Research
A SCIENCE PARTNER JOURNAL

RESEARCH ARTICLE

Realization of High-Reliable Coherent-State Quantum Secure Communication

Xinlei Chen†, Geng Chai†, Lei Wang, Sijie Wang, Xiaojie Chen, and Zhengwen Cao*

Laboratory of Quantum Information and Technology, School of Electronic Information, Northwest University, Xi'an 710127, China.

*Address correspondence to: caozhw@nwu.edu.cn
†These authors contributed equally to this work.

Citation: Chen X, Chai G, Wang L, Wang S, Chen X, Cao Z. Realization of High-Reliable Coherent-State Quantum Secure Communication. *Research* 2026;9:Article 1290. https://doi.org/10.34133/research.1290

Submitted 23 March 2026
Revised 27 April 2026
Accepted 28 April 2026
Published 1 June 2026

Copyright © 2026 Xinlei Chen 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 (CC BY 4.0).

Continuous-variable quantum secure communication encoded by Gaussian mapping offers high-capacity and high transmission rates. For the theoretically secure encryption scheme of a 1-time pad, a highly reliable coherent-state quantum secure communication system has been established, and its security has been quantitatively evaluated using Wyner's wiretap channel theory. We also propose an information reconstruction scheme based on multidimensional rotation to extract secret messages at low-to-medium signal-to-noise ratios. Meanwhile, to address the unbalanced optical path, we design a self-balanced homodyne detector based on a programmable gain amplifier, achieving an electronic noise variance of $1.624 \times 10^{-7}\,V^2$ and a bandwidth of 715 MHz. In 10-km optical fiber transmission, the system successfully achieved secure transmission of the dichroic image, processed 1,536 information blocks, each containing 2^{10} continuous variables, with a block error rate of approximately 8.78×10^{-5}, and ultimately achieved the secrecy capacity of 2.44×10^5 bits per second.

Introduction

As we transition from the era of traditional computing to the new era of quantum computing, numerous vital cybersecurity issues must be reconsidered. The 1-time pad is an encryption technique that cannot be cracked in cryptography, and its key is a single-use preshared key [1]. However, with advances in theory and technology, quantum computers can bypass existing defense mechanisms with their formidable computing power, completely disrupting or cracking the digital encryption systems that modern information and communication infrastructure rely on [2,3].

To address the security threats posed by brute-force key-cracking, quantum communication provides protection against eavesdropping and computational cracking based on the principles of uncertainty, measurement collapse, and the noncloning theorem in quantum mechanics [4–6]. The groundbreaking BB84 quantum key distribution (QKD) protocol established an essential milestone in quantum communication [7], which marks an essential milestone in quantum communication. Since then, quantum communication technology has continued to develop and some practical schemes have been applied in information security. For example, QKD has been used to ensure the security of information transmission [7,8]; quantum teleportation enables long-distance transmission of information without the need for direct transmission of physical carriers [9]; quantum secure communication (QSC) [10], also known as quantum secure direct communication, is different from QKD, which transmits random numbers over a quantum channel. QSC provides a direct method for the legitimate communication parties to transmit secret messages through the quantum channel [10,11]. There are 2 primary methods for establishing the quantum correlation between communication parties in QSC. The first is the 2-step protocol based on dense coding, which uses Einstein–Podolsky–Rosen pairs, whose theoretical security depends on error-free transmission of the checking sequence, and also identifies the secure transmission conditions under noisy channels [11]. Subsequently, the team used random single-photon bit encoding to propose another scheme without entanglement sources, namely the DL04 protocol, which can ensure its security [12].

QSC emerged after QKD, but numerous theoretical protocols and applications have been developed over the past 2 decades. QSC has gradually become a research hotspot in QSC [13]. Typical advances include the use of the Greenberger–Horne–Zeilinger state [14], multiuser QSC networks [15,16], 1-step QSC [17], passive-state preparation QSC [18], decoy-state QSC [19,20], receiver-device-independent QSC [21], QSC based on quantum error correction code [22], and semantic QSC [23]. At the same time, measurement-device-independent protocols and device-independent protocols have also been proposed, laying a solid foundation for using actual devices for QSC in communication [24–26]. In terms of experiments, the early experiments based on the single-photon platform have confirmed that QSC can operate under noise and loss [27]. Entanglement-based QSC using quantum memory has been experimentally demonstrated [28], including a 500-m implementation based on optical fiber entanglement sources [29]. These pioneering experiments realized early QSC protocols and established a solid foundation for subsequent technological

development. Sun et al. [30] employed delay encoding to replace quantum memory, thereby addressing the bottleneck posed by the lack of practical quantum memory. Subsequently, the integration of classical coding theory with QSC was developed to tackle the security challenges of high loss and code errors [31], with the security analysis completed using Wyner's wiretap channel theory and the first practical system being developed [32,33]. These technological advances enabled QSC to utilize optical fibers for intercity communication, reaching a maximum distance of 100 km [34]. Additionally, experimental demonstrations of QSC on optical fiber channels have been achieved without active polarization compensation [35].

In addition to optical fiber communication solutions, QSC based on single photons has been implemented in free-space channels [36]. Furthermore, QSC has been combined with postquantum cryptography to construct secure repeaters, enabling the establishment of large-scale quantum communication networks while mitigating the security risks associated with trusted repeaters [37]. Recently, a key breakthrough was achieved in a 1-way quasi-QSC protocol with single photons, demonstrating stable transmission at 2.38 kilobits per second over 104.5 km of optical fiber [38], with a 4,760-fold rate increase compared to 2022 [34]. In network scenarios, a QSC scheme employing a dual-pumped structure successfully achieved 300-km QSC among 4 pairs of users [39].

The QSC technology mentioned above is based on discrete variable systems. Due to its early research and rapid development, the related demonstration models and experiments have matured quickly. In contrast, continuous variable (CV) protocols are compatible with classical electro-optical communication devices and transmit continuous symbols, thereby achieving higher communication capacity and faster communication rates. The first CV quantum secure communication (CV QSC) protocol employed coherent states as light sources [40]. Since then, various CV QSC protocols based on single-mode and entangled states have emerged [41–44]. Among them, the Gaussian mapping (GM) provides a convenient and efficient modulation method to achieve accurate Gaussian modulation. Moreover, the feasibility and effectiveness of the 2-step CV QSC based on GM have been experimentally verified in the optical fiber channel, and the corresponding parameter estimation scheme is established [43]. In addition, a 20 megabits-per-second high-speed quantum radio-frequency-over-light communication based on CV quantum dense coding with entangled states has been experimentally realized [45]. Recent studies have shown that the deterministic purification scheme applied to the coherent-state system can effectively suppress excess noise [46], and QSC experiments with squeezed states have also been demonstrated [47]. Furthermore, a highly reliable QSC based on the concatenation of Gottesman–Kitaev–Preskill codes and quantum low-density parity-check codes has been developed [48].

Although protocols based on CV entanglement sources are feasible, their system complexity is considerably higher than that of single-mode implementations. In this context, we develop an experimental platform for coherent-state QSC based on a 1-time-pad scheme. The main contributions of this work are summarized as follows:

- This study successfully achieved highly reliable and secure transmission of the dichroic image in a 10-km standard single-mode fiber channel by building a coherent-state QSC with a 1-time pad experimental system, verifying the feasibility of the established system in actual communication scenarios.
- The accurate transmission of secret messages relies on the strong correlation between the statistical characteristics (SC) of Gaussian variables shared by the communicating parties. However, as the transmission distance increases or channel conditions degrade, significant discrepancies in SC may arise, leading to reduced accuracy in message recovery at the receiver. To address this issue, we propose an information reconstruction scheme based on a multidimensional rotation model, which includes both direct and indirect reconstruction modes. The core idea is to enable all parties to mutually recover Gaussian variables, reconstruct their statistical properties, and accurately extract secret messages through multidimensional rotation and inverse operations.
- During the detection stage, we observe that unbalanced optical paths introduce additional common-mode noise, which severely degrades system performance. To address this issue, we design and implemented a self-balanced homodyne detector (self-BHD) based on a programmable gain amplifier. The proposed self-BHD enables automatic balancing at high bandwidth without requiring any modification to the optical path or the introduction of additional optical components. Ultimately, an electronic noise variance of 1.624×10^{-7} V^2 was achieved, with a bandwidth of 715 MHz.
- Finally, on the basis of the proposed information reconstruction and the designed self-BHD, an efficient coherent-state QSC system was successfully implemented. In this system, the original image is encoded in 1,536 information blocks after GM, each containing 2^{10} CV quantum states. The experimental results indicate that the system achieved a secrecy capacity of 2.44×10^5 bits per second under the condition of a 10-km fiber channel, with a block error rate of about 8.78×10^{-5}, substantially improving image quality and demonstrating the practical value of this system in quantum communication applications.

The paper is structured as follows. Results and Discussion first introduces the system setup, followed by simulation analysis, and then verifies the system performance through image transmission experiments. Conclusion summarizes the above results. Methods presents the information reconstruction scheme in detail and provides a quantitative evaluation of the system security.

Results and Discussion

System implementation

The experimental setup for the proposed system is shown in Fig. 1. On Bob's side, coherent light pulses with 100 ns and a repetition frequency of 1 MHz are generated by a 1,550-nm laser diode and an amplitude modulator (AM1) and divided into weak signal light and strong local oscillator (LO) light using an extremely unbalanced beam splitter (BS1) [49]. The 2 quadratures of the signal light are modulated by another amplitude modulator (AM2) and the phase modulator (PM1) to obtain the Gaussian distribution. The signal pulse is attenuated to the quantum level by a variable optical attenuator and then sent to Alice via a 10-km optical fiber channel. The optical isolator allows the signal light to enter only the secret-message modulation module via 1 port of the polarization beam splitter (PBS2). At Alice's side, the modulation of the secret messages is accomplished using an amplitude modulator (AM4) and a phase modulator (PM3).

