SCIENCE CHINA
Information Sciences

• LETTER •

July 2026, Vol. 69, Iss. 7, 179403:1–179403:2
https://doi.org/10.1007/s11432-025-4608-6

Highly reliable quantum secure direct communication based on concatenated GKP-QLDPC codes

Lei WANG, Geng CHAI*, Zhengwen CAO* & Xinlei CHEN

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

Received 12 March 2025/Revised 30 June 2025/Accepted 18 September 2025/Published online 27 April 2026

Citation Wang L, Chai G, Cao Z W, et al. Highly reliable quantum secure direct communication based on concatenated GKP-QLDPC codes. Sci China Inf Sci, 2026, 69(7): 179403, https://doi.org/10.1007/s11432-025-4608-6

Communication security requires sufficient updates to counter the threat of quantum technologies in the new era of quantum computing. Quantum secure direct communication (QSDC) as a robust candidate is able to withstand various attacks under infinite computational resources and enable the near-instantaneous delivery of secret messages without key management [1]. Existing research on QSDC shows that methods to improve the secrecy capacity cannot simultaneously address the requirements of noise suppression and transmission reliability. Quantum error correction (QEC) techniques utilize the redundancy of entanglement between multiple physical qubits to encode a logical state that can correct the errors of qubits. In particular, the concatenated bosonic encoding architecture formed by Gottesman-Kitaev-Preskill (GKP) codes [2] as inner layer codes and DV quantum codes, such as repetition codes and surface codes [3], as outer layer codes, is conducive to fault-tolerant quantum computation and long-distance quantum communication. However, surface codes fail to satisfy a linear relation between the distance and the number of physical qubits and lead to a poor code rate, which means more consumption of quantum resources and lower actual communication efficiency.

In this study, we propose a QSDC protocol based on the GKP code and quantum low-density parity-check (QLDPC) codes to tackle noise and eavesdropping interferences and achieve highly reliable message transmission. The properties of stabilizer codes are exploited to illustrate the processes of state preparation, quantum encoding, and decoding in the form of quantum circuits. In the decoding process, the outer decoder employs the min-sum iterative decoding algorithm on the QLDPC code combined with the syndromes provided by the inner GKP code for error correction. The secrecy capacity of the protocol is evaluated through the wiretap channel theory, whose required channel parameters are acquired through the numerical Monte Carlo simulation of the QEC. Additionally, due to the excellent performance of the GKP-QLDPC code, the proposed protocol exhibits benefits with regard to resource consumption and communication efficiency.

QSDC protocol. The block diagram of the QSDC protocol based on cascaded GKP-QLDPC codes is visualized as shown in Figure 1. The designed QSDC protocol utilizes two non-orthogonal GKP states, Z-basis states $\{|0\rangle_{\rm GKP}, |1\rangle_{\rm GKP}\}$ for delivering messages and X-basis states $\{|+\rangle_{\rm GKP}, |-\rangle_{\rm GKP}\}$ for eavesdropping detection. Based on QLDPC codes $[\![n, k, d]\!]$ [4], the transmission of n Z-basis states is referred to as message rounds, and the transmission of n X-basis states is referred to as detection rounds. The properties of GKP codes and QLDPC codes can be found in Appendix A. The detailed procedures of the protocol are described as follows.

