

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

Zhengwen Cao(曹正文), Yujie Wang(王禹杰), Geng Chai(柴庚)†, Xinlei Chen(陈欣蕾), and Yuan Lu(卢缘)

Citation : Chin. Phys. B, 2025, 34 (**2**): 020308. DOI: 10.1088/1674-1056/ad9ff7
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)

Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

Established conversions for hybrid entangled states assisted by error-predicted parity-discriminated devices

Fang-Fang Du(杜芳芳), Zhi-Guo Fan(范志国), Xue-Mei Ren(任雪梅), Ming Ma(马明), and Wen-Yao Liu(刘文耀)

Chin. Phys. B, 2025, 34 (**1**): 010303. DOI: 10.1088/1674-1056/ad8fa0

Deep-learning-assisted optical communication with discretized state space of structured light

Minyang Zhang(张敏洋), Dong-Xu Chen(陈东旭), Pengxiang Ruan(阮鹏祥), Jun Liu(刘俊), Dong-Zhi Fu(付栋之), Jun-Long Zhao(赵军龙), and Chui-Ping Yang(杨垂平)

Chin. Phys. B, 2024, 33 (**12**): 120304. DOI: 10.1088/1674-1056/ad8553

Realization of quantum permutation algorithm in high dimensional Hilbert space

Dong-Xu Chen(陈东旭), Rui-Feng Liu(刘瑞丰), Pei Zhang(张沛), Yun-Long Wang(王云龙), Hong-Rong Li(李宏荣), Hong Gao(高宏), Fu-Li Li(李福利)

Chin. Phys. B, 2017, 26 (**6**): 060305. DOI: 10.1088/1674-1056/26/6/060305

Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum

Wang Le (王乐), Zhao Sheng-Mei (赵生妹), Gong Long-Yan (巩龙延), Cheng Wei-Wen (程维文)

Chin. Phys. B, 2015, 24 (**12**): 120307. DOI: 10.1088/1674-1056/24/12/120307

SPECIAL TOPIC — Quantum communication and quantum network

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

Zhengwen Cao(曹正文), Yujie Wang(王禹杰), Geng Chai(柴庚)†, Xinlei Chen(陈欣蕾), and Yuan Lu(卢缘)

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

(Received 26 September 2024; revised manuscript received 6 December 2024; accepted manuscript online 17 December 2024)

Quantum secure direct communication (QSDC) is a communication method based on quantum mechanics and it is used to transmit secret messages. Unlike quantum key distribution, secret messages can be transmitted directly on a quantum channel with QSDC. Higher channel capacity and noise suppression capabilities are key to achieving long-distance quantum communication. Here, we report a continuous-variable QSDC scheme based on mask-coding and orbital angular momentum, in which the mask-coding is employed to protect the security of the transmitting messages and to suppress the influence of excess noise. The combination of orbital angular momentum and information block transmission effectively improves the secrecy capacity. In the 800 information blocks $\times$1310 bits length 10-km experiment, the results show a statistical average bit error rate of 0.38%, a system excess noise value of 0.0184 SNU, and a final secrecy capacity of 6.319×10^6 bps. Therefore, this scheme reduces error bits while increasing secrecy capacity, providing a solution for long-distance large-scale quantum communication, which is capable of transmitting text, images and other information of reasonable size.

Keywords: continuous-variable quantum direct communication, orbital angular momentum, mask coding

PACS: 03.67.Hk, 03.67.Bg, 03.67.–a

DOI: 10.1088/1674-1056/ad9ff7 **CSTR:** 32038.14.CPB.ad9ff7

1. Introduction

With the continuous development of science and technology, information security has gradually become the focus of attention. The security of communication systems is seriously threatened by quantum computing and distributed computing. In order to combat the upheaval of the information age and ensure the security of information transmission, communication approaches based on the basic principles of quantum mechanics came into being. The rapid rise of quantum communication has brought more possibilities to our lives.[1] At present, quantum communication mainly includes quantum key distribution (QKD)[2–6] and quantum secure direct communication (QSDC).[7]

Unlike QKD, QSDC, which was proposed in 2000, allows the direct transmission of secret messages rather than keys.[7] This reduces the steps involved in the communication process and the complexity of information transmission while improving efficiency.[8] In early research on QSDC, many relevant protocols[9–11] were developed for different information carriers. A two-step QSDC protocol with an entangled state was proposed by Deng *et al.* in 2003.[12] Its security was verified by comparing the joint statistical results of the first security judgment with the threshold value. Moreover, the DL04 protocol with a single photon was proposed by Long *et al.*,[13] promoting the development of QSDC. They have been proven to provide information-theoretic security and are theoretically feasible. In addition, industry scholars have proposed various QSDC protocols, such as the entangled states protocol,[14,15] the Greenberger–Horne–Zeilinger states protocol,[16,17] the quantum-memory-free QSDC protocol,[18,19] the device-independent QSDC, and the measurement device-independent QSDC protocol.[20–24]

In recent years, quantum direct communication technology has also been experimentally validated, such as in entangled-state and single-photon QSDC experiments,[25,26] which have been reported to verify the principles of QSDC protocols based on a single photon and entanglement. The first QSDC experiment based on long-range entanglement has been reported and the performance of the QSDC system was theoretically analyzed. The results showed that QSDC can be achieved on several hundreds of kilometers of fiber optic links using current optical communication technology, providing a method to extend QSDC to further distances.[27] Long *et al.* reported the implementation of a practical quantum-secure communication system. The system adopted a low-density parity check code serial encoding scheme and operated in high-noise and high-loss real-world environments.[28] In order to push QSDC into practical applications, some critical issues must be addressed. Cao *et al.* reported the continuous variable QSDC experimental demonstration, verifying the feasibility and effectiveness of the communication method in fiber optic channels, and proposed a parameter estimation for sig-

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

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

nal classification in actual channels, laying the foundations for grading reconciliation.[29] Cao *et al.* proposed an improved scheme based on coherent state CV-QSDC, which effectively reduced the system noise to the original 0.58, and improved the safety performance of the system by 43.6%.[30] The two-mode squeezed state entanglement source used in this experiment is a common continuous variable entanglement source. The two-mode squeezed state can be generated with the help of the parameters of spontaneous parameter down conversion. It is a common choice for preparing entanglement sources. Its structure is simple and its cost is low.[8] At the same time, because of the entanglement property of the two-mode squeezed state, any measurement of one mode will affect the other mode. This property can be used to detect potential eavesdropping behavior, thus enhancing the security of communication.