After being reflected by the Faraday rotator, the polarization direction of the light rotates 90°, changing from horizontal to vertical polarization. Thus, it can be ensured that the polarization state emerging from PBS2 must be vertical and then transmitted to Bob through the same channel. Similarly, PBS1 and optical isolator ensure that the pulses transmitted from Alice are output only through ports aligned with their polarization. Subsequently, Faraday rotator restores the signal pulse's polarization direction to its initial state for measurement. At the beam splitter BS6, the signal pulse interferes with the LO light. Among these components, the phase modulator (PM4) modulates the LO path phase to select the measured quadrature components.

Because interference is highly sensitive to phase difference, random phase drift in the signal light disrupts stable interference with the LO light, thereby affecting the demodulation of secret messages. To this end, phase correction can be achieved by alternating transmission of quantum signal and classical reference pulses. In the specific implementation, odd-order pulses are used as signal carriers to carry Gaussian-modulated quantum information. Even-order pulses are used as phase references and without phase changes [46]. Meanwhile, by regulating the voltages of the electro-optic modulators AM2 and PM1, the reference pulse amplitude is increased to approximately 500 times the mean amplitude of the signal pulse. Finally, the self-BHD extracts the modulation information of the signal light.

Coherent-state QSC protocol: The basic communication protocol involves 2 parties, Alice, the sender of secret messages, and Bob, the receiver. The goal is to enable Alice to send secret messages to Bob based on the Gaussian random numbers transmitted by Bob. Therefore, Alice and Bob need Gaussian modulators, and the forward and backward channels refer to the 2 opposite transmission directions of a physical channel [46,50]. The specific process of the protocol is as follows:

1. Bob generates 2 sets of Gaussian random numbers G_1 and G_2 with zero mean and variance V_B to modulate the quadrature position x and momentum p of coherent states. He sends the modulated quantum states to Alice through the forward quantum channel.
2. The 2 Gaussian sequences received by Alice can be represented as $t_1 G_1$ and $t_1 G_2$ (channel excess noise is not considered for easy understanding), where t_1 is a parameter determined by the transmittance of the forward channel. Alice uses a BS to split the received coherent-state light into 2 beams, 1 for eavesdropping detection. Secret messages are transmitted using another beam when no eavesdropping is detected.
3. After determining channel security, Alice maps the secret message to 2 Gaussian random sequences M_1 and M_2 with zero mean and variance V_A through GM (see Supplementary Materials Section S1.1 for details) and then modulates the light beam that transmits the secret message using these 2 sequences. The modulated beam is transmitted back to Bob through the backward channel, which can be given by $t_1 t_2 G_1 + t_2 M_1$ and $t_1 t_2 G_2 + t_2 M_2$. t_2 is a parameter determined by the backward channel transmittance.
4. Bob employs heterodyne detection to measure both quadrature components simultaneously. Under ideal detection conditions, the parameters t_1 and t_2 are estimated to derive the Gaussian random sequences M_1 and M_2. Through inverse GM, Bob can successfully decode the secret messages originally encoded by Alice from M_1 and M_2.

Simulation results analysis

This section will simulate the system performance of direct and indirect schemes based on security analysis (see the "System security analysis" section for details). The classic error-correcting code selected is the polar code, constructed based on channel polarization [51]. Currently, only this coding technique can theoretically be proven to achieve Shannon capacity and has linear complexity. Due to the need to construct an orthogonal matrix, the maximum dimension of multidimensional rotation is 8 dimensions $d = 8$. The simulation is set to include 2^{15} sub-information blocks per information block, for a total of 10^7 information blocks. Gaussian variables are divided into 8 equal-probability intervals. The other parameters in the simulation are as follows: modulation variance $V_B = 5$ SNU, $V_A = 8$ SNU, excess noise ϵ is 0.01; the standard loss of single-mode optical fiber cable is 0.2 dB/km.

The information reconstruction of this scheme involves a complex decoding process. With numerous secret messages and long code lengths, substantial computational resources are needed for encoding and decoding, potentially causing delays and difficulties in reconstruction. Algorithm optimization and hardware improvements are essential to address these issues. We adopt a general processing unitaccelerated hybrid decoding [52] approach combining belief propagation (BP) [53] and successive cancellation list (SCL) decoding [54]. Although SCL decoding offers superior bit error rate performance for polar codes by leveraging sequential node correlations, it lacks parallel processing capabilities. In contrast, BP decoding enables efficient parallelization. This hybrid mechanism (Algorithm 1) synergistically integrates both methods to achieve accuracy and efficiency. Taking direct information reconstruction as an example, Bob calculates the log-likelihood ratio (LLR) of the received information

$$\mathrm{LLR} = \frac{2\|M_2\|\left\|M_2'\right\|v^D}{\sqrt{d}\sigma^2} \tag{1}$$

Algorithm 1: BP hybrid SCL decoding scheduling algorithm for information reconstruction (Taking direct information reconstruction as an example).

Data: d, rotation dimension; $R\left(s'^D, s_x^D\right)$, rotation mapping function; s_y^D, normalized sequence;
Result: s'^D, Bob obtained after decoding;
Initialization;
while *All information blocks decoding not completed* **do**
  $v^D \leftarrow R\left(s'^D, s_x^D\right) s_x^D$;
  Calculate LLR based on v^D;
  if *Enough buffer storage* **then**
    Start BP Decoder;
    if CRC *correct* **then**
      Stop and decoding success;
      Decoding output s^D;
    else
      Copy failed codewords to buffer;
    end
  else
    if *Buffer not empty* & SCL*s idle* **then**
      Start idle SCL Decoder;
    else
      if SCL *decoder finished* **then**
        Free buffers;
      else
        if *All codewords decoded* **then**
          Stop and decoding success;
          Decoding output s^D;
        else
          Copy failed codewords to buffer;
        end
      end
    end
  end
  $s'^D \leftarrow (-1)^{s^D}/\sqrt{d}$;
end

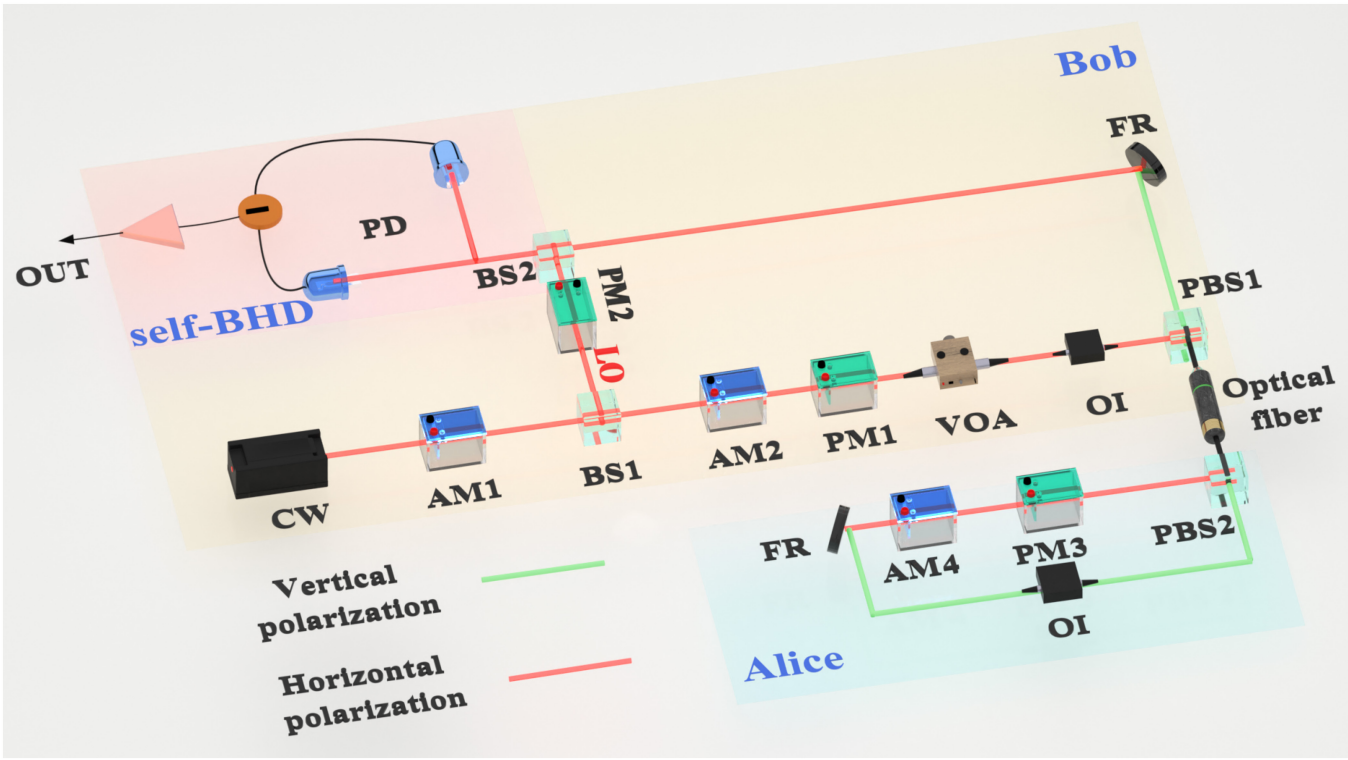


Fig. 1. Experiment setup. CW, 1,550-nm continuous-wave light source; BS, beam splitter; AM, amplitude modulator; PM, phase modulator; VOA, variable optical attenuator; OI, optical isolator; PBS, polarization beam splitter; FR, Faraday rotator; PD, photodiode; self-BHD, self-balanced homodyne detector; LO, local oscillator. Alice and Bob are in the same laboratory and separated by a 10-km optical fiber spool.