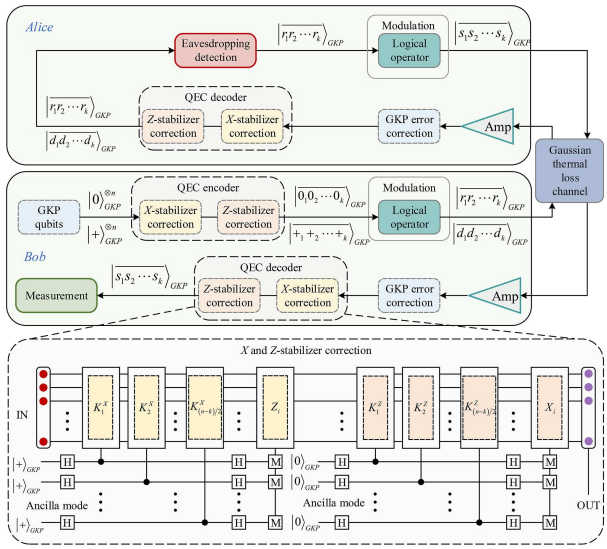

Figure 1 (Color online) The block diagram of QSDC protocol based on cascaded GKP-QLDPC codes. Amp, quantum-limited optical amplifier. The panel below is the quantum circuit diagram for encoding and decoding in quantum error correction codes. H, Hadamard gate; M, measurement.

(a) Preparation and encoding. Bob randomly selects message rounds and detection rounds with corresponding probabilities p_z and p_x, respectively, and $p_x + p_z = 1$. In the message round, Bob prepares a sequence of random numbers of length k, denoted as $r_1 r_2 \cdots r_k$, where $r \in (0, 1)$. Meanwhile, Bob uses n bits of Z-basis state $|0\rangle_{\rm GKP}$ to prepare the k-bit logical zero state

* Corresponding author (email: chai.geng@nwu.edu.cn, caozhw@nwu.edu.cn)

$\left|\overline{0_1 0_2 \cdots 0_k}\right\rangle_{\mathrm{GKP}}$. After that, the logical zero state is encoded to the logical state $\left|\overline{r_1 r_2 \cdots r_k}\right\rangle_{\mathrm{GKP}}$ by selecting the corresponding logical X operators according to the sequence of random numbers. Similar to the message round, Bob in the detection round prepares X-basis states of length k, where $|+\rangle_{\mathrm{GKP}}$ refers to "0" and $|-\rangle_{\mathrm{GKP}}$ refers to "1". The prepared logical zero state $\left|\overline{+_1 +_2 \cdots +_k}\right\rangle_{\mathrm{GKP}}$ is transformed into logical state $\left|\overline{d_1 d_2 \cdots d_k}\right\rangle_{\mathrm{GKP}}$ under the same encoder according to the random number $d_1 d_2 \cdots d_k$ of k bits. Please refer to Appendix B for more details of the encoding process. Finally, Bob transmits the encoded logical state to Alice over a Gaussian thermal-loss channel (T_1, ε_1), called the forward channel transmission, where T and ε represent the transmittance and excess noise, respectively.

(b) Error correction. Before each error correction, a quantum-limited amplifier is utilized to convert the transmission loss in the channel into Gaussian random displacement noise with a coefficient related to the transmittance T_1. Alice performs Steane error correction for each physical GKP state of the received logical state, which involves syndrome extraction as well as displacement correction. Afterwards, the GKP analog information is applied to estimate the logical errors and send them to the decoder of the external QLDPC code. In the second level of error correction, the syndrome information obtained from the measurements of the stabilizer is also passed to the decoder. Based on these two syndromes, the decoder estimates the most probable errors through an iterative decoding algorithm and performs the appropriate logical operators to accomplish the error correction.

(c) Eavesdropping detection. Alice randomly chooses some rounds to perform X-based measurements on the logical states and announces the corresponding measured results in the selected rounds. Bob selects the measured results that belong to the detection rounds to compare them with the preparation information and obtains the estimated values of quantum bit error rate (QBER) and loss in the forward channel. The secrecy capacity can be evaluated based on the estimated parameters. If the secrecy capacity is greater than zero, the communication continues; otherwise, the communication terminates.