Although QSDC has made significant progress in both theory and engineering, it still needs to be further investigated in terms of engineering implementation and practicality. In order to achieve long-distance quantum communication, communication protocols need to have higher channel capacity and noise suppression capabilities. The multiplexing of orbital angular momentum (OAM) and mask-coding is an effective way to solve this problem. OAM is a basic photon physical quantity, which has great application potential in optical research.[31] Photonic OAM has promising characteristics for realizing multiplexing technology. At present, OAM is often employed in the following aspects: using higher-dimensional Hilbert space to encode information in quantum information processing systems,[32] and as an efficient carrier of information reuse. The OAM state has infinity and orthogonality properties, making it an effective approach to implementing multiplexing technology; it can also effectively increase the capacity of the QSDC protocol. In addition, incorporating mask-coding technology into the protocol can effectively enhance the anti-interference ability of information during transmission.[33–35]

Here, we firstly propose a mask-coding-assisted continuous-variable quantum direct communication method based on OAM multiplexing and verify its feasibility through experiments. According to Wyner's wiretap channel model, the performance of the proposed protocol is analyzed. In our experiment, the hash function is used to mask the secret messages into a random sequence to improve the security of information transmission. Taking advantage of the orthogonality between OAM modes, each mode can be regarded as an independent sub-channel, which changes the information block from serial transmission to parallel transmission and improves the communication capacity of the system. Finally, in the 800 information blocks $\times$1310 bits length 10 km experiment, the results show that the statistical average of the bit error rate reaches 0.38%. The system excess noise is 0.0184 SNU and the final secrecy capacity is 6.319×10^6 bps, fully validating the feasibility of the proposed protocol.

The paper is organized as follows. In Section 2, we provide a detailed introduction to the designed protocol and analyze its performance based on Wyner's model; in Section 3, the experimental results are analyzed based on parameter estimation by building an experimental platform. The conclusion and discussion are presented in Section 4.

2. Protocol and performance analysis

The first part of this section introduces the content of the protocol, as shown in Fig. 1. By combining it with the Wyner's eavesdropping channel model, as shown in Fig. 3, the second part specifically analyzes the improvement brought about by the OAM multiplexing and mask-coding in this protocol.

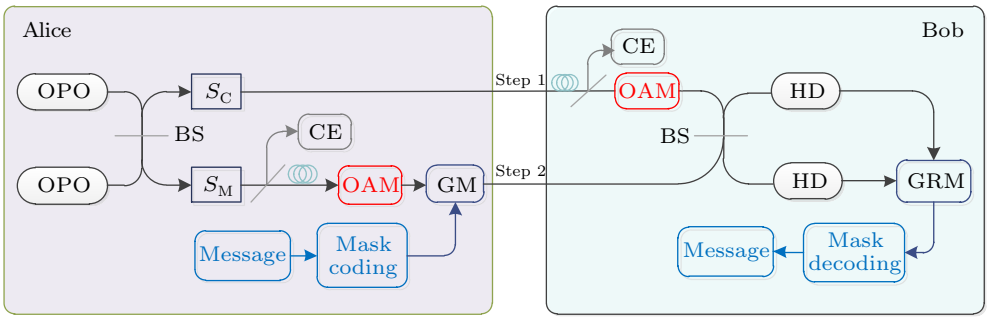


Fig. 1. System diagram of mask-coding-assisted CV-QSDC based on OAM multiplexing. OPO: optical parametric oscillator; BS: beam splitter; S_C: detection light; S_M: signal light; CE: checking eavesdropping; OAM: orbital angular momentum; GM: Gaussian mapping; HD: homodyne detection; GRM: Gaussian remapping.

2.1. Protocol description

Step 1 (preparation of entangled light) In this protocol, Alice uses two-mode compressed light as entangled light. Alice uses a 50:50 beam splitter to couple two single-mode squeezed entangled states to prepare a two-mode squeezed entangled state, which respectively are recorded as S_C (detection light) and S_M (signal light). Alice retains the signal light S_M and sends the detection light S_C after OAM multiplexing to Bob through the quantum channel. Specifically, the quadrature components of the single-mode squeezed states are expressed

as

$$\begin{cases} x_1 = \exp(-r)\,|0\rangle_{x_1}, \quad p_1 = \exp(r)\,|0\rangle_{p_1}, \\ x_2 = \exp(-r)\,|0\rangle_{x_2}, \quad p_2 = \exp(r)\,|0\rangle_{p_2}, \end{cases} \tag{1}$$

where r (>0) is the squeezing factor, x and p denote the quadrature position and quadrature momentum, respectively. $|0\rangle$ denotes the vacuum state. Then quadrature components of the two-mode squeezed entangled state can be expressed as

$$\begin{cases} x_{S_C} = \frac{1}{\sqrt{2}}(x_1 + x_2), \quad p_{S_C} = \frac{1}{\sqrt{2}}(p_1 - p_2), \\ x_{S_M} = \frac{1}{\sqrt{2}}(x_2 - x_1), \quad p_{S_M} = \frac{1}{\sqrt{2}}(p_2 + p_1). \end{cases} \tag{2}$$

Step 2 (channel security detection) Alice divides the detection light S_C and signal light S_M into two parts, a and b, respectively. The preprocessing scheme for entangled light is shown in Fig. 2. Furthermore, b is used for security detection and identity authentication, while a is used for information carrying and measurement. In order to achieve OAM multiplexing of beams, the S_{Ca} is transformed by a group of spatial light modulators (SLMs) with a spiral phase of $\exp(\mathrm{i}l_p\theta)$ to obtain S_{Cai}. Alice performs the same operation on S_{Ma} after channel security detection, identity authentication, and mask-coding:

$$E^{\mathrm{MUX}}_{S_{Cai}}(\boldsymbol{r},\theta,t) = \sum_{p=1}^{N} E_{S_{Cai}}(\boldsymbol{r},t)\exp(\mathrm{i}l_p\theta), \tag{3}$$

where, $E^{\mathrm{MUX}}_{S_{Cai}}(\boldsymbol{r},\theta,t)$ is the quantized light field of S_{Cai}, and $E_{S_{Cai}}(\boldsymbol{r},t)$ is the quantized light field of S_{Cai}. The definition of $E_{S_{Cai}}(\boldsymbol{r},t)$ will be provided in the following text. Alice randomly selects time slots to measure the quadrature components of S_{Mb}, and then tells Bob the selected time slots and measurement results. After receiving the detection light S_C, Bob selects the same time slots as Alice to measure the quadrature components of S_{Cb}, and makes a joint judgment using Alice's measurement results:

$$\left\langle \left[\triangle \left(\frac{x_{mA} \pm x_{mB}}{\sqrt{2}} \right) \right]^2 \right\rangle + \left\langle \left[\triangle \left(\frac{p_{mA} \pm p_{mB}}{\sqrt{2}} \right) \right]^2 \right\rangle \leq 2, \tag{4}$$

where $x(p)_{mA}$ and $x(p)_{mB}$ represent the measurement results of both communication parties. If Bob's measurement results and Alice's measurement results are against Eq. (4), the quantum channel is safe and communication continues; otherwise, the communication is terminated.

