SCIENCE CHINA
Information Sciences

• Supplementary File •

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

Lei WANG[1], Geng CHAI[1*], Zhengwen CAO[1*] & Xinlei CHEN[1]

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

Appendix A GKP-QLDPC code

Appendix A.1 GKP code

The GKP code exploits continuous degrees of freedom for bosonic modes in quadrature position (q) and momentum (p) and stabilizes infinite-dimensional oscillator spaces into two-dimensional subspaces corresponding to a single qubit via the properties of stabilizer codes [1–3]. The stabilizers on the two commuting components are

$$\hat{S}_q = \hat{D}\left[2\sqrt{\pi}, 0\right], \hat{S}_p = \hat{D}\left[0, 2\sqrt{\pi}\right], \tag{A1}$$

where the displacement operator is denoted as $\hat{D}\left[\alpha, \beta\right] = e^{i(\alpha\hat{q} - \beta\hat{p})}$. These two stabilizers exhibit periodic functions of $\hat{q}$ and $\hat{p}$, respectively, which enables the subspace corresponding to the GKP code to be stabilized. The Heisenberg uncertainty principle states that q and p cannot be measured simultaneously, but the commutativity of two operators implies that can be acquired simultaneously through the measurements of two components modulo a regular interval.

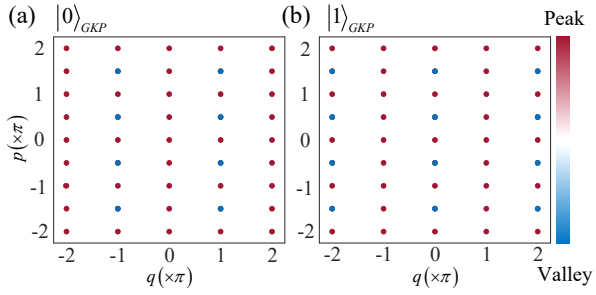

Figure A1 The Wigner functions in phase space of ideal Z-based GKP states. Each dot represents a Dirac delta function.

For the square-lattice GKP code, the standard states in the Z- and X-basis are given by

$$|0\rangle_{GKP} = \sum_{n\in\mathbb{Z}} \left|q = 2n\sqrt{\pi}\right\rangle, \quad |1\rangle_{GKP} = \sum_{n\in\mathbb{Z}} \left|q = (2n+1)\sqrt{\pi}\right\rangle, \tag{A2}$$

and

$$|+\rangle_{GKP} = \sum_{n\in\mathbb{Z}} \left|p = 2n\sqrt{\pi}\right\rangle, \quad |-\rangle_{GKP} = \sum_{n\in\mathbb{Z}} \left|p = (2n+1)\sqrt{\pi}\right\rangle. \tag{A3}$$

Under the same basis, two GKP states representing different information realize their mutual transitions through the displacement $\sqrt{\pi}$. The results will fall in the interval $\left[-\sqrt{\pi}/2, \sqrt{\pi}/2\right)$ from measuring the $q(p)$ component of the $Z(X)$-basis state due to the measurement values modulo $\sqrt{\pi}$. Obviously, there is no effect on the carried information for the displacement noise with an absolute value less than $\sqrt{\pi}/2$ [4, 5]. The Wigner functions of the Z-based GKP states in the ideal case are shown in Figure A1.

There are two common ways, Steane-based and teleportation-based [6,7], to implement GKP error correction by stabilizer measurements combined with displacement operators. For any unknown GKP state, error correction always includes noise reductions on the q and p components. In realistic scenarios, ancillary GKP states with finite squeezing introduce additional

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

noise into the data GKP states. Since the series structure produces an error propagation effect in the error correction of two components compared to the parallel structure, the teleportation-based error correction causes less interference than the Steane error correction. However, the two ways are equivalent in the assumption of ideal error correction.