When BP decoding fails the cyclic redundancy check after maximum iterations, the codeword is forwarded to a parallel SCL decoder. The computational overhead has been reduced by implementing BP and SCL decoding on the general processing unit. The system's throughput can be approximated as

$$T_{hyb} = \frac{T_{\mathrm{BP}} \cdot T_{\mathrm{SCL}}}{\mathrm{IBER}_{\mathrm{BP}} \cdot T_{\mathrm{BP}} + T_{\mathrm{SCL}}} \tag{2}$$

where T_{BP} is the time required for BP decoding, including the number of iterations and the duration of each iteration. T_{SCL} is the time required for the SCL decoding, which is only executed when the BP decoding fails. $\mathrm{IBER}_{\mathrm{BP}}$ is the information block error rate for BP decoding.

Figure 2A.a and A.b compare IBER with and without information reconstruction under different signal-to-noise ratio (SNR) environments. It can be seen that without information reconstruction (solid black line), the IBER is around 10^{-1}, and when the SNR is below 0 dB, the IBER exceeds 0.5. This result indicates that, under low-to-medium SNR conditions, extracting secret messages without information reconstruction is poor. However, the curves for direct (blue curve with crosses) and indirect (red curve with stars) information reconstruction are always lower than those without information reconstruction, indicating a significant improvement in information extraction accuracy. Especially when the SNR approaches 5 dB, IBER reduces by at least 10^7 times compared to without information reconstruction, and the minimum is around 10^{-8}. This marked improvement confirms that the proposed information reconstruction can enhance IBER performance in coherent-state QSC, enabling the system to extract more secret messages with lower IBER at low-to-medium SNR, meeting the needs of high reliability and secure communication. In addition, Fig. 2A.a and A.b also reveal a trend: As the code rate decreases, IBER also decreases, indicating that the information reconstruction effect is more ideal under low-code-rate conditions. However, low code rates often affect the system's overall decoding efficiency. Therefore, the most suitable code rate should be selected based on specific environments and requirements to achieve optimal system performance in practical applications.

Figure 2A.c and A.d simulate and analyze the secrecy capacity with and without information reconstruction under different channel losses. The dashed lines represent the theoretical secrecy capacity curve under different information reconstruction schemes when IBER = 0. By comparison, as the channel loss increases, the black curve representing information reconstruction without is always lower than the curve without information reconstruction, which approaches 0. Meanwhile, the performance of information reconstruction is close to its theoretical secrecy capacity. This indicates that information reconstruction greatly improves secrecy capacity and exhibits greater tolerance to channel loss, which is expected to play a key role in long-distance communication applications of CV QSC systems. Furthermore, by comparing Fig. 2A.c and Fig. 2A.d, it can be observed that the indirect outperforms the direct in terms of secrecy capacity and channel loss tolerance, while the direct scheme is relatively simple. Therefore, a suitable reconstruction scheme can be selected based on different practical application environments to achieve optimal performance and implementation efficiency.

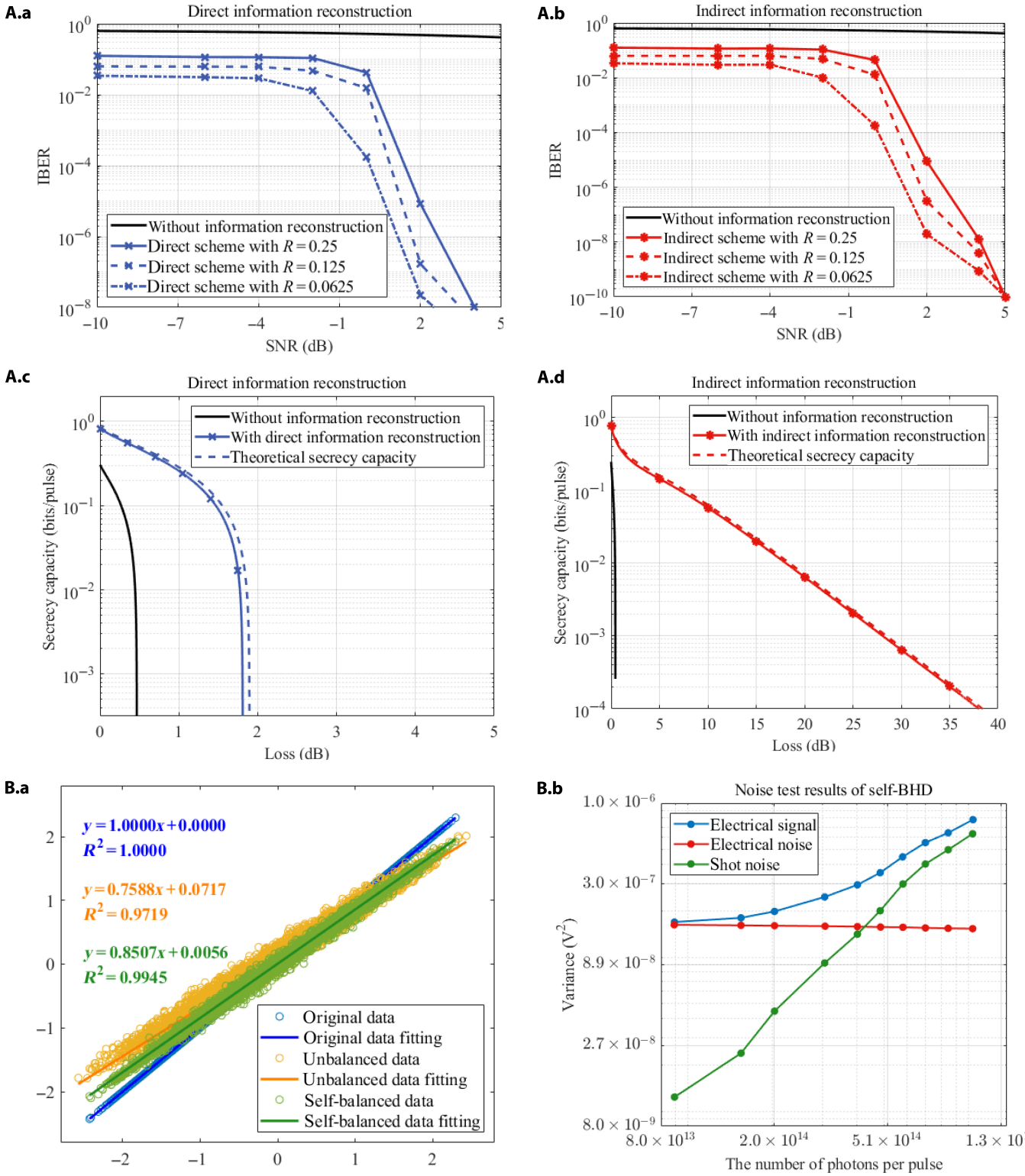


Fig. 2. (A) Comparison of information block error rate (IBER) and secrecy capacity with and without information reconstruction's coherent-state quantum secure communication (QSC) system under different signal-to-noise ratio (SNR) environments. (A.a) The IBER of direct information reconstruction. (A.b) The IBER of indirect information reconstruction. The horizontal axis represents the SNR, which ranges from −10 to 5 dB, and the vertical axis represents IBER. (A.c) Secrecy capacity of direct information reconstruction. (A.d) Secrecy capacity of indirect information reconstruction. The horizontal axis represents the channel loss, and the vertical axis represents the secrecy capacity. The black solid line represents the case without information reconstruction, the blue curve with crosses represents the application of direct reconstruction, the red curve with stars represents the application of indirect reconstruction, and the different line shapes represent different polar code rates $Rc = 0.25$, $Rc = 0.125$, and $Rc = 0.0625$. The dashed lines represent the theoretical secrecy capacity curves of the proposed scheme under different information reconstruction schemes. (B) The test results of relevant indicators of the self-balanced homodyne detector (self-BHD). (B.a) Statistical distribution of data under self-balanced and unbalanced optical paths. (B.b) Electrical noise test results of self-BHD.

Experimental verification and analysis

This section conducts experimental verification of the proposed scheme based on the experimental setup shown in Fig. 1 and analyzes the experimental results. As the system's key component, the modulation and detection of quantum signals directly determine the system's performance. At the end of modulation, we adopt Gaussian modulation. This technology has the advantage of high information capacity and maintains good compatibility with classical communication systems. The module has recently been optimized, enabling the modulation of the quantum signal through adaptive photoelectric calibration in an field-programmable gate array-based miniaturized unit [55]. During the detection stage, we observed that an unbalanced optical path would introduce additional common-mode noise, substantially affecting system performance. Thus, we designed a self-BHD to compensate for the unbalanced optical path and then applied it to the experimental platform. The designed self-BHD is detailed in the Supplementary Materials Section S1.2. This self-BHD achieves high-bandwidth automatic balance control without modifying the optical path or adding optical devices. It should be noted that existing methods involve the addition of variable optical attenuators to achieve self-balance, but such solutions would reduce the detection efficiency of the system [56].