Step 3 (identity authentication) Similarly, Bob randomly selects other time slots on the remaining S_{Cb} for measurement, and then sends the time slots and measurement results to Alice. Alice also conducts joint measurement through Eq. (4). The purpose of this phase is for Alice to verify and confirm Bob's identity. If the identity is legitimate, Alice goes to the next step. Otherwise, the communication is terminated.

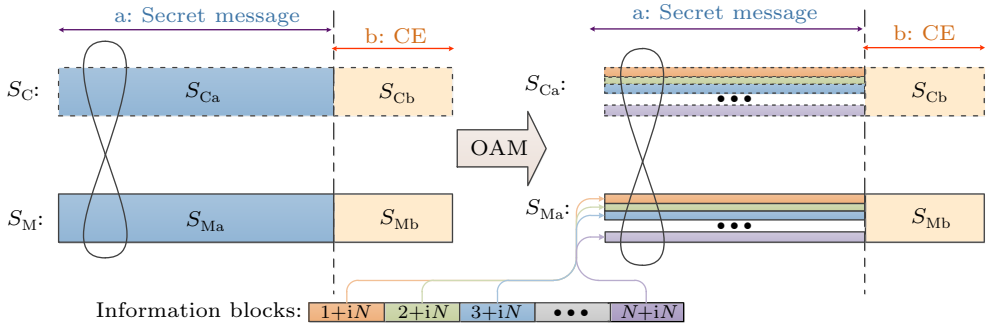


Fig. 2. Preprocessing of entangled light. S_C: detection light; S_M: signal light; the subscript "a" is used for security detection and identity authentication, while the subscript "b" is used for information carrying and measurement; CE: checking eavesdropping; OAM: orbital angular momentum; N: OAM multiplexing modes.

Step 4 (information mask-coding) Alice employs mask-coding to mask the secret messages to obtain a random message sequence M.[36] This protocol takes the hash function cluster designed by the Toeplitz matrix as an example to illustrate the mask-coding:

(i) Alice randomly selects a random code sequence s of length $k+n-1$ and constructs a $k\times n$ binary Toeplitz matrix (where k is the length of the secret messages and n is the length of the masked target). The Toeplitz matrix, also known as a constant quantity matrix, has equal elements on the same diagonal parallel to the main diagonal, each row of the matrix is the result of moving one element to the right relative to the row above it, and the newly added position on the left is filled by another sequence. The $k\times n$ Toeplitz matrix can be represented as follows:[35]

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & \cdots & a_{1,n} \\ a_{1,n} & a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n-1} \\ a_{1,n-1} & a_{1,n} & a_{1,1} & a_{1,2} & \cdots & a_{1,n-2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1,k} & a_{1,k-1} & a_{1,k-2} & a_{1,k-3} & \cdots & a_{1,n-k+1} \end{bmatrix}_{k\times n}. \tag{5}$$

Taking secret message $m=001$, $n=5$ as an example, Alice selects a random number sequence $s = a_1a_2a_3a_4a_5a_6a_7 = 1100100$ and constructs a Toeplitz matrix as follows:

$$T_{oe} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_7 & a_1 & a_2 & a_3 & a_4 \\ a_6 & a_7 & a_1 & a_2 & a_3 \end{bmatrix}_{3\times 5} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}. \tag{6}$$

(ii) Alice transforms the Toeplitz matrix into rows to ob-

tain a standardized matrix

$$T'_{\rm oe} = [A_{T_{\rm oe}}|E] = \left[\begin{array}{cc|ccc} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right]. \tag{7}$$

Among them, the sub-matrix $A_{T_{\rm oe}}$ and the randomized redundant sequence $R_{\rm oe} = [1\ 0]^{\rm T}$ are used to construct the matrix $[R_{\rm oe}\ \ m - A_{T_{\rm oe}} R_{\rm oe}]^{\rm T}$, as shown in Eq. (8), and then the masked message sequence $M = 10000$ is obtained,

$$M = \left[\begin{array}{c} R_{\rm oe} \\ m - A_{T_{\rm oe}} R_{\rm oe} \end{array}\right] = \left[\begin{array}{c} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{array}\right] = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{8}$$

(iii) Alice sends Bob the starting digit of the random sequence s used through the classic authentic channel after demultiplexing and measurement, so that Alice and Bob share the same hash function to assist Bob in extracting secret information.

Step 5 (Gaussian mapping) Alice first unifies the mask message sequence M to obtain a balanced sequence M', so that the sequence M' has a stable uniform distribution.[37] Then the balanced sequence is mapped to a set of Gaussian random numbers with zero mean and variance $V_{\rm a}$. This protocol takes each information block containing 3 bits as an example,[38] and the Gaussian random number is divided into 8 intervals according to the principle of equal probability. The corresponding Gaussian intervals are $[-7,-3.25]$, $(-3.25,-1.91]$, $(-1.91,-0.90]$, $(-0.90,0]$, $(0,0.90]$, $(0.90,1.91]$, $(1.91,3.25]$, $(3.25,+7]$, and the eight intervals from left to right correspond to 000 to 111 of a 3-bit binary string.

Step 6 (information multiplexing) Alice generates OAM signal lights with different modes $\{S_{{\rm Ma}i}|i = 1,2,\ldots,N\}$ from signal light $S_{\rm Ma}$ through spatial light modulators,[39] and groups the information blocks according to OAM's modes N. Each information block is modulated on the quadrature component (x or p) of $S_{{\rm Ma}i}$ in order to obtain the final information beam $S_{\rm info}$, as shown in the Fig. 2. Specifically, the quantized light field of the signal light $S_{{\rm Ma}i}$ can be expressed as

$$E_{S_{{\rm Ma}i}}(\boldsymbol{r},t) = K \times {\rm i}\left[a\,{\rm e}^{-{\rm i}(\omega t - \boldsymbol{k}\cdot\boldsymbol{r})} - a^{\dagger}\,{\rm e}^{{\rm i}(\omega t - \boldsymbol{k}\cdot\boldsymbol{r})}\right], \tag{9}$$

where $K = \left(\frac{\hbar\omega}{2\varepsilon_0 V}\right)^{1/2}$ and $\hbar$ is the Planck constant. ε_0 is the dielectric constant, ω is the angular frequency, $\boldsymbol{k}$ represents the wave number and $\boldsymbol{r}$ represents the wave vector. a and $a^{\dagger}$ represent the generation operator and the annihilation operator, respectively. The quantized light field of the OAM beam generated by Alice is represented as

$$E^{\rm MUX}_{S_{{\rm Ma}i}}(\boldsymbol{r},\theta,t) = \sum_{p=1}^{N} E_{S_{{\rm Ma}i}}(\boldsymbol{r},t) \times \exp({\rm i}l_p\theta), \tag{10}$$