To facilitate understanding, the schematic of Steane error correction is shown in Figure A2. The direct measurement of an unknown quantum state can provide information about noise interferences, but also destroys their superposition. In general, the operation of the stabilizer acts on the GKP state without altering its state [5], denoted as

$$\hat{S}_q|\mu\rangle_{GKP} = \hat{S}_p|\mu\rangle_{GKP} = |\mu\rangle_{GKP}, \tag{A4}$$

where $\mu \in (0, 1, +, -)$. The GKP states are stabilized by these two operators, satisfying the relation $\hat{q} = \hat{p} = 0 \bmod \sqrt{\pi}$. Thus, the GKP states affected by noises can be indirectly attained through the measurement of stabilizers, with the assistance of additional ancillary GKP states. As shown in Figure A2, two GKP stabilizers are measured through the Steane error correction. Here, the measurement of stabilizer $\hat{S}_q$ is achieved through a sum gate with the assistance of a prepared ancillary state $|+\rangle_{GKP}$, where the sum gate acts as

$$\begin{aligned} \hat{q}_D \to \hat{q}_D,\ \hat{p}_D \to \hat{p}_D - \hat{p}_A, \\ \hat{q}_A \to \hat{q}_A + \hat{q}_D,\ \hat{p}_A \to \hat{p}_A. \end{aligned} \tag{A5}$$

The $\hat{q}_D$ component of the data mode is transferred to the ancillary mode through this gate, and the sum of the two modes in q component is gained from measuring the ancillary mode with the homodyne detector. Since the ancillary mode meets the relation $\hat{q}_A = 0 \bmod \sqrt{\pi}$, the measurement result module $\sqrt{\pi}$ is equivalent to a direct measurement of the data mode. The result q_0 belongs to the interval $\left[-\sqrt{\pi}/2, \sqrt{\pi}/2\right)$ and is feedback to the data mode through the displacement operator $\hat{D}$ to accomplish error correction. Also, the p component of the ancillary mode satisfies relation $\hat{p}_A = 0 \bmod 2\sqrt{\pi}$ and so does not affect the information carried by the data mode. In addition, the measurement of the stabilizer $\hat{S}_p$ relies on the ancillary mode $|0\rangle_{GKP}$ and the inverse sum gate.

In DV quantum information processing, a unitary group composed of four single qubit operators $\{I, X, Y, Z\}$ is employed to represent the manipulation of qubits [8]. Moreover, linear combinations of quantum gates sufficiently represent arbitrary forms of noise suffered by qubits. Among them, the X and Z operators are called bit-flip and phase-flip errors, respectively, and are able to represent the Y operators, which correspond to the simultaneous occurrence of both types of errors. In the square-lattice GKP code, the logical Z and X operators are conveniently realized via the displacement operator, denoted as

$$Z = \sqrt{\hat{S}_q} = e^{i\sqrt{\pi}\hat{q}}, \quad X = \sqrt{\hat{S}_p} = e^{-i\sqrt{\pi}\hat{p}}. \tag{A6}$$

The two logical operators are implemented by displacing $\sqrt{\pi}$ on different components, respectively.

In contrast to DV qubits, GKP states provide analog information that enhances robustness against noises. After the measurements of the two stabilizers of the GKP state module $\sqrt{\pi}$, one can access the error syndrome information $\{q_0, p_0\} \in \left[-\sqrt{\pi}/2, \sqrt{\pi}/2\right)$. The noise-induced offset $\xi_{q(p)}$ belongs to the interval $\left[\sqrt{\pi}/2, 3\sqrt{\pi}/2\right)$, and the syndrome information is $\xi_{q(p)} - \sqrt{\pi}$. After correction, the quadrature component of the GKP state evolves to $\hat{q}(\hat{p}) \to \hat{q}(\hat{p}) + \xi_{q(p)} - q_0(p_0) = \hat{q}(\hat{p}) + \sqrt{\pi}$, which leads to a logical error $X(Z)$. However, the offset belongs to the interval $\left[3\sqrt{\pi}/2, 5\sqrt{\pi}/2\right)$, and the syndrome information is $\xi_{q(p)} - 2\sqrt{\pi}$, where the correction-induced displacement $2\sqrt{\pi}$ does not change the properties of the GKP state and thus does not introduce a logical error. At the end of the stabilizer measurements, the syndrome information belongs to the interval $\left|\xi_{q(p)} - n\sqrt{\pi}\right| < \sqrt{\pi}/2$. The correction leads to a logical error for an odd number n, and is successful for an even number n.