Firstly, we tested and compared the output signals in a balanced and an unbalanced optical path to evaluate the detector's performance. In short, enable the self-balanced function, record the output signal after the optical path is balanced, then turn off the function, and manually set the programmable-gain amplifier gain to the same value to simulate an unbalanced optical path. The test results are shown in Fig. 2B.a. The self-balanced (green fitting line) not only exhibits better linear characteristics than the unbalanced (yellow) but also markedly improves agreement with the initial signal (blue). The test results for the variance of the output electrical signal, the electrical noise, and the shot noise of the detector under different LO intensities are shown in Fig. 2B.c. When the input LO intensity of the self-BHD is 128 μW, the number of photons per pulse is 10^{15}, and the shot noise is about 6.7 dB higher than the electrical noise. In addition, the self-BHD has the following characteristics: The electronic noise variance is 1.624×10^{-7} V^2, the bandwidth is about 715 MHz, with a gain fluctuation in the passband less than 3 dB, and the common-mode rejection ratio of the self-BHD is 59.77 dBm. Please refer to the illustration in the Supplementary Materials Section S1.2 for specific test results.

To demonstrate the effectiveness of this scheme more intuitively, we selected the dichroic image shown in Fig. 3A. In the experiment, 1,536 information blocks were transmitted, each containing 2^{10} variables. To simplify the measurement system's complexity, we measure only 1 quadrature component, randomize it, perform symbol mapping, and then apply spherical mapping to both the original and symbol-mapped sequences. The number of intervals divided is 8, the multidimensional rotation dimension is $d = 8$, and the polar code rate is $R_c = 0.125$. All experimental data were decoded on an NVIDIA GeForce RTX 2080 Ti. To ensure the reliability of the results, each information block is independently decoded 10^4 times. Experimental performance of 10-km optical fiber transmission is shown in Table 1, which also compares the error rates of the existing systems [43,45] with our system. Our system can achieve an error rate of 8.78×10^{-5} at 1.39 dB, indicating a greater information extraction advantage than previous systems. Figure 3B and C present the experimental results of excess noise and channel transmittance for 1,536 information blocks in the backward channel. The results indicate that the fluctuation range is relatively small, with mean values of 0.017 (SNU) and 0.568, respectively, confirming the experimental system has good stability.

Figure 3D shows the SC of Gaussian variables of P-component in the backward channel between Alice and Bob, indicating the validity of the experiment's measured data and providing a data basis for subsequent information reconstruction steps. Fig. 3E is the restored image without information reconstruction corresponding to Fig. 3A. After direct information reconstruction, the SC of Alice and Bob's Gaussian variables are shown in Fig. 3F, and the corresponding restored images are shown in Fig. 3G. Figure 3H and I, respectively, show the SC of Gaussian variables and the restored images after indirect information reconstruction. By comparing these restored images with the original images, we can observe that information reconstruction shows clear advantages compared to without information reconstruction, with substantial improvements in image accuracy and clarity. These results further validate the effectiveness of the proposed information reconstruction, indicating that it can effectively enhance the system's reliability and anti-interference ability. The relationship between the transmission distance and the secrecy capacity is shown in in Fig. 3J. The yellow circle represents the results based on entangled state CV QSC in a 5-km optical fiber [43]. The star markings represent the results of discrete variable QSC under 30- and 100-km optical fiber transmission, respectively [34]. The triangle corresponds to the results obtained by the system using both direct and indirect information reconstruction modes in a 10-km optical fiber. The dashed line represents the theoretical secrecy capacity for indirect information reconstruction, and the solid line with stars represents the secrecy capacity at different code rates (this relationship is derived based on the calibration parameters in Table 1). It is worth noting that all experimental data points for the compared systems lie below this system's curve, highlighting its marked advantage in improving confidentiality capacity and demonstrating its application prospects in long-distance communication.

Conclusion

This work establishes a coherent-state QSC experimental platform and achieves reliable image transmission. Among them, the original image is encoded in 1,536 information blocks after GM, each containing 2^{10} CV quantum states. The system achieved a secrecy capacity of 2.44×10^5 bits per second under a 10-km fiber channel, fully verifying the feasibility and practicality of the proposed scheme. Specifically, we propose an information reconstruction scheme based on a multidimensional rotation mathematical model to solve the problem of poor accuracy in extracting secret messages under low-to-medium SNR, which includes 2 methods: direct and indirect reconstruction, and the lower limit of secrecy capacity for these 2 schemes was calculated separately based on Wyner's wiretap channel theory. Subsequently, the results show that information reconstruction performs excellently at low-to-medium SNRs (−10 to 5 dB) and can efficiently extract secret messages. Compared to without information reconstruction, IBER reduces up to 10^7 times, which improves the accuracy of secret messages. Furthermore, in response to the issue of an unbalanced optical path, we have also designed a self-BHD based on a programmable gain amplifier. The test results show that the electronic noise variance of the detector is 1.624×10^{-7} V^2, and the bandwidth is about 715 MHz. Finally, the established experimental platform verified the coherent-state QSC system with

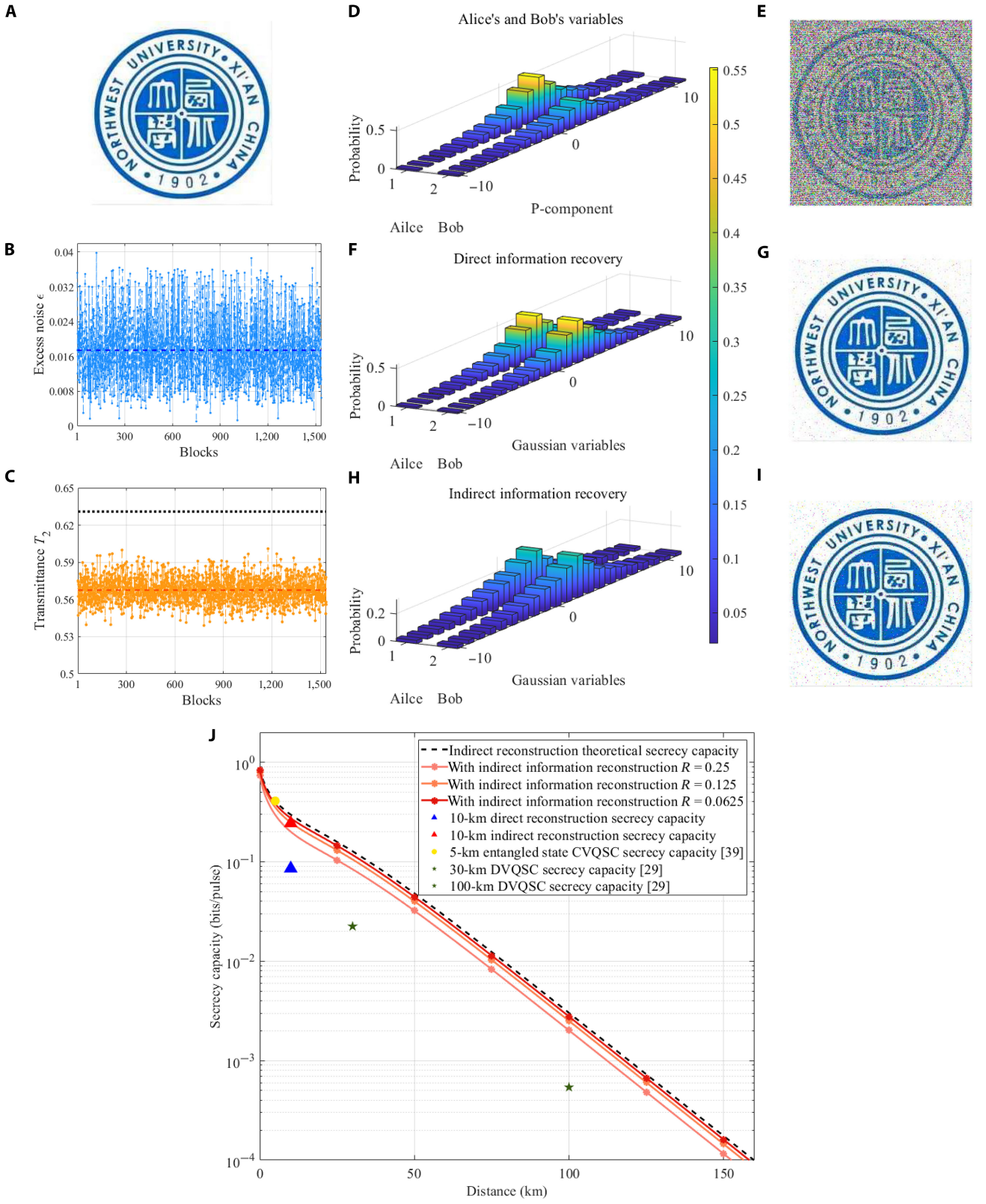


Fig. 3. Experimental results. (A) Original image. (B) Excess noise results. (C) Channel transmittance results. The small solid circles in (B) and (C) represent the results of these 1,536 information blocks as the objects of observation. The dashed line represents the average value of all information blocks. The dashed line between points represents the data's volatility. The black dotted line represents the theoretical upper bound of channel transmittance. (D) SC of P-component Gaussian variables for Alice and Bob. The horizontal axis represents Gaussian variables, and the vertical axis represents probability. (E) The restored image without information reconstruction. (F) Gaussian variables of both communication parties after direct information reconstruction. (G) The restored image after direct information reconstruction. (H) Gaussian variables of both communication parties after indirect information reconstruction. (I) The restored image after indirect information reconstruction. (J) The relationship between the transmission distance and the secrecy capacity.