where l_p represents the topological charge of OAM beam, and N is the number of modes used for multiplexing. The quantized light field of the final signal light beam $S_{\rm info}$ generated by Alice is represented as

$$\begin{aligned} E_{S_{\rm info}}(\boldsymbol{r},\theta,t) &= E^{\rm MUX}_{S_{{\rm Ma}i}}(\boldsymbol{r},\theta,t)\exp\left({\rm i}\frac{\pi V_{\rm b}}{V_\pi}\right) \\ &\quad\times\exp\left[{\rm i}\sum_{p=1}^{N}\frac{\pi A_p}{V_\pi}\cos(\omega_k t+\phi_p)\right] \\ &= E^{A_p}\left\{\hat{a}_A\exp\left[{\rm i}\left(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t\right)\right]\right. \\ &\quad\left.+\hat{a}_A^{\dagger}\exp\left[-{\rm i}\left(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t\right)\right]\right\}, \end{aligned} \tag{11}$$

where $V_{\rm b}$ represents the bias voltage of the amplitude modulator, V_π represents the half-wave voltage of the phase modulator, A_p represents a random number obeying Rayleigh distribution for amplitude modulation, ϕ_p represents a uniformly distributed random number for phase modulation and $\hat{a}_A$ represents the dimensionless complex amplitude operator after Gaussian modulation.

Step 7 (demultiplexing and measurement) After receiving the signal light $S'_{\rm info}$ (after channel transmission), Bob separates N OAM beams of $S'_{{\rm Ca}i}$ from the detection light $S'_{\rm C}$ (after channel transmission), and separates the N OAM beams signal light $S'_{{\rm Ma}i}$ from $S'_{\rm info}$. The detection light $S'_{{\rm C}i}$ with the same mode OAM signal light $S'_{{\rm M}i}$ can be measured and recovered to a Gaussian plane light from the spiral phase. After passing through the quantum channel, the optical light of the detection light and signal light received by Bob are

$$\begin{cases} E^{\rm Bob}_{S'_{\rm C}}(t) = E_{S_{\rm C}}\cdot\exp({\rm i}\phi), \\ E^{\rm Bob}_{S'_{\rm info}}(t) = E_{S_{\rm info}}\cdot\exp({\rm i}\phi), \end{cases} \tag{12}$$

where $\exp({\rm i}\phi)$ represents the evolution of channel transmission.[39] Bob performs CV Bell detection on the detection light and signal light, and the measurement results can be written as

$$I^{l_q} \propto \int_0^{+\infty}\int_0^{2\pi}\left|E^{\rm MUX}_{S'_{{\rm Ma}i}} + \left[E^{\rm MUX}_{S'_{{\rm Ca}i}}\right]^{*}\right|^2 \boldsymbol{r}\,{\rm d}\boldsymbol{r}\,{\rm d}\theta, \tag{13}$$

where $*$ represents conjugate transformation. The result after removing the direct-current component can be expressed as

$$\begin{aligned} I^{l_p} &= {\rm Re}\left\{\int_0^{+\infty}\int_0^{2\pi} E^{\rm MUX}_{S'_{{\rm Ma}i}} + \left[E^{\rm MUX}_{S'_{{\rm Ca}i}}\right]^{*}\boldsymbol{r}\,{\rm d}\boldsymbol{r}\,{\rm d}\theta\right\} \\ &= {\rm Re}\left\{\int_0^{+\infty}\int_0^{2\pi}\left[\sum_{p=1}^{N} E_{S'_{{\rm Ma}i(p)}}\exp({\rm i}l_q\theta)\right]\right. \\ &\quad\left.\times E_{S'_{{\rm Ca}i}}\exp(-{\rm i}l_q\theta)\boldsymbol{r}\,{\rm d}\boldsymbol{r}\,{\rm d}\theta\right\}. \end{aligned} \tag{14}$$

In addition, different modes of OAM light satisfy orthogonal characteristics, and only vortex light with the same mode

can be successfully demultiplexed and measured during detection. The joint measurement result is represented as

$$\begin{cases} x_{\mathrm{m}} = \frac{1}{\sqrt{2}}\left(x'_{S'_{\mathrm{Mai}}} - x'_{S'_{\mathrm{Cai}}}\right), \\ p_{\mathrm{m}} = \frac{1}{\sqrt{2}}\left(p'_{S'_{\mathrm{Mai}}} + p'_{S'_{\mathrm{Cai}}}\right). \end{cases} \tag{15}$$

Step 8 (information extraction) Bob then remaps the measured results through information reconciliation to obtain the masked message sequence. Alice sends the description sequence s of the hash function to Bob. Subsequently, Bob uses sequence s to perform mask-decoding on the masked message sequence. Corresponding to step 4, the original secret message $m = 001$ can be obtained. At this point, the communication between the two parties ends.

$$m = T'_{\mathrm{oe}}M = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}. \tag{16}$$

2.2. System performance analysis

The channel with eavesdroppers is called the eavesdropping channel, and the secrecy capacity is the maximum secure transmission rate between Alice and Bob. According to the communication model in Wyner's wiretap channel theory,[40] as shown in Fig. 3, the difference between the main channel capacity and the eavesdropping channel capacity in Wyner's wiretap channel model is defined as the secrecy capacity between the two communication parties:

$$\begin{aligned} C_{\mathrm{s}} &\geq Q_{\mathrm{B}}[2 - h_4(e)] - Q_{\mathrm{E}}\left[h(\epsilon_x) + h(\epsilon_z)\right] \xrightarrow{\mathrm{def}} C_{\mathrm{M}} - C_{\mathrm{W}} \\ &= Q_{\mathrm{B}} I_{\mathrm{AB}} - Q_{\mathrm{E}}\chi_{\mathrm{BE}}, \end{aligned} \tag{17}$$

where C_{s} represents the secrecy capacity, C_{M} represents the main channel capacity, C_{W} represents the eavesdropping channel capacity, I_{AB} represents the amount of mutual information between Alice and Bob,[41] and χ_{BE} represents the Holevo bound that eavesdropper Eve can obtain. Q_{B} is the reception rate of Bob, Q_{E} is the maximum rate Eve can access the qubits. The secrecy capacity with orbital angular momentum multiplexing can be calculated as

$$C_{\mathrm{s}}^{\mathrm{MUX}} = \sum_{n=1}^{N}\left(C_{\mathrm{M}n} - C_{\mathrm{W}n}\right) = \sum_{n=1}^{N}\left(Q_{\mathrm{B}n} I_{\mathrm{AB}n} - Q_{\mathrm{E}n}\chi_{\mathrm{BE}n}\right), \tag{18}$$

where N is the number of OAM modes. Taking the measurement of quantum signals using CV Bell detection as an example, I_{AB} can be represented as