Appendix A.2 GKP-QLDPC concatenation framework

GKP states are stabilized from an infinite-dimensional Hilbert space to a two-dimensional discrete Hilbert space by stabilizers, and thus can be employed as quantum resources in DV quantum codes to accomplish encoding and decoding. We first describe QEC codes by means of the stabilizer form.

The form of stabilizer codes is a highly efficient and convenient means of creating correspondences between quantum codes and preparation circuits, error correction circuits, and logical gate operations [9]. A qubit $|\Psi\rangle$ stabilized by an operator K can be represented as $K|\Psi\rangle = |\Psi\rangle$. Thus there is an eigenvalue of $+1$ for this qubit for the operator K. For groups composed of single qubit operators, there exists a subgroup under matrix multiplication, and the elements of the group satisfy the commutation and anti-commutation rules, which is denoted as the Pauli group $\mathcal{P}$. The Pauli group of N-qubits is the N fold tensor product of all elements in $\mathcal{P}$, which is denoted as $\mathcal{P}_N = \mathcal{P}^{\otimes N}$. Then, an N-qubit stabilizer state $|\Psi\rangle_N$ is defined by the N generators of an Abelian (all elements commute) subgroup S in $\mathcal{P}_N$. An $[\![n, k, d]\!]$ quantum stabilizer code exists $m = n - k$ stabilizer generators that stabilizes the 2^n-dimensional Hilbert space into the 2^m-dimensional Hilbert space, and the redundant space is utilized for the warning of error syndromes. The weight $\omega(E)$ of a Pauli operator $E \in \mathcal{P}_n$ is the number of quantum bits that fail to meet the identity of Pauli matrices. The error correction capacity of the code is reflected in the minimum weight d of the error $E \in \mathcal{P}_n/S$ commuting with all stabilizers.

Low-density parity-check (LDPC) codes [10] are widely practiced in classical domains since their ability to approach an upper bound on the amount of information that can be reliably transmitted over a noisy channel, as proposed by Shannon. The corresponding QLDPC codes [11] have been extensively studied because of their advantages in low weight stabilizers and low-complexity decoding algorithms compared to other quantum codes. QLDPC codes that satisfy the Calderbank-Shor-Steane (CSS) [12,13] structure are able to be completely characterized through two classical codes, which is relatively convenient for the comprehension of the QEC principle. Quantum CSS stabilizer codes are represented via the operators of pure

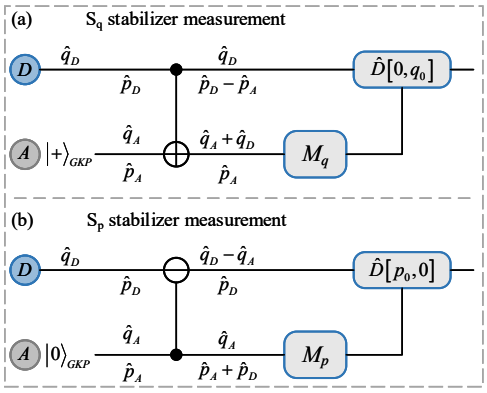

Figure A2 GKP Steane error correction. The $S_q(S_p)$ stabilizer measurement requires a single GKP ancilla $|+_{GKP}\rangle(|0_{GKP}\rangle)$. The sum gate and inverse sum gate are marked as controlled-$\oplus$ and controlled-$\ominus$, respectively, and control the data qubit (marked as D) and the ancillary mode (marked as A) to perform the corresponding operations. Then the ancillary mode is measured in the $\hat{q}(\hat{p})$ component and the syndrome $q_0(p_0)$ is acquired through the outcome modulo $\sqrt{\pi}$. Finally the correction operation is accomplished through the application of the displacement operator $\hat{D}$.

