, Huang D, Zeng G. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys Rev A*. 2018;97(5):Article 052326.
44. Lupo C, Ottaviani C, Papanastasiou P, Pirandola S. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. *Phys Rev Lett*. 2018;120(22):Article 220505.
45. Chai G, Huang P, Cao Z, Zeng G. Suppressing excess noise for atmospheric continuous-variable quantum key distribution via adaptive optics approach. *New J Phys*. 2020;22(10):Article 103009.
46. Chai G, Li D, Cao Z, Zhang M, Huang P, Zeng G. Blind channel estimation for continuous-variable quantum key distribution. *Quantum Eng*. 2020;2(2):Article e37.
47. Du H, Huang D. Multi-attack detection: General defense strategy based on neural networks for cv-qkd. *Photonics*. 2022;9(3):177.
48. Zhong H, Xiaodong W, Deng M, Huang D, Xiong S, Guo Y. Passive-state preparation for continuous variable quantum key distribution in atmospheric channel. *Quantum Inf Process*. 2021;20(8):258.
49. Wang T, Huang P, Zhou Y, Liu W, Zeng G. Practical performance of real-time shot-noise measurement in continuous-variable quantum key distribution. *Quantum Inf Process*. 2018;17(1):11.

50. Liao Q, Wang Y, Huang D, Guo Y. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt Express*. 2018;26(16):19907–19920.
51. Li Y, Huang P, Wang S, Wang T, Li D, Zeng G. A denial-of-service attack on fiber-based continuous-variable quantum key distribution. *Phys Lett A*. 2018;382(45):3253–3261.
52. Cao Z, Wang L, Liang K, Chai G, Peng J. Continuous-variable quantum secure direct communication based on Gaussian mapping. *Phys Rev Appl*. 2021;16(2):Article 024012.
53. Zhao H, Li H, Yuehan X, Huang P, Wang T, Zeng G. Simple continuous-variable quantum key distribution scheme using a Sagnac-based Gaussian modulator. *Opt Lett*. 2022;47(12):2939–2942.
54. Chen R, Huang P, Li D, Zhu Y, Zeng G. Robust frame synchronization scheme for continuous-variable quantum key distribution with simple process. *Entropy*. 2019;21(12):1146.
55. Xiaodong W, Wang Y, Li S, Zhang W, Huang D, Guo Y. Security analysis of passive measurement-device-independent continuous-variable quantum key distribution with almost no public communication. *Quantum Inf Process*. 2019;18:Article 372.
56. Bai D, Huang P, Ma H, Wang T, Zeng G. Practical analysis of continuous-variable quantum key distribution using a nondeterministic noiseless linear amplifier. *Int J Theor Phys*. 2018;57:3081–3097.
57. Zhang X, Zhang Y, Zhao Y, Wang X, Song Y, Guo H. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Phys Rev A*. 2017;96(4):Article 042334.
58. Papanastasiou P, Ottaviani C, Pirandola S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys Rev A*. 2017;96(4):Article 042332.
59. Qin H, Kumar R, Alléaume R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys Rev A*. 2016;94(1):Article 012325.
60. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photonics*. 2013;7(5):378–381.
61. Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys Rev A*. 2010;81(6):Article 062343.
62. Chai G, Cao Z, Liu W, Zhang M, Liang K, Peng J. Novel continuous-variable quantum secure direct communication and its security analysis. *Laser Phys Lett*. 2019;16(9):Article 095207.
63. He G, Zhu J, Zeng G. Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations. *Phys Rev A*. 2006;73(1):Article 012314.
64. Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys Rev A*. 2007;76(4):Article 042305.