Table 1. Overview of experimental performance of 10-km optical fiber transmission. SNU represents the unit of shot-noise units. V_A, Alice's modulation variance; ϵ, excess noise; T_2, the backward channel transmittance; IBER, information block error rate; SC, secrecy capacity; bps, bit per second; T_{hyb}, throughput of the hybrid decoder; SNR, signal-to-noise ratio.

Parameter	V_A (SNU)	ϵ (SNU)	T_2	IBER	SC	T_{hyb}
Value	10	0.017	0.568	8.78×10^{-5}	2.44×10^5 bps	38.52 Mbit/s
	Cao et al. [43]		Liang et al. [45]		Our work	
SNR (dB)	1.89		11 ~ 12		1.39	
Error rate	10^{-3}		$(3.0 \pm 0.9) \times 10^{-4}$		8.78×10^{-5}	

information reconstruction and self-BHD. The results show that this system exhibits excellent image transmission performance and achieves an IBER of about 8.78×10^{-5}. This achievement strongly confirms the effectiveness and applicability of this information reconstruction mechanism in practical systems.

The information reconstruction scheme proposed in this study effectively improves the transmission reliability of the coherent-state QSC system. However, in the scheme, transmitting additional information through the classical channel still incurs communication resource occupation, which limits the system's efficiency to some extent. In response to this technical bottleneck, subsequent research will focus on breaking through the dependence on classical channels and will be committed to developing an efficient information reconstruction mechanism based on quantum channels. The breakthrough in this direction is expected to substantially enhance the practical value of the CV QSC system and promote its engineering process.

Methods

Information reconstruction for coherent-state QSC

Secret messages can be transmitted through Gaussian modulation using GM [43]. However, unknown channel characteristics and imperfect devices inevitably affect quantum state transmission and measurement. These factors lead to considerable discrepancies between the Gaussian variables SC of Alice's encoded messages and Bob's received signals. Although the GM interval has a certain tolerance for noise, as this deviation increases, the system's tolerance will gradually decrease, affecting the accuracy of secret messages.

An information reconstruction scheme is proposed to address the above issues. Alice divided the secret message into M information blocks and performed uniformization into subinformation blocks through GM (GM rules are based on precommunication agreements) to obtain Gaussian variables M_1 and M_2. Alice uses M_1 and M_2 to modulate the 2 quadrature components that transmit the secret messages. The modulated output beam is sent to Bob through the backward channel. After measuring and removing the effect of his previously modulated information, Bob holds 2 sets of Gaussian variables $M_{1'}$ and $M_{2'}$ that are related but inconsistent with the sequences M_1 and M_2. The quantum channel involved is simplified into a standard linear model to describe the correlation between Alice and Bob's data, namely: $M_{1'} = t_2 M_1 + Z, t_2 = \sqrt{\eta T_2}, T_2$ is the backward channel transmittance, η is the detector efficiency, Z is the total Gaussian noise in the backward channel, satisfying a Gaussian distribution $\mathcal{N}(0, \sigma^2)$, and σ^2 is the noise variance.

In the information reconstruction stage, the communication parties use multidimensional rotation [57] based on the correlations among the Gaussian variables they hold, allowing them to recover the Gaussian variables of each other. Two schemes use different methods for recovering random numbers: direct and indirect reconstruction (as shown in Fig. 4A).

Direct information reconstruction: Bob recovers the Gaussian variables that carry the secret messages sent by Alice.

1. Symbol mapping: Alice performs multidimensional rotation on her Gaussian variables in the direct information reconstruction, as shown in Fig. 4A. Firstly, she performs symbol mapping on 1 of the 2 sequences. For example, Alice conducts symbol mapping on the M_1 sequence, mapping positive values to "0" and negative values to "1", thus generating a set of binary sequences. Subsequently, he randomly selected a sequence c^D (the superscript D represents the direct scheme) of length K from the binary sequence based on the error correction code rate R_c ($R_c = K/N$, N is the number of subinformation blocks in an information block). Then, she encoded it as s^D of length N using classical error correction codes.
2. Spherical mapping: Alice performs the spherical mapping on sequences s^D and M_2, with a specified dimension of d. The specific mapping relationship is as follows

$$s'^D = \left(s_1^D, s_2^D, \cdots, s_d^D\right) \to \left(\frac{(-1)^{s_1^D}}{\sqrt{d}}, \frac{(-1)^{s_2^D}}{\sqrt{d}}, \cdots, \frac{(-1)^{s_d^D}}{\sqrt{d}}\right) \quad (3)$$

$$s_x^D = M_2 / \|M_2\| = \frac{M_2}{\sqrt{\sum_{i=1}^{d} M_{2_i}^2}} \quad (4)$$

Then, Alice calculates the rotation matrix $R\left(s'^D, s_x^D\right)$ by combining the d-dimensional sphere sequences s'^D and normalized sequence s_x^D after spherical mapping, which satisfies $R\left(s'^D, s_x^D\right) s_x^D = s'^D$, i.e., $H\left(s'^D | s_x^D, R\right) = 0$. Bob sends the functions R and $\|M_2\|$ to Alice through the classical authentication channel.

3. Alice's Gaussian variables reconstruction: Bob uses the received R and the local Gaussian variables $M_{2'}$ to restore Alice's Gaussian variables M_2. The specific steps are as

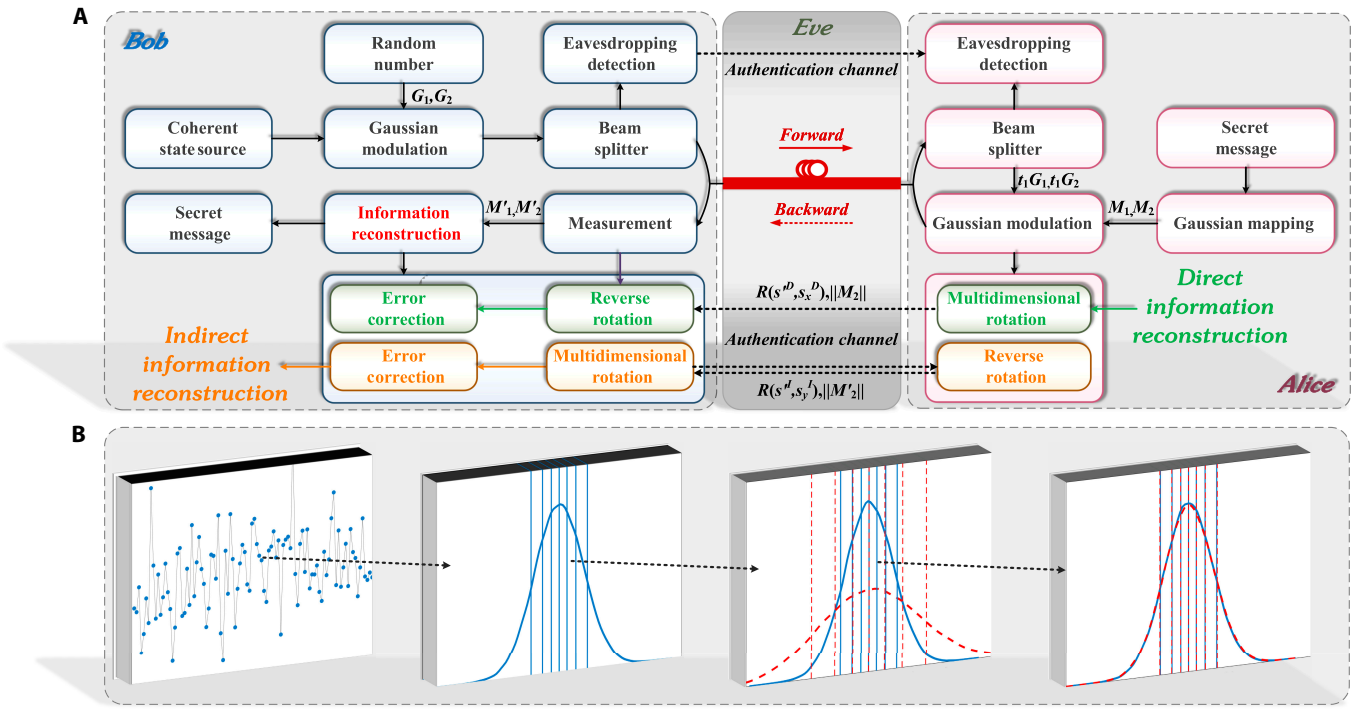


Fig. 4. (A) Process diagram of direct information reconstruction and indirect information reconstruction scheme. G_1, G_2, 2 sets of Gaussian random numbers generated by Bob. t_1, a parameter determined by the transmittance of the forward channel. M_1, M_2, the Gaussian variables sent by Alice. M'_1, M'_2, the Gaussian variables received by Bob. $R(s'^D, s_x^D)$, the rotation matrix of direct information reconstruction. $R(s'^I, s_x^I)$, the rotation matrix of indirect information reconstruction. Dashed lines transmit classical information, while quantum information is sent via a thick purple solid line. (B) From left to right, the randomly generated initial Gaussian sequence, SC after Gaussian mapping (GM), SC after the quantum channel of both communication parties, and SC after information reconstruction. The solid line represents Alice's SC and interval division, and the dashed line represents Bob's.

follows: Firstly, Bob performs the same rotation on the local sequence M_2, mapping it to the normalized sequence s_y^D (similar to sequence M_2). Then, he calculates the auxiliary sequence $v^D = R(s'^D, s_x^D)s_y^D$ and decodes it, then performs spherical mapping to obtain the sequence s'^D. Next, Bob reversely rotates s_y^D to get the sequence s_x^D

$$s_x^D = R(s'^D, s_x^D)^{-1} s'^D \tag{5}$$

In this way, Bob can calculate the Gaussian variables of Alice's modulation information

$$M_2 = \|M_2\| s_x^D \tag{6}$$

4. Error correction: Through the above calculation, when the auxiliary sequence s^D is decoded correctly, Bob performs inverse GM on the obtained M_2 to get the secret messages. If s^D decoding fails, this information block will be retransmitted.