X-type and pure Z-type. Specifically, two classical error-correction codes $C_{[n,k_1,d_1]}$ and $C_{[n,k_2,d_2]}$ are considered, with the parity-check matrices H_X and H_Z, respectively, which result in a quantum CSS code $[\![n, k = k_1 + k_2 - n, d \geqslant \min(d_1, d_2)]\!]$ with the parity-check matrix $H = (H_X|H_Z)$ [14]. The code rate of a quantum code is defined as $R = k/n$. These two parity-check matrices need to meet the condition $H_X H_Z^T = 0$ to ensure the commutability among the stabilizers. k and n denote the number of information qubits and encoded physical qubits, respectively. In particular, each row in the parity-check matrix of the quantum stabilizer code corresponds to each of its stabilizers. Since the noise experienced by a qubit can be completely decomposed into X-type and Z-type errors, the decoding procedure can be performed based on the matrices H_X and H_Z, respectively.

In general, the framework of QLDPC codes consists of four modules: the input DV qubits, the multi-qubit encoder, the channel, and the multi-qubit decoder [15]. The resulting extended GKP-QLDPC concatenation framework replaces input qubits with GKP states and inserts GKP error correction in front of the multi-qubit decoder. As an example, the concatenation framework of GKP codes with the repetition code [16] is shown in Figure A3. Under the operation of sum gates, an arbitrary qubit $|\varphi\rangle_{GKP} = \alpha|0\rangle_{GKP} + \beta|1\rangle_{GKP}$ is encoded as $\alpha|000\rangle_{GKP} + \beta|111\rangle_{GKP}$. After channel transmission, one can assume that only the first qubit has a bit-flip error as event 1, and that only the first qubit has no bit-flip error as event 2. The probabilities of these two cases are written as P_1, P_2, and the probabilities of occurrence of the logical error in the three qubits are denoted as p_1, p_2, p_3. Correspondingly, the relations $P_1 = p_1 \cdot (1 - p_2) \cdot (1 - p_3)$ and $P_2 = (1 - p_1) \cdot p_2 \cdot p_3$ are satisfied. If the GKP state is used as the DV qubit, the two events receive same syndrome information, and p_1, p_2, p_3 are all equal to an average error probability. In the case where only small error probabilities are considered, one always obtains $P_1 > P_2$ and can only determine the occurrence of event 1. But with the GKP analog information, p_1, p_2, p_3 are differentiated and it is possible to distinguish two events. The specific connection between the probability and the analog information can be found in Eq. (D6). Thus, the combination of GKP states not only provides additional capability of error correction but also provides analog information to enhance the decoding of the outer stabilizer codes.

So far, most studies about the GKP code have focused on their concatenation with repetition codes or two-dimensional topological codes [17]. However, such codes have the drawback that it always encodes a fixed number of logical qubits for a given topology. This implies an asymptotically zero code rate and indicates that the increasing distance d comes at the expense of the growing number of physical qubits. In comparison, QLDPC codes encode multiple logical qubits into one block that enables higher code rates and reduces the overhead of quantum resources [18]. Since both the rate and distance of QLDPC codes scale linearly with the code length, this property means utilizing fewer quantum resources to achieve stronger error correction, which is conducive to high-rate and high-efficiency quantum information processing. In addition, the low weight of QLDPC codes reduces the circuit depth and facilitates their experimental realization. Therefore, the GKP-QLDPC concatenation structure has significant advantages in constructing highly reliable quantum communications. The more detailed concatenation model could refer to [19].

Appendix B QEC encoder and decoder

The core of the designed protocol is the QEC encoder and decoder with GKP states. In particular, the advantage of the stabilizer form is the simplicity of the construction of quantum circuits. A quantum CSS code $[\![n, k, d]\!]$ contains $n - k$ stabilizers, $\left(K_1^X, \cdots, K_{(n-k)/2}^X\right)$ and $\left(K_1^Z, \cdots, K_{(n-k)/2}^Z\right)$, corresponding to each row of the parity-check matrix. Considering the quantum circuit of X and Z-stabilizer correction, for any input state, $|\varphi\rangle_{IN}$, some ancillary modes initialized to $|0\rangle_{GKP}$ are used as control qubits to perform stabilizer operators. Taking the stabilizer K_i^X as an example, after the second Hadamard gate, the state of the system composed of ancillary mode and input state can be expressed as

$$|\varphi\rangle_{OUT} = \frac{1}{2}\left(|\varphi\rangle_{IN} + K_i^X|\varphi\rangle_{IN}\right)|0\rangle_{GKP} + \frac{1}{2}\left(|\varphi\rangle_{IN} - K_i^X|\varphi\rangle_{IN}\right)|1\rangle_{GKP}. \tag{B1}$$