(d) Message modulation. First, Alice and Bob screen out the remaining detection rounds to guarantee the success of message modulation. Alice prepares secret messages $m_1 m_2 \cdots m_k$ of length k, where $m \in (0, 1)$. Then, Alice encodes logical state $\left|\overline{r_1 r_2 \cdots r_k}\right\rangle_{\mathrm{GKP}}$ to logical state $\left|\overline{s_1 s_2 \cdots s_k}\right\rangle_{\mathrm{GKP}}$ by selecting appropriate logical X operator $\bar{X}_1^{m_1} \bar{X}_2^{m_2} \cdots \bar{X}_k^{m_k}$ based on the secret messages. The logical state carrying the secret messages is transmitted to Bob through a Gaussian thermal-loss channel (T_2, ε_2), called the backward channel transmission. Forward and backward channels represent two directions of transmission on the same physical channel.

(e) Measurement. Before the measurement, Bob first performs a channel conversion using a quantum-limited amplifier with coefficients related to the transmittance T_2, followed by GKP and QLDPC error correction. Bob acquires the Gaussian value of each physical GKP state on the q component using a homodyne detector and obtains binary information through the results modulo $2\sqrt{\pi}$. Finally, secret messages delivered by Alice are deduced from the preparation and measurement information.

According to the wiretap channel theory [5], the secrecy capacity of the proposed protocol can be expressed as

$$C_S = Q_{\mathrm{Bob}} \cdot (1 - h(e_z)) - Q_{\mathrm{Eve}} \cdot h(e_x), \tag{1}$$

where Q_{Bob} and Q_{Eve} represent the reception rates of Bob and Eve, respectively. Here, $h(\cdot)$ denotes the binary Shannon entropy. It is obvious that the key parameters determining the transmission reliability are the QBERs on the X and Z basis, that is, e_x and e_z. The details are presented in Appendix C.

System performance. To validate the system performance of the proposed protocol, we built simulated experiments to acquire relevant parameters. Through the noise model, the relationship between the parameters of the Gaussian thermal loss channel and the Gaussian random displacement channel is established, thereby obtaining the probability of occurrence of logical errors in different transmission environments. Furthermore, a syndrome-based iterative decoding algorithm is utilized to enhance the decoding performance of the concatenated codes. Finally, we substitute the parameters obtained from the numerical Monte Carlo simulation into the equation for calculating secrecy capacity to evaluate the system performance. Specifically, we select the $[\![7, 1, 3]\!]$ Steane code and $[\![544, 80, 12]\!]$ LP-QLDPC code with a close code rate and get the error probability after error correction so as to compare the estimated secrecy capacity. The results show that long codes can provide a lower logical error rate under conditions where the noise is below the error threshold. Thus, the proposed protocol can provide highly reliable communication as expected. The details of simulation experiments are provided in Appendix D.

Conclusion. In this study, we propose a QEC-based QSDC protocol with error correction implemented with GKP codes in the inner layer and QLDPC codes in the outer layer. The secrecy capacity of the QSDC system is analyzed through the wiretap channel theory, and the simulation approach of the QEC provides its required channel parameters. Simulation results demonstrate that the advantages of the long code in achieving the low logical error rate and high secrecy capacity are highly significant, which is applicable to the requirements of highly reliable and secure communications. Furthermore, the proposed protocol has the potential to be implemented through optical GKP states.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62571432, 62071381, 62301430) and Shaanxi Fundamental Science Research Project for Mathematics and Physics (Grant No. 23JSY014).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
2 Gottesman D, Kitaev A, Preskill J. Encoding a qubit in an oscillator. Phys Rev A, 2001, 64: 012310
3 Noh K, Chamberland C, Brandão F G S L. Low-overhead fault-tolerant quantum error correction with the surface-GKP code. PRX Quantum, 2022, 3: 010315
4 Raveendran N, Rengaswamy N, Rozpędek F, et al. Finite rate QLDPC-GKP coding scheme that surpasses the CSS Hamming bound. Quantum, 2022, 6: 767
5 Pan D, Long G L, Yin L, et al. The evolution of quantum secure direct communication: on the road to the Qinternet. IEEE Commun Surv Tut, 2024, 26: 1898–1949