Indirect information reconstruction: Alice recovers the Gaussian variables measured by Bob.

1. Symbol mapping: In the indirect reconstruction, as shown in Fig. 4A, Bob performs symbol mapping on 1 of the 2 sequences he holds M'_1 and M'_2, such as mapping M'_1. Then, he randomly selects a portion of the binary sequence c^I with a length of K from the mapped sequence and encodes c^I into the sequence s^I using a classical error correction code with code rate R_c (the superscript I represents the indirect scheme).
2. Spherical mapping: Bob performs spherical mapping on sequence s^I and M'_2, with d-dimension, and the mapping relationship is similar to the direct scheme

$$s'^I = (s_1^I, s_2^I, \cdots, s_d^I) \to \left(\frac{(-1)^{s_1^I}}{\sqrt{d}}, \frac{(-1)^{s_2^I}}{\sqrt{d}}, \cdots, \frac{(-1)^{s_d^I}}{\sqrt{d}} \right) \tag{7}$$

$$s_y^I = M'_2 / \|M'_2\| = \frac{M'_2}{\sqrt{\sum_{i=1}^{d} M'^2_{2i}}} \tag{8}$$

Bob calculates the rotation matrix $R(s'^I, s_y^I)$ using the sequence s'^I and s_y^I, which also satisfies $R(s'^I, s_y^I)s_y^I = s'^I$. Bob sends R and $\|M'_2\|$ to Alice through the classical authentication channel.

3. Bob's Gaussian variables reconstruction: Alice uses the received R and the local Gaussian sequence M_2 to restore Bob's Gaussian sequence M'_2. The steps are as follows: Firstly, Alice performs the same rotation on the local sequence M_2, mapping it to the sequence s_x^I, and calculates the auxiliary sequence $v^I = R(s'^I, s_y^I)s_x^I$. Decoding sequence v^I and normalizing yields sequence s'^I, which is then reverse rotated to obtain s_y^I

$$s_y^I = R(s'^I, s_y^I)^{-1} s'^I \tag{9}$$

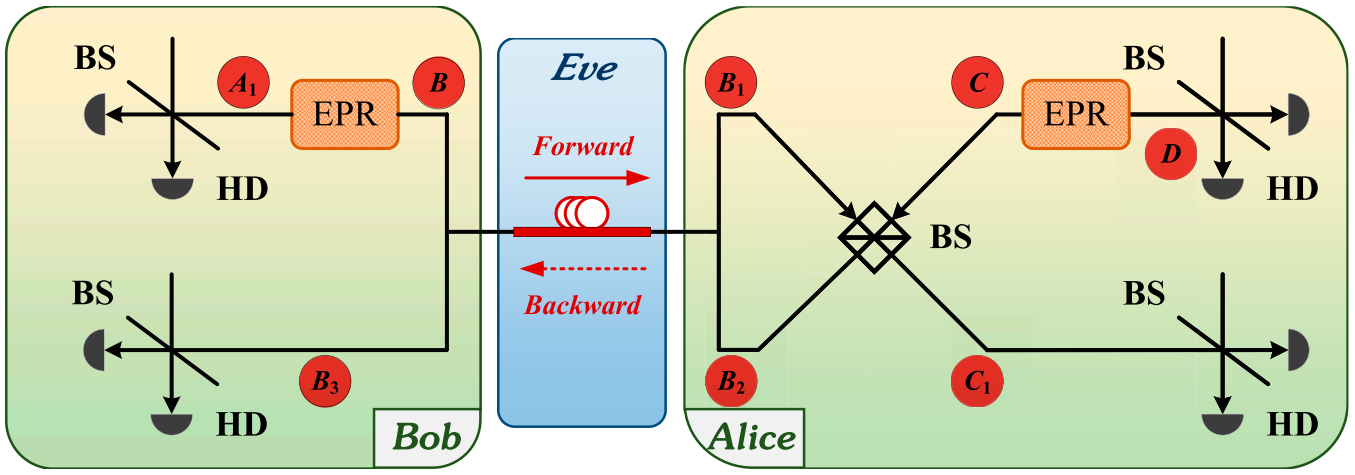


Fig. 5. System diagram of entanglement-based model of continuous variable (CV) quantum secure communication (QSC) using coherent state. EPR, entangled source; BS, beam splitter; HD, heterodyne detection; $A_1 \sim D$, quantum states.

In this way, Alice can calculate the Gaussian variables measured by Bob

$$M_2' = \|M_2'\| s_y^I \tag{10}$$

4. Error correction: Through the above steps, when the auxiliary sequence s^I is decoded correctly, Alice can obtain the correct M_2'. By comparing the inverse GM intervals of 2 sets of Gaussian variables M_2 and M_2', it can be determined where Bob will obtain the error information after the inverse GM. Alice can notify Bob of the location of the error information through the classical authentication channel. Bob performs inverse GM on sequence M_2' to obtain subinformation blocks and then corrects based on the edge information notified by Alice, thereby obtaining the secret messages. If s^I decoding fails, this information block will be retransmitted.

System security analysis

At the protocol implementation level, communication systems usually adopt the prepare-and-measure model for experimental implementation (as shown in Fig. 1A); in security analysis, the entanglement-based model is used (as shown in Fig. 5), but these 2 models have been proved to be mutually equivalent [58]. According to Wyner's wiretap channel theory, the maximum information transmission capacity between Alice and Bob in a noisy environment can be modeled as the main channel C_M [33]. Eve's eavesdropping behavior and environmental noise are modeled by the eavesdropping channel C_W, representing the maximum amount of information Eve can extract from eavesdropping symbols without violating the basic principles of quantum mechanics.

Wiretap channel theory suggests that when the secrecy capacity C_S is greater than zero, both legitimate parties can ensure the transmission security of secret messages through some encoding method at a capacity lower than C_S [32,33]. Essentially, secrecy capacity C_S is the difference between the capacity of the main channel and the capacity of the wiretap channel, that is

$$C_S = C_M - C_W. \tag{11}$$

CV QSC's core for calculating the secrecy capacity is the covariance matrix $\rho_{A_1B_3C_1D}$. The covariance matrix measured by Bob can be expressed as $\Gamma_{X_1X_2Y_1Y_2} = \frac{1}{2}\left(\rho_{A_1B_3C_1D} + \mathbb{I}_8\right)$, where $X_1X_2Y_1Y_2$ are the classical information of the collapse of $A_1B_3C_1D$ after measurement. The main channel capacity C_M is represented as

$$C_M = I\left(X_2 : \left(Y_1, Y_2\right)\right) = \log_2 \frac{\det\Gamma_{X_2} \det\Gamma_{Y_1Y_2}}{\det\Gamma_{X_2Y_1Y_2}}. \tag{12}$$

When the eavesdropper adopts collective attacks, it should be noted that the C_W calculation for direct and indirect is different. In the direct scheme, the secret-message recovery relies on the multidimensional rotation of the data sent by Alice, hence $C_W = S_{Y_2E}$, the quantum mutual information between Alice and Eve. In the indirect scheme, secret-message recovery relies on the multidimensional rotation of data sent by Bob, hence $C_W = S_{X_2E}$, the quantum mutual information between Bob and Eve.

For the convenience of analyzing protocol security, when Bob initially prepares and distributes a quantum state with variance V, after Alice receives the quantum state but before measurement, the corresponding covariance matrix of the system's state $\rho_{A_1B_3C_1D}$ is

$$\begin{bmatrix} V_B\mathbb{I}_2 & * & * & \\ \sqrt{\tau T_1 T_2\left(V_B^2-1\right)}\sigma_Z & \left[\tau T_1 T_2\left(V_B+\chi_{\text{line1}}\right)+(1-\tau)T_2V_A+T_2\chi_{\text{line2}}\right]\mathbb{I}_2 & * & * \\ -\sqrt{(1-\tau)T_1\left(V_B^2-1\right)}\sigma_Z & -\sqrt{\tau(1-\tau)T_2}\left[T_1\left(V_B+\chi_{\text{line1}}\right)-V_A\right]\mathbb{I}_2 & \left[(1-\tau)T_1\left(V_B+\chi_{\text{line1}}\right)+\tau V_A\right]\mathbb{I}_2 & * \\ & \sqrt{(1-\tau)T_2\left(V_A^2-1\right)}\sigma_Z & \sqrt{\tau\left(V_A^2-1\right)}\sigma_Z & V_A\mathbb{I}_2 \end{bmatrix} \tag{13}$$

where V_B is Bob's modulation variance, $\chi_{\text{line1}} = 1/T_1 - 1 + \epsilon_1$ represents the linear noise, T_1 is the channel transmittance, ϵ_1 is excess noise, and all are calculated with shot noise as a unit.