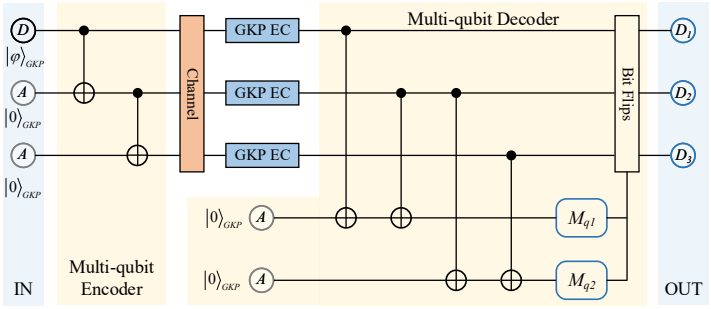

Figure A3 Circuit on the concatenation of the GKP code with the three-qubit bit-flip code. EC, error correction.

The q component of the ancillary mode is then measured. With the measurement $|0\rangle_{GKP}$, the input state is projected to

$$|\varphi\rangle_{OUT} = |\varphi\rangle_{IN} + K_i^X |\varphi\rangle_{IN}. \tag{B2}$$

Since the stabilizer is Hermitian, i.e., $K_i^X \cdot K_i^X = \mathrm{I}$, thus $K_i^X |\varphi\rangle_{OUT} = |\varphi\rangle_{OUT}$. Here $|\varphi\rangle_{OUT}$ is a $+1$ eigenstate of K_i^X, so the output state is stabilized. If the measurement result is $|0\rangle_{GKP}$, the input state is projected to

$$|\varphi\rangle_{OUT} = |\varphi\rangle_{IN} - K_i^X |\varphi\rangle_{IN}, \tag{B3}$$

which is the -1 eigenstate of K_i^X, so the output state is not stabilized by the stabilizer. This process is the measurement of the stabilizers, and the process of performing the logical operators (Z_i and X_i) based on the measurements is the error correction.

Based on the properties of the above circuits, the logical zero state can be conveniently constructed using the ancillary states $|0\rangle^{\otimes n}$, denoted as [9,20]:

$$\underbrace{|\overline{00\cdots0}\rangle}_{k} = \prod_{i=1}^{n-k} \left(\mathrm{I}^{\otimes n} + K_i\right) \underbrace{|00\cdots0\rangle}_{n}, \tag{B4}$$

where I represents the second order unit matrix. The classical information corresponding to the constructed logical zero state is an k-bit zero. Further, this circuit not only accomplishes state preparation but also performs error correction. For the error correction, after measuring each X-stabilizer, one synthesizes the measurements to infer the error position i and corrects the error using a single Z operator. Correspondingly, one can infer the position i based on the measurements of all Z-stabilizers and use a single X operator to correct the error. The completion of error correction in the X-stabilizer and Z-stabilizer marks the end of error correction of the logical state.

The modulation for the logical zero state is necessary for the goal of information transmission. Assuming that the code word to be delivered is $c_1c_2\cdots c_k$ and $c \in (0,1)$, the logical zero state can be converted to the logical state $|c_1c_2\cdots c_k\rangle$ via the logical operators, indicated as

$$|\overline{c_1c_2\cdots c_k}\rangle = \left(\overline{X}_1^{c_1}\overline{X}_2^{c_2}\cdots\overline{X}_k^{c_k}\right)|\overline{00\cdots0}\rangle, \tag{B5}$$

where $\overline{X}_i$ represents the logical X operator at the i-th bit of the logical state.