$$I_{\mathrm{AB}} = 2 \times \frac{1}{2}\log_2\left(\frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}}\right) = \log_2\left(\frac{V + \chi_{\mathrm{tot}}}{1 + \chi_{\mathrm{tot}}}\right), \tag{19}$$

where $V = V_{\mathrm{a}} + 1$, $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + (\chi_{\mathrm{h}}/T)$ represents the total noise, $\chi_{\mathrm{line}} = 1/T - 1 + \varepsilon$ represents the linear noise present in the channel, and $\chi_{\mathrm{h}} = 2(1 + v_{\mathrm{el}})/\eta - 1$ represents the detection noise from CV Bell detection, wherein v_{el} represents the electrical noise and η represents the detection efficiency. Moreover χ_{BE} can be represented as

$$\chi_{\mathrm{BE}} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{20}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$. λ_i is the symplectic eigenvalue calculated according to the covariance matrix corresponding to the quantum state ρ_{AB}, ρ_{EF}, ρ_{AFG} at each stage, which can be obtained from

$$\begin{cases} \lambda_{1,2} = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \\ \lambda_{3,4} = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right], \\ \lambda_5 = 1, \end{cases} \tag{21}$$

where

$$\begin{cases} A = V^2(1-2T) + 2T + T^2(V + \chi_{\mathrm{line}}), \\ B = T^2(V\chi_{\mathrm{line}} + 1)^2, \\ C = \frac{A\chi_{\mathrm{het}}^2 + B + 1 + 2\chi_{\mathrm{het}}(V\sqrt{B} + T(V + \chi_{\mathrm{line}})) + 2T(V^2 - 1)}{T^2(V + \chi_{\mathrm{tot}})^2}, \\ D = \frac{(V + \sqrt{B}\chi_{\mathrm{het}})^2}{T^2(V + \chi_{\mathrm{tot}})^2}. \end{cases} \tag{22}$$

Then we can get the system performance of Gaussian mapping CV-QSDC based on OAM and mask-coding when the eavesdropper attacks the communication system with a collective attack. Four modes of OAM beams are selected in this protocol, and the secrecy capacity can be expressed as $C_{\mathrm{s}}^{\mathrm{MUX}} = \sum_{n=1}^{4}\left(Q_{\mathrm{B}n} I_{\mathrm{AB}n} - Q_{\mathrm{E}n}\chi_{\mathrm{BE}n}\right)$.

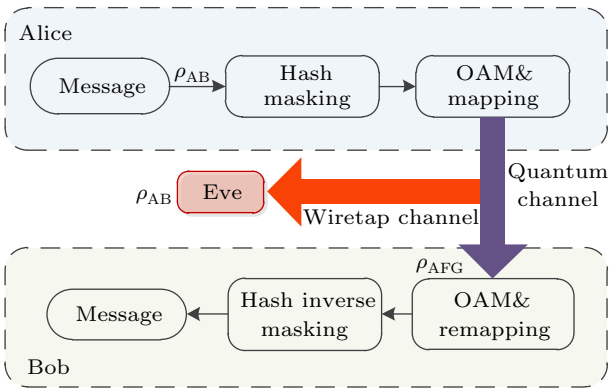


Fig. 3. Wyner's wiretap channel model. Quantum channel: main channel between Alice and Bob; wiretap channel: eavesdropping channel of Eve; OAM: orbital angular momentum; ρ_{AB}: initial state between Alice and Bob; ρ_{EF}: auxiliary state of Eve; ρ_{AFG}: receiving state after eavesdropping and interference.

In combination with Subsection 2.2, the relationship between secrecy capacity and transmission distance is calculated for different Q_{B} and Q_{E}. According to Fig. 4, in different transmission environments, this scheme can improve system performance as compared with existing schemes. On the other hand, under the same multiplexing conditions, the lower the

system error rate, the more significant the performance improvement effect of this scheme. Furthermore, in this scheme, mask-coding is used to protect the transmission security of massages and resist the influence of channel noise. The combination of orbital angular momentum and information block transmission can effectively improve system performance.

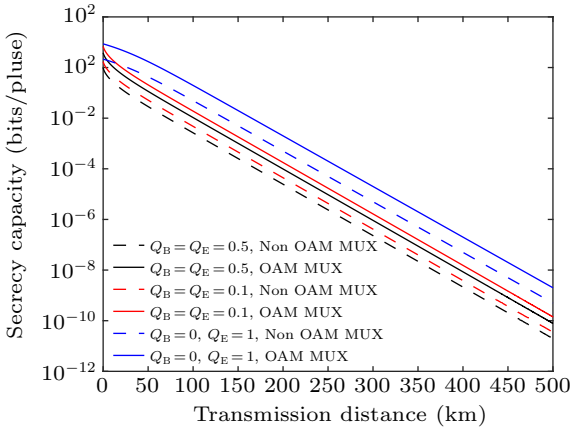


Fig. 4. Secrecy capacity. The dotted line indicates the secrecy capacity without orbital angular momentum multiplexing under different Q_B and Q_E, and the solid line indicates the secrecy capacity with orbital angular momentum multiplexing under different Q_B and Q_E.

3. Experimental analysis

This section introduces the experimental analysis of the proposed scheme. First of all, the set-up of the experimental platform is introduced. Then, the parameters of the experimental data are estimated, and the results finally are analyzed to draw a conclusion.

3.1. Experiment implementation

This protocol requires the multiplexing of four OAM modes, and the experimental platform setup is shown in Fig. 4. In this experiment, we divide the information block into four parts and estimate the parameters of the 800-blocks data results, and based on the measurement results, the core parameters of the system are estimated to evaluate the effectiveness of the experiment.

Alice employs a commercial frequency-stabilized 1550 nm wavelength continuous-wave (CW) laser with 150 kHz linewidth as the signal laser, and uses a customized 10 GHz lithium niobate electro-optic amplitude modulator to transform the CW light into an optical pulse train with 2 ns pulse width and at a repetition rate of 50 MHz. The NOPA cavity consists of two flat concave mirrors with a radius of curvature of 30 mm. A type-II KTP crystal is placed in the center of the cavity, and the cavity bandwidth is 28 MHz.[42] Then, Alice prepares a two-mode squeezed entangled state by passing an optical pulse through a non-degenerate optical parametric amplifier, one as signal light and another as detection light. After that, the detection light is sent to Bob after passing a variable optical attenuator.[43] After the signal light is adjusted through the optical fiber delay line, it is divided into four ways through a three-component beam splitter. Alice preprocesses the secret messages according to Subsection 2.1 and rotates the four modulated signal lights through spatial light modulators to four orthogonal OAMs, and then sends them to Bob after a multiplexer. The introduction of optical devices to modulate the compressed light will not cause the compression to disappear, but the entanglement property will still exist if compression occurs. The entanglement form of the two-mode compressed light after passing through each optical device is given in Ref. [44].