Taking direct information recovery as an example, X_2 is the measurement result of B_3. The covariance matrix $\Gamma_{A_1C_1D|X_2}$ of state A_1C_1D with measurement result X_2 as a condition is calculated as follows

$$\Gamma_{A_1C_1D|X_2} = \Gamma_{A_1C_1D} - C^T_{A_1C_1DX_2}\left(\Gamma_{X_2} + \mathbb{I}_2\right)^{-1} C_{A_1C_1DX_2}. \tag{14}$$

The submatrices of the above conditional covariance matrix (obtained by rearranging the rows and columns of $\rho_{A_1B_3C_1D}$) are as follows

$$\Gamma_{X_2} = \left[\tau T_1 T_2\left(V_B + \chi_{\text{line1}}\right) + (1-\tau)T_2 V_A + T_2\chi_{\text{line2}}\right]\mathbb{I}_2 \tag{15}$$

$$\Gamma_{A_1C_1D} = \begin{bmatrix} V_B\mathbb{I}_2 & * & \\ -\sqrt{(1-\tau)T_1\left(V_B^2-1\right)}\sigma_Z & \left[(1-\tau)T_1\left(V_B+\chi_{\text{line1}}\right)+\tau V_A\right]\mathbb{I}_2 & * \\ & \sqrt{\tau\left(V_A^2-1\right)}\sigma_Z & V_A\mathbb{I}_2 \end{bmatrix} \tag{16}$$

$$C_{A_1C_1DX_2} = \left[\sqrt{\tau T_1 T_2\left(V_B^2-1\right)}\sigma_Z - \sqrt{\tau(1-\tau)T_2}\left[T_1\left(V_B+\chi_{\text{line1}}\right)-V_A\right]\right.$$
$$\left.\mathbb{I}_2\sqrt{(1-\tau)T_2\left(V_A^2-1\right)}\sigma_Z\right] \tag{17}$$

In the proposed scheme, the calculation of S_{Y_2E} and S_{X_2E} is limited by the Holevo bound

$$S_{Y_2E} = S(E) - S\left(E|m_A\right) \overset{\text{purification}}{\rightarrow} = S\left(A_1B_3C_1D\right) - S\left(A_1B_3C_1|D\right) \tag{18}$$

$$S_{X_2E} = S(E) - S\left(E|m_B\right) \overset{\text{purification}}{\rightarrow} = S\left(A_1B_3C_1D\right) - S\left(A_1C_1D|B_3\right) \tag{19}$$

where $S(\rho)$ is the von Neumann entropy of a quantum state and $S\left(E|m_{A(B)}\right)$ is the conditional entropy of the quantum state that Eve grasps after knowing Alice's (Bob's) measurement results. Since $S(E) = S\left(A_1B_3C_1D\right)$ is the von Neumann entropy of the system, it is independent of the choice of scheme, and therefore, it is the same for both direct and indirect schemes. According to Williamson's theorem, the calculation of the Gaussian state von Neumann entropy can be simplified by the symplectic eigenvalues of the covariance matrix

$$S_{Y_2E} = \sum_{i=1}^{4} G\left(\lambda_i\right) - \sum_{i=1}^{3} G\left(\lambda_i^D\right) \tag{20}$$

$$S_{X_2E} = \sum_{i=1}^{4} G\left(\lambda_i\right) - \sum_{i=1}^{3} G\left(\lambda_i^I\right) \tag{21}$$

where the function $G(x)$ is defined as

$$G(x) \coloneqq \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right). \tag{22}$$

The following symplectic invariants $\Delta_{m,k}$ must first be established to determine the symplectic eigenvalues of the covariance matrix $\Gamma_{A_1B_3C_1D}$ [59].

$$\Delta_{m,k} = \mathcal{M}_{2k}\left(i\Omega\Gamma_{A_1B_3C_1D}\right), \tag{23}$$

where m is the number of modes, $\Omega = \oplus_{i=1}^{m}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. $\mathcal{M}_{2k}\left(i\Omega\Gamma_{A_1B_3C_1D}\right)$ is the $2k$-order principal minor of the $2m \times 2m$ matrix $\Omega\Gamma_{A_1B_3C_1D}$, that is, the sum of the determinants of all $2k \times 2k$ submatrices of $\Omega\Gamma_{A_1B_3C_1D}$. Then, the symplectic eigenvalues can be used to solve the polynomial of the following 4 modes, 3 modes, and 2 modes

$$z^4 - \Delta_{4,1}z^3 + \Delta_{4,2}z^2 - \Delta_{4,3}z + \Delta_{4,4} = 0 \tag{24}$$

$$z^3 - \Delta_{3,1}z^2 + \Delta_{3,2}z - \Delta_{3,3} = 0. \tag{25}$$

Specifically, we noticed that although information recovery can extract secret messages, it provides Eve with additional information. Therefore, the secrecy capacity after information recovery should be rewritten as

$$C_S^D = I_{AB} - S\left(M_2 : E, R\right) \tag{26}$$

$$C_S^I = I_{AB} - S\left(M_2' : E, R\right) \tag{27}$$

Alice and Bob can estimate the upper bound of S_{Y_2E} and S_{X_2E} on the basis of their covariance matrix. However, $S\left(M_2 : E, R\right)$ and $S\left(M_2' : E, R\right)$ cannot be inferred from them. Fortunately, we have the following theorem.

Theorem: Let $\mathcal{A}$ and $\mathcal{B}$ be classical random variables, and let $\mathcal{E}$ be a random quantum state. If $\mathcal{A}$ and $\mathcal{B}$ are independent of each other, then $S(\mathcal{A}:\mathcal{E},\mathcal{B}) \leq S(\mathcal{A},\mathcal{B}:\mathcal{E})$ [57].

Next, according to the chain rule of mutual quantum information

$$S\left(M_2\, s_x^D : E\right) = S\left(M_2 : E\right) + S\left(s_x^D : E|M_2\right). \tag{28}$$

Since s_x^D is a symbol mapping of M_1's random sequence and then encoded, independently of M_2, this means that $S\left(s_x^D : E|M_2\right) = 0, S\left(M_2, s_x^D : E\right) = S\left(M_2 : E\right) = S_{Y_2E}$. Coincidentally, in information recovery, M_2 and R are independent of each other, so there is $S\left(M_2 : E, R\right) \leq S\left(M_2, R : E\right)$ Then, since R is a function of M_2 and s_x^D, $S\left(M_2 : E, R\right) \leq S\left(M_2, R : E\right) = S\left(M_2 : E\right) = S_{Y_2E}$. $S\left(M_2' : E, R\right)$ can also derive $S\left(M_2' : E, R\right) \leq S_{X_2E}$ Then, the lower bound of secrecy capacity after information recovery remains:

$$C_S^D = I_{AB} - S\left(M_2 : E, R\right) \geq I_{AB} - S_{Y_2E} \tag{29}$$

$$C_S^I = I_{AB} - S\left(M_2' : E, R\right) \geq I_{AB} - S_{X_2E} \tag{30}$$

In addition, due to the possibility of errors during the decoding process, the recovery of random numbers is not accurate, manifested as an IBER in the information recovery. Since we are calculating the secrecy capacity of the backward channel, a

coefficient of $\frac{1}{2}$ needs to be introduced. Given this, the final expression for the secrecy capacity is

$$C_S^D = \frac{1}{2}\left((1-\mathrm{IBER})I_{AB} - S_{Y_2E}\right) \tag{31}$$

$$C_S^I = \frac{1}{2}\left((1-\mathrm{IBER})I_{AB} - S_{X_2E}\right) \tag{32}$$

where IBER is the ratio of erroneous information blocks to the total number.

Acknowledgments

Funding: This work is supported by the National Natural Science Foundation of China (62571432, 62301430, and 62071381) and Shaanxi Fundamental Science Research Project for Mathematics and Physics (Grant No. 23JSY014).
Author contributions: Conceptualization: Xinlei C. Design and interpretation of experiments: G.C. and Xinlei C. Data acquisition and analysis: Xinlei C. and G.C. Drafting and revising the manuscript: Xinlei C., L.W., Xiaojie C. and S.W. Statistical analysis: Xinlei C., G.C. and L.W. Administrative and supervisory support: Z.C.
Competing interests: The authors declare that they have no competing interests.

Data Availability

The materials and data can be obtained from the corresponding author on reasonable request.

Supplementary Materials

Figs. S1 to S4
References [60,61]