Through Gaussian elimination, the parity-check matrix H of the stabilizers can be transformed into the standard form

$$H_{std} = \left(\begin{array}{ccc|ccc} \mathrm{I} & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & \mathrm{I} & E \end{array}\right). \tag{B6}$$

All the matrices in matrix $\left[\begin{array}{ccc|ccc} \mathrm{I} & A_1 & A_2 & B & C_1 & C_2 \end{array}\right]$ have r rows, while the respective column dimensions are r, $n-k-r$, k, r, $n-k-r$ and k, respectively, and r is the rank of the matrix H_{std}. The matrices in matrix $\left[\begin{array}{ccc|ccc} 0 & 0 & 0 & D & \mathrm{I} & E \end{array}\right]$ have $(n-k-r)$ rows. The commutativity between the logical X operator and the stabilizer is then used to get $\overline{X} = [0E^T\mathrm{I}|C_2^T 00]$ [21], which contains k logical operators $\left(\overline{X}_1, \cdots, \overline{X}_k\right)$. Thus, a combination of logical X operators can transform a logical zero state into a required information state.

Appendix C Security analysis

The proposed protocol contains multiple quantum states in a round of transmission, but these states experience the same channel and suffer from noise independent of each other, so that security analysis of one of the states is feasible. Based on Wyners' wiretap channel theory, the secrecy capacity of single qubits is denoted as [22,23]:

$$C_S = \max\left\{I\left(A:B\right) - I\left(A:E\right)\right\}, \tag{C1}$$

where $I(A:B)$ and $I(A:E)$ indicate the mutual information between Alice and Bob, and between Alice and Eve, respectively. The former is limited by the noise coding theorem in the classical fields, expressed as

$$I(A:B) \leqslant Q_{Bob} \cdot (1 - h(e_z)), \tag{C2}$$

where Q_{Bob} denotes Bob's reception rate, which is related to the loss of two-way transmission and the received efficiency of the detector. e_z represents the QBER of the received Z-basis states, while $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ represents the binary Shannon entropy.

The amount of information an eavesdropper extracts depends on the specific type of attack. Under collective attacks [24], the eavesdropper Eve performs a joint operation on the quantum states passed in the forward channel and her own ancillary states to maximize the gains. In detail, the density matrix of Bob's initially prepared quantum states can be expressed as

$$\rho^B = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2}. \tag{C3}$$

Under Eve's interferences, Alice receives quantum states sent from Bob, with the density matrix denoted as

$$\rho^{BE} = U\left(\rho^B \otimes |E\rangle\langle E|\right)U^+, \tag{C4}$$

where $|E\rangle$ and U denote the ancillary state prepared and the operation performed by Eve, respectively.

It is assumed that the classical "0" and "1" in Alice's secret messages are equal probability, and their modulations are denoted by I and X, respectively. Then the encoded quantum state is

$$\rho^{ABE} = \left(\rho_0^{BE} + \rho_1^{BE}\right)/2, \tag{C5}$$

where $\rho_0^{BE} = I\rho^{BE}I$ and $\rho_1^{BE} = X\rho^{BE}X^+$. The upper bound on the amount of information Eve can access is

$$I(A:E) \leqslant \chi = \max_{\{U\}}\left\{S\left(\left(\rho_0^{BE} + \rho_1^{BE}\right)/2\right) - \left(S\left(\rho_0^{BE}\right) + S\left(\rho_1^{BE}\right)\right)/2\right\}, \tag{C6}$$

where χ indicates the Holevo upper bound and $S(\cdot)$ represents the von Neumann entropy. Based on the Gram matrix method [25,26], a specific upper bound can be obtained, denoted as

$$I(A:E) \leqslant Q_{Eve} \cdot h(e_x), \tag{C7}$$

where Q_{Eve} means the reception rate of Eve, and e_x means the QBER of X-basis states in the forward channel. At this point, the secrecy capacity can be calculated by Eqs.(C2) and (C7).

Appendix D System performance analysis

In order to analyze the performance of the QSDC system with GKP-LDPC codes, we need to build the simulation system to obtain the relevant parameters. It is the channel model as well as the decoding algorithm that needs attention. The parameters of the Gaussian thermal loss channel in our QSDC protocol cannot be directly converted to the probability of occurrence of the logical error in the GKP states, so a connection between the two needs to be established for determining the analog information provided by the GKP states. In addition, the syndrome information obtained after the measurements of the stabilizers is employed to determine the GKP states that might be in fault, and we use a syndrome-based iterative decoding algorithm to achieve a better decoding performance. Finally, the relevant communication parameters obtained through Monte Carlo simulations are substituted into the equation of the secrecy capacity to access the system performance of QSDC assisted by different GKP-QLDP codes.