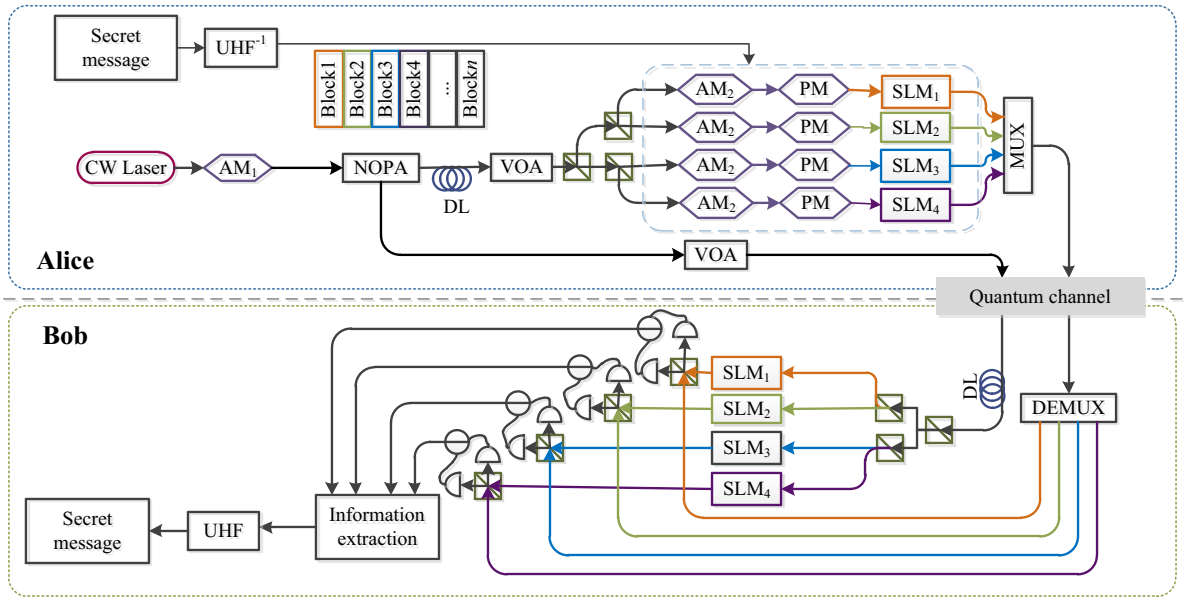


Fig. 5. Experiment setup. CW, 1550 nm continuous wave light source; UHF, hash forward transformation; DL, fiber optic delay line; AM, amplitude modulator; PM, phase modulator; VOA, variable optical attenuator; Block$i$, the information block after partitioning; NOPA, non degenerate optical parametric amplifier; SLMi, spatial light modulator; MUX, OAM multiplexing; DEMUX, OAM demultiplexing.

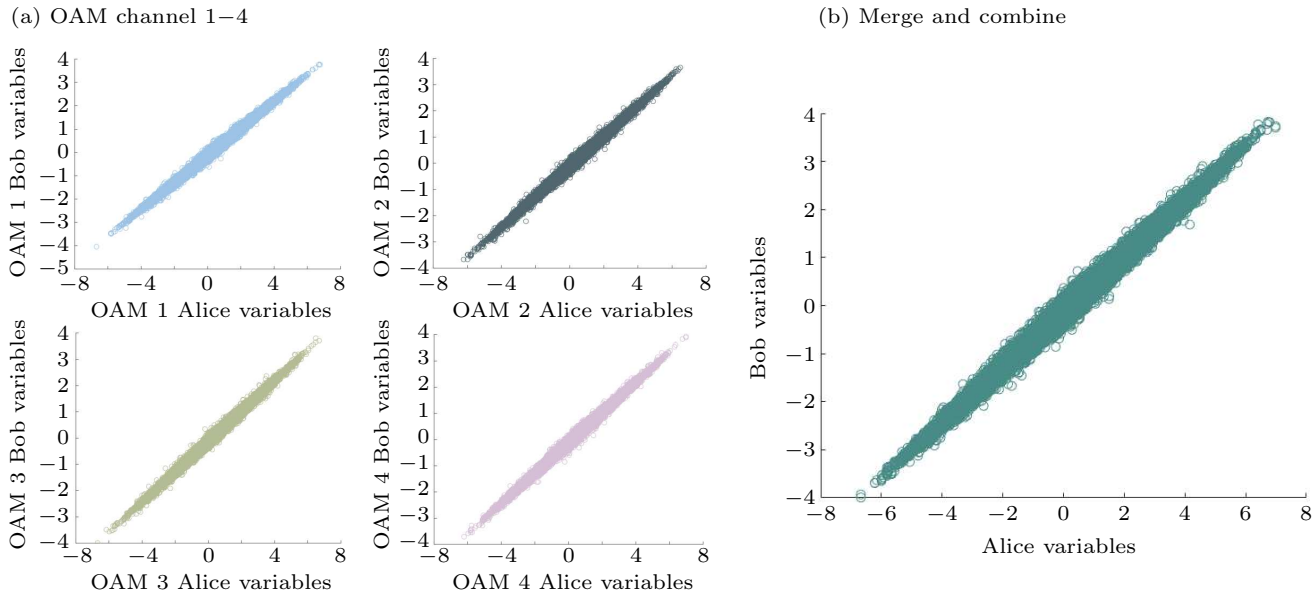


Fig. 6. Autocorrelation analysis results of four-channel multiplexing OAM data. Panel (a) shows the cross-correlation analysis results of each OAM channel, and panel (b) shows the cross-correlation analysis result of all data obtained after merging the four-channel data.

Bob receives two lights passing through 10 km quantum channel. Concretely speaking, Bob receives the detection light and then processes it through the same three-component beam splitter and spatial light modulators as Alice for subsequent CV Bell detection. When Bob receives the modulated signal light, it is demultiplexed to be combined with the detection light for CV Bell measurement. Finally, the messages after demultiplexing and measuring are extracted and the whole experimental process is completed.

The correlation between the data of the four OAM modes and the overall data is shown in Fig. 6, and the estimated parameters are shown in Table 1. From Fig. 5, it can be seen that the correlation of each OAM channel tends to be consistent, consistent with the overall data correlation, and does not affect the overall correlation, which verifies the effectiveness and feasibility of the experiment. According to Table 1, the estimated results of the system parameters are consistent with the data correlation in Fig. 5, which verifies the feasibility of using orbital angular momentum multiplexing in quantum communication.

Table 1. Parameter estimation results of the experimental variable.