References

1. Rubin F. One-time pad cryptography. *Cryptologia*. 1996;20(4):359–364.
2. Ladd TD, Jelezko F, Laflamme R, Nakamura Y, Monroe C, O'Brien JL. Quantum computers. *Nature*. 2010;464:45–53.
3. Bhatia V, Ramkumar K. An efficient quantum computing technique for cracking RSA using Shor's algorithm. In: *2020 IEEE 5th International Conference on Computing, Communication and Automation (ICCCA)*. Greater Noida (India): IEEE; 2020. p. 89–94.
4. Robertson HP. The uncertainty principle. *Phys Rev*. 1929;34:163.
5. Namiki M, Pascazio S. Wave-function collapse by measurement and its simulation. *Phys Rev A*. 1991;44(1):39.
6. Piqueira JRC. Quantum information theory: Non-cloning, entanglement and teleportation. *Revista Brasileira De Ensino De Fisica*. 2011;33:4303.
7. Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Theor Comput Sci*. 2014;560:7–11.
8. Wang S, Yin Z-Q, He D-Y, Chen W, Wang R-Q, Ye P, Zhou Y, Fan-Yuan G-J, Wang F-X, Chen W, et al. Twin-field quantum key distribution over 830-km fibre. *Nat Photonics*. 2022;16(2):154–161.
9. Pirandola S, Eisert J, Weedbrook C, Furusawa A, Braunstein SL. Advances in quantum teleportation. *Nat Photonics*. 2015;9(10):641–652.
10. Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*. 2002;65(3):Article 032302.
11. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A*. 2003;68:Article 042317.
12. Deng FG, Long GL. Secure direct communication with a quantum one-time pad. *Phys Rev A: At Mol Opt Phys*. 2004;69:Article 052319.
13. Pan D, Long G-L, Yin L, Sheng Y-B, Ruan D, Ng SX, Lu J, Hanzo L. The evolution of quantum secure direct communication: On the road to the Qinternet. *IEEE Commun Surv Tutor*. 2024;26(3):1898–1949.
14. Jin X-R, Ji X, Zhang Y-Q, Zhang S, Hong S-K, Yeon K-H, Um C-I. Three-party quantum secure direct communication based on GHZ states. *Phys Lett A*. 2006;354(1-2):67–70.
15. Deng FG, Li XH, Li CY, Zhou P, Zhou HY. Quantum secure direct communication network with Einstein–Podolsky–Rosen pairs. *Phys Lett A*. 2006;359(5):359–365.
16. Qi Z, Li Y, Huang Y, Feng J, Zheng Y, Chen X. A 15-user quantum secure direct communication network. *Light Sci Appl*. 2021;10(1):183.
17. Sheng YB, Zhou L, Long GL. One-step quantum secure direct communication. *Sci Bull*. 2022;67(4):367–374.
18. Ying J-W, Wang J-Y, Xiao Y-X, Gu S-P, Wang X-F, Zhong W, Du M-M, Li X-Y, Shen S-T, Zhang A-L, et al. Passive-state preparation for quantum secure direct communication. *Sci Chin Phys Mech Astron*. 2025;68:Article 240312.
19. 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 Chin Phys Mech Astron*. 2021;64: Article 120311.
20. Ying J-W, Wang J-Y, Xiao Y-X, Gu S-P, Wang X-F, Zhou L, Sheng Y-B. Passive decoy state quantum secure direct communication. *Fundam Res*. 2025; https://doi.org/10.1016/j.fmre.2025.12.008
21. Liu C, Zhang C, Gu SP, Wang XF, Zhou L, Sheng YB. Receiver-device-independent quantum secure direct communication. *Sci Chin Phys Mech Astron*. 2025;68:Article 250311.
22. Ding CW, Wang WY, Zhang WD, Zhou L, Sheng YB. Quantum secure direct communication based on quantum error correction code. *Appl Phys Lett*. 2025;126:Article 024002.
23. Pan D, Long GL. Semantic quantum secure direct communication. *AAPPS Bull*. 2026;36:2.
24. Zhou Z, Sheng Y, Niu P, Yin L, Long G, Hanzo L. Measurement-device-independent quantum secure direct communication. *Sci Chin Phys Mech Astron*. 2020;63:Article 230362.
25. Zhou L, Sheng YB, Long GL. Device-independent quantum secure direct communication against collective attacks. *Sci Bull*. 2020;65(1):12–20.
26. Zhou L, Xu BW, Zhong W, Sheng YB. Device-independent quantum secure direct communication with single-photon sources. *Phys Rev Appl*. 2023;19(1):Article 014036.
27. Hu J-Y, Yu B, Jing M-Y, Xiao L-T, Jia S-T, Qin G-Q, Long G-L. Experimental quantum secure direct communication with single photons. *Light Sci Appl*. 2016;5:e16144–e16144.
28. 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.
29. Zhu F, Zhang W, Sheng Y, Huang Y. Experimental long-distance quantum secure direct communication. *Sci Bull*. 2017;62(22):1519–1524.

30. Sun Z, Qi R, Lin Z, Yin L, Long G, Lu J. Design and implementation of a practical quantum secure direct communication system. In: *2018 IEEE Globecom Workshops (GC Wkshps)*. Abu Dhabi (United Arab Emirates): IEEE; 2018. p. 1–6.
31. Qi R, Sun Z, Lin Z, Niu P, Hao W, Song L, Huang Q, Gao J, Yin L, Long G-L. Implementation and security analysis of practical quantum secure direct communication. *Light Sci Appl*. 2019;8:22.
32. Wyner AD. The wire-tap channel. *Bell Syst Tech J*. 1975;54(8):1355–1387.
33. Wu J, Lin Z, Yin L, Long GL. Security of quantum secure direct communication based on Wyner's wiretap channel theory. *Quantum Eng*. 2019;1:Article e26.
34. 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(1):83.
35. 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 Chin Phys Mech Astron*. 2022;65:Article 120311.
36. Pan D, Lin Z, Wu J, Zhang H, Sun Z, Ruan D, Yin L, Long GL. Experimental free-space quantum secure direct communication and its security analysis. *Photon Res*. 2020;8:1522–1531.
37. Long GL, Pan D, Sheng YB, Xue Q, Lu J, Hanzo L. An evolutionary pathway for the quantum internet relying on secure classical repeaters. *IEEE Netw*. 2022;36(3):82–88.
38. Pan D, Liu YC, Niu P, Zhang H, Zhang F, Wang M, Song XT, Chen X, Zheng C, Long GL. Simultaneous transmission of information and key exchange using the same photonic quantum states. *Sci Adv*. 2025;11:Article eadt4627.
39. Yang Y, Li Y, Li H, Wu C, Zheng Y, Chen X. A 300-km fully-connected quantum secure direct communication network. *Sci Bull*. 2025;70(9):1445–1451.
40. Pirandola S, Braunstein SL, Mancini S, Lloyd S. Quantum direct communication with continuous variables. *Europhys Lett*. 2008;84(2):548–551.
41. Meslouhi A, Hassouni Y. A quantum secure direct communication protocol using entangled modified spin coherent states. *Quantum Inf Process*. 2013;12(7):2603–2621.
42. Srikara S, Thapliyal K, Pathak A. Continuous variable direct secure quantum communication using Gaussian states. *Quantum Inf Process*. 2020;19:132.
43. Cao Z, Lu Y, Chai G, Yu H, Liang K, Wang L. Realization of quantum secure direct communication with continuous variable. *Research*. 2023;6:0193.
44. Zuo Z, Liang Z, Mao N, Wang Y, Guo Y. Continuous-variable quantum secure direct communication against dual-sequence Gaussian attacks with quantum memory. *Sci Chin Phys Mech Astron*. 2026;69:Article 240314.
45. Liang S, Cheng J, Qin J, Li J, Shi Y, Yan Z, Jia X, Xie C, Peng K. High-speed quantum radio-frequency-over-light communication. *Phys Rev Lett*. 2024;132(14):Article 140802.
46. Wang L, Chai G, Cao Z, Chen X, Liang K, Peng J. Quantum purification for coherent states and its application. *Sci Chin Phys Mech Astron*. 2025;68:Article 220313.
47. Paparelle I, Mousavi F, Scazza F, Bassi A, Paris M, Zavatta A. Experimental direct quantum communication with squeezed states. *Opt Express*. 2025;33(14):28917–28934.
48. Wang L, Chai G, Cao Z, Chen X. Highly reliable quantum secure direct Communica tion based on concatenated GKP-QLDPC codes. *Sci China Inf Sci*. 2026; https://doi.org/10.1007/s11432-025-4608-6
49. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys Rev Lett*. 2020;125(1):Article 010502.
50. Ghorai S, Diamanti E, Leverrier A. Composable security of two-way continuous-variable quantum key distribution without active symmetrization. *Phys Rev A*. 2019;99(1):Article 012311.
51. Arikan E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans Inf Theory*. 2009;55:3051–3073.
52. Cammerer S, Leible B, Stahl M, Hoydis J, Sten B. Combining belief propagation and successive cancellation list decoding of polar codes on a GPU platform. In: *2017 IEEE international Conference on Acoustics, Speech and Signal Processing (ICASSP)*. New Orleans (LA): IEEE; 2017. p. 3664–3668.
53. Raviv T, Goldman A, Vayner O, Be'ery Y, Shlezinger N. CRC-aided learned ensembles of belief-propagation polar decoders. In: *2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Seoul (Korea): IEEE; 2024. p. 8856–8860.
54. Tal I, Vardy A. List decoding of polar codes. *IEEE Trans Inf Theory*. 2015;61(5):2213–2226.
55. Chai G, Yuan Y, Cao Z, Yu H, Chen X, Peng J. FPGA-based microsystematic design of Gaussian modulation for continuous-variable quantum communication. *Phys Rev Appl*. 2023;20(5):Article 054037.
56. Jia Y, Wang X, Hu X, Hua X, Zhang Y, Guo X, Zhang S, Xiao X, Yu S, Zou J. Silicon photonics-integrated time-domain balanced homodyne detector for quantum tomography and quantum key distribution. *New J Phys*. 2023;25:Article 103030.
57. Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys Rev A*. 2008;77:Article 042325.
58. Grosshans F, Cerf NJ, Wenger J, Tualle-Brouri R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inf Comput*. 2003;3(7):535–552.
59. Wang T, Yu S, Zhang YC, Gu W. A generalized entanglement-based scheme for Gaussian modulated coherent state continuous-variable quantum key distribution. *J Phys B Atomic Mol Phys*. 2015;48(13):Article 135504.
60. Cooper M, Cooper M, Söller C, Smith BJ. High-stability time-domain balanced homodyne detector for ultrafast optical pulse applications. *J Mod Opt*. 2013;60:611–616.
61. Zou M, Mao Y, Chen TY. Rigorous calibration of homodyne detection efficiency for continuous-variable quantum key distribution. *Opt Express*. 2022;30(13):22788–22797.