Parameter\Channels	OAM 1	OAM 2	OAM 3	OAM 4	MUX channel
$\hat{T}$	0.6273	0.6284	0.6271	0.6274	0.6275
$\hat{\varepsilon}$ (SNU)	0.0184	0.0184	0.0184	0.0184	0.0184

3.2. Parameter estimation

This section performs parameter estimation on the variable after passing through the channel to ensure the validity of experimental data, and to estimate the information obtained by Alice and Bob with the help of calculating the error rate of this experiment. In parameter estimations, it is necessary to obtain the confidence interval. Here, we introduce the normal model[45,46] of Alice and Bob's variables:

$$y = tx + z, \tag{23}$$

where $t = \sqrt{\eta T} \in R$. z follows the normal distribution of variance $\sigma^2 = N_0 + \eta T\varepsilon + v_{\mathrm{el}}$. Similar to the analysis in Ref. [46], the maximum-likelihood estimator $\hat{t}$, $\hat{\sigma}^2$ and $\hat{\sigma}_0^2$ can be calculated according to the following equation:

$$\begin{cases} \hat{t} = \frac{\sum_{i=1}^{\mathcal{N}} x_i y_i}{\sum_{i=1}^{\mathcal{N}} x_i^2}, \ \hat{\sigma}^2 = \frac{1}{\mathcal{N}} \sum_{i=1}^{\mathcal{N}} (y_i - \hat{t}x_i)^2, \\ \hat{\sigma}_0^2 = \frac{1}{\mathcal{N}'} \sum_{i=1}^{\mathcal{N}'} y_{0i}^2, \ \hat{V}_{\mathrm{a}} = \frac{1}{\mathcal{N}} \sum_{i=1}^{\mathcal{N}} x_i^2. \end{cases} \tag{24}$$

These estimators are independent and satisfy the following distribution:

$$\begin{cases} \hat{t} \sim N\left(t, \frac{\sigma^2}{\sum_{i=1}^{N} x_i^2}\right), \\ \frac{\mathcal{N}\hat{\sigma}^2}{\sigma^2}, \ \frac{\mathcal{N}'\hat{\sigma}_0^2}{\sigma_0^2}, \ \frac{\mathcal{N}\hat{V}_{\mathrm{a}}}{V_{\mathrm{a}}} \sim \chi^2(m-1). \end{cases} \tag{25}$$

From this, the confidence intervals of these parameters can be calculated as

$$\begin{cases} t \in [\hat{t} - \Delta t, \hat{t} + \Delta t], \\ \sigma^2 \in \left[\hat{\sigma}^2 - \Delta\sigma^2, \hat{\sigma}^2 + \Delta\sigma^2\right], \\ \sigma_0^2 \in \left[\hat{\sigma}_0^2 - \Delta\sigma_0^2, \hat{\sigma}_0^2 + \Delta\sigma_0^2\right], \\ V_{\mathrm{a}} \in \left[\hat{V}_{\mathrm{a}} - \Delta V_{\mathrm{a}}, \hat{V}_{\mathrm{a}}^2 + \Delta V_{\mathrm{a}}\right], \end{cases} \tag{26}$$

where

$$\begin{cases} \Delta t = z_{\varepsilon_{\mathrm{PE}}/2} \sqrt{\frac{\hat{\sigma}^2}{m V_{\mathrm{a}}}}, \ \Delta\sigma^2 = z_{\varepsilon_{\mathrm{PE}}/2} \frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \\ \Delta V_{\mathrm{a}} = z_{\varepsilon_{\mathrm{PE}}/2} \frac{\hat{V}_{\mathrm{a}}^2\sqrt{2}}{\sqrt{N}}, \ \Delta\sigma_0^2 = z_{\varepsilon_{\mathrm{PE}}/2} \frac{\hat{\sigma}_0^2\sqrt{2}}{\sqrt{N'}}, \end{cases} \tag{27}$$

wherein parameter $z_{\varepsilon_{\mathrm{PE}}/2}$ satisfies the following relationship:

$$\begin{cases} 1 - \mathrm{erf}\left(\frac{z_{\varepsilon_{\mathrm{PE}}/2}}{\sqrt{2}}\right) = \frac{\varepsilon_{\mathrm{PE}}}{2}, \\ \mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp\left(-\tau^2\right) \mathrm{d}\tau. \end{cases} \tag{28}$$

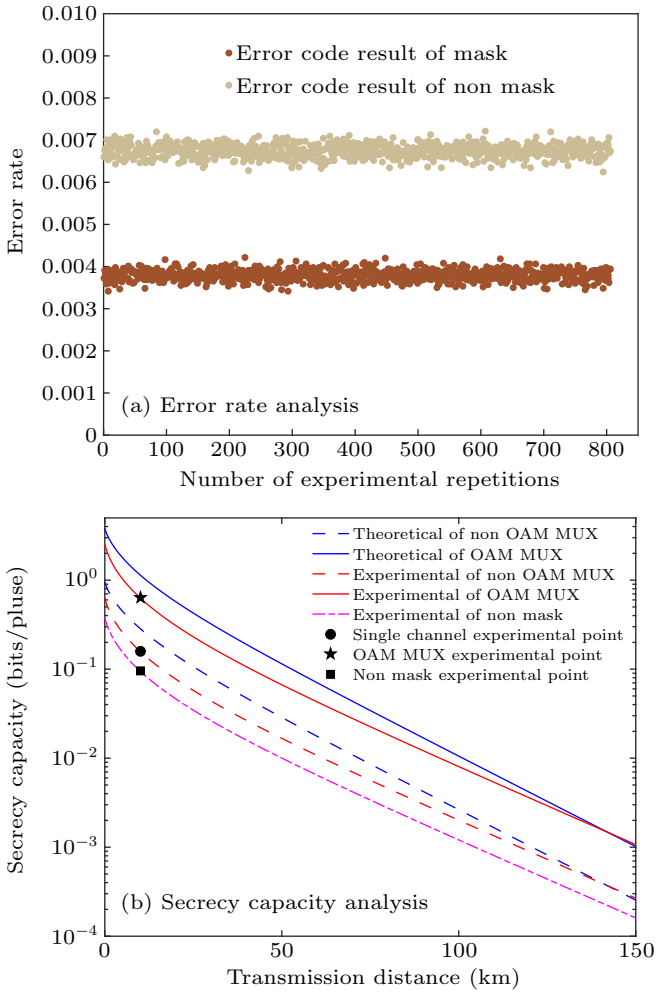


Fig. 7. Results analysis. Panel (a) shows the estimated bit error rate of more than 800 groups of different secret information transmitted by the proposed protocol, and the light colors represent results obtained without masking operations under the same conditions, in which the efficiency of the detector is 0.5. In panel (b), the blue line indicates the amount of mutual information between Alice and Bob, and the red line indicates the amount of mutual information with eavesdroppers; the dotted line indicates the result without OAM multiplexing, and the solid line indicates the results after OAM multiplexing; the dotted dashed line indicates the results without OAM multiplexing and masking; the "⋆" mark refers to the results obtained through experiments, and the "●" mark refers to the results obtained without reuse under the same conditions, the "■" mark refers to the results obtained without reuse and mask under the same conditions.

The system error rate results for masked message extraction are shown in Fig. 7(a). It can be seen that the error rate of the experimental system remains stable, with an average of 0.0038. Compared with the results of similar schemes,[28] the average error rate is about 0.60% at a distance of 1.5 km; we can achieve a longer transmission distance with the same order of error rate. This verifies that mask-coding can be used to protect the transmission security of information in the channel and resist the influence of channel noise, further reflecting the stability and feasibility of the experimental system.

Based on the parameter estimation results in Fig. 6 and Table 1, as well as the transmission error rate in Fig. 7(a), the relationship between system transmission distance and secrecy capacity is shown in Fig. 7(b). The four curves in Fig. 7(b) represent the theoretical value of multiplexing, experimental value of multiplexing, single-channel theoretical value, and single-channel experimental value from top to bottom, respectively. At the same distance, this scheme has a significant improvement in secrecy capacity compared to existing schemes, which is determined by the quanta of observable orbital angular momentum in the experiment. At the same time, there is a certain gap between the experimental value and the theoretical value; this gap is caused by channel errors. In future, further research can be conducted on quantum state oriented coding and decoding techniques to reduce transmission errors and further improve system performance.

4. Discussion and conclusion

Based on a QSDC scheme from the perspective of both protocol and experiment, in terms of ensuring the security and performance of the protocol, the combination of mask-coding technology and orbital angular momentum multiplexing not only improves the security capacity of the system, but also effectively combats the impact of channel noise and eavesdropping. The experimental results show that in the transmission of 800 information blocks $\times 1310$ bits length, the statistical average of the bit error rate for this scheme is 0.38%, the system excess noise is 0.0184 SNU, and the final security capacity is 6.319×10^6 bps. Therefore, the proposed protocol ensures that legitimate parties can obtain more confidential information while improving both security and transmission efficiency. The research on the actual security of the protocol will further optimize our protocol and address more complex communication environments, which will be the focus of our work in the future. Therefore, the proposed protocol will further enrich QSDC technology and promote the implementation of practical QSDC systems.

Acknowledgments

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

References

[1] Pirandola S, Andersen U L, Banchi L, *et al.* 2020 *Advances in Optics and Photonics* **12** 1012
[2] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[3] Cao Z W, Chen X L, Chai G, Liang K X and Yuan Y 2023 *Phys. Rev. Applied* **19** 044023
[4] Jouguet P, Kunz-Jacques S, Diamanti E, *et al.* 2012 *Phys. Rev. A* **86** 032309

[5] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575
[6] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[7] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[8] Pan D, Long G L, Yin L, *et al*. 2024 *IEEE Communications Surveys & Tutorials* **26** 1898
[9] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *J. Phys. A: Math. Gen.* **35** L407
[10] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2001 arXiv:quant-ph/0111106 [quant-ph]
[11] Cai Q Y and Li B W 2004 *Phys. Rev. A* **69** 054301
[12] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[13] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[14] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[15] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[16] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[17] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 *Phys. Lett. A* **354** 67
[18] Sun Z, Qi R, Lin Z, Yin L, Long G and Lu J 2018 *IEEE Globecom Workshops (GC Wkshps)*, December 09-13, 2018, Abu Dhabi, United Arab Emirates, p. 1
[19] Sun Z, Song L, Huang Q, *et al*. 2020 *IEEE Transactions on Communications* **68** 5778
[20] Zhou L, Sheng Y B and Long G L 2020 *Science Bulletin* **65** 12
[21] Zhou L, Xu B W, Zhong W, *et al*. 2023 *Phys. Rev. Applied* **19** 014036
[22] Zhou Z R, Sheng Y B, Niu P H, *et al*. 2020 *Sci. China Phys. Mech. Astron.* **63** 230362
[23] Yan Y F, Zhou L, Zhong W and Sheng Y B 2021 *Front. Phys.* **16** 11501
[24] Hong Y P, Zhou L, Zhong W, *et al*. 2023 *Quantum Inf. Process* **22** 111
[25] Zhou L, Xu B W, Zhong W and Sheng Y B 2023 *Phys. Rev. Applied* **19** 014036
[26] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[27] Zhu F, Zhang W, Sheng Y and Huang Y 2017 *Science Bulletin* **62** 1519
[28] Qi R Y, Sun Z, Lin Z S, *et al*. 2019 *Light Sci. Appl.* **8** 22
[29] Cao Z, Lu Y, Chai G, Yu H, Liang K X and Wang L 2023 *Research* **6** 0193
[30] Wang L, Chai G, Cao Z W and Chen X L 2025 *Sci. China Phys. Mech. Astron.* **68** 220313
[31] Allen L, Beijersbergen M W, Spreeuw R J C and Woerdman J P 1992 *Phys. Rev. A* **45** 8185
[32] Mafu M, Dudley A, Goyal S, *et al*. 2013 *Phys. Rev. A* **88** 032305
[33] Cheng W, Guilley S and Danger J L 2022 *IEEE Transactions on Information Forensics and Security* **17** 1624
[34] Cao Z W, Chen X L, Chai G and Peng J Y 2023 *Laser Phys. Lett.* **20** 045201
[35] Li D, Huang P, Zhou Y, *et al*. 2018 *IEEE Photonics Journal* **10** 1
[36] Long G L and Zhang H 2021 *Science Bulletin* **13** 1267
[37] Srikara S, Thapliyal K and Pathak A 2020 *Quantum Inf. Process* **19** 132
[38] Cao Z, Wang L, Liang K, Chai G and Peng J Y 2021 *Phys. Rev. Applied* **16** 024012
[39] Jin D, Guo Y, Wang Y J and Huang D 2020 *J. Appl. Phys.* **127** 213102
[40] Liang K X, Cao Z W, Chen X L, Wang L, Chai G and Peng J Y 2023 *Front. Phys.* **18** 51301
[41] Wu J W, Lin Z S, Yin L G and Long G L 2019 *Quantum Engineering* **1** 51301
[42] Yan Z H, Jia X J, Su X L, Duan Z Y, Xie C D and Peng K C 2005 *Phys. Rev. A* **85** 040305(R)
[43] Chai G, Yuan Y, Cao Z W, Yu H, Chen X L and Peng J Y 2023 *Phys. Rev. Applied* **20** 054037
[44] Rendell R W and Rajagopal A K 2005 *Phys. Rev. A* **72** 012330
[45] Jouguet P, Kunz-Jacques S, Diamanti E and Leverrier A 2012 *Phys. Rev. A* **86** 032309
[46] Chai G, Liang K X, Liu W Q, Huang P, Cao Z W and Zeng G H 2019 *Int. J. Theor. Phys.* **5** 3746