Appendix D.1 Noise model

In CV quantum regimes, the noise is generally of two categories, namely, losses and thermal noises. As a result, three common channel models are derived as well, the pure-loss channel, Gaussian random displacement channel and Gaussian thermal loss channel [27], where the last one is a combination of the first two channels.

The Gaussian thermal loss channel is defined as

$$\mathcal{N}[T, \bar{n}_{th}](\hat{\rho}_1) = \mathrm{Tr}_2\left[\hat{B}(T)\left(\hat{\rho}_1 \otimes \hat{\rho}_{\bar{n}_{th}}\right)\hat{B}^\dagger(T)\right], \tag{D1}$$

where $\hat{B}(T)$ denotes a beam splitter unit with the transmittance $T \in [0,1]$. $\hat{\rho}_{\bar{n}_{th}}$ denotes the thermal state with an average photon number $\bar{n}_{th}$, from which the noise variance is expressed as $v = 2\bar{n}_{th} + 1$ [28]. Also, Tr_2 indicates the partial trace of the mode.

The quantum-limited amplification channel is denoted as

$$\mathcal{A}[G](\hat{\rho}_1) = \mathrm{Tr}_2\left[\hat{S}_2(G)\left(\hat{\rho}_1 \otimes |0\rangle\langle 0|_2\right)\hat{S}_2^\dagger(G)\right], \tag{D2}$$

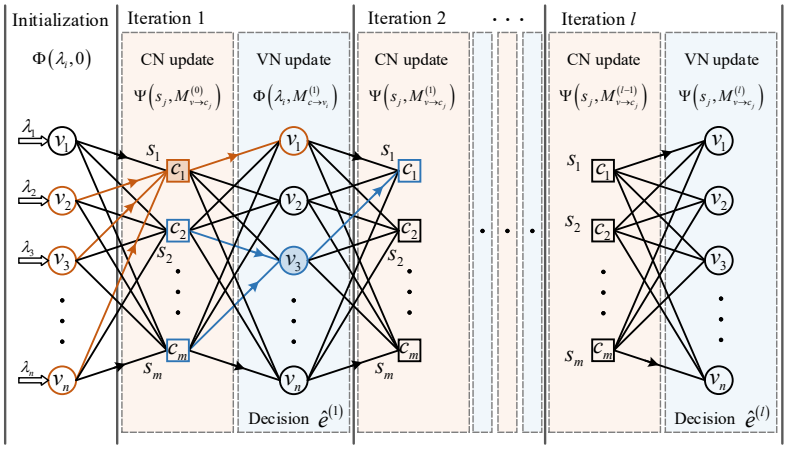

Figure D1 The update process of syndrome-based iterative message passing decoder in the Tanner graph. The decoding process involves the check node update Ψ and the variable node update Φ, shown as the orange connecting lines and the blue connecting lines, both avoiding messages from the target node. Unlike the traditional syndrome-based decoder, the log-likelihood ratio λ_i of each variable node is initialized through the error likelihood provided by the corresponding GKP state. In each iteration, the update Ψ and update Φ are performed sequentially, followed by the decision update $\hat{\Phi}$. Up to the maximum number of iterations l_{max}, the termination condition of the iterative decoder is that the syndrome $\hat{s}^{(l)}$ obtained from the estimated error $\hat{e}^{(l)}$ matches the measured syndrome s.

where $\hat{S}_2(G)$ represents the two-mode squeezed unit with a gain G and $|0\rangle$ indicates the vacuum state. The Gaussian random displacement channel is represented as

$$\mathcal{N}\left[\sigma^2\right](\hat{\rho}) = \frac{1}{\pi\sigma^2}\int d^2\alpha e^{-\frac{|\alpha|^2}{\sigma^2}}\hat{D}(\alpha)\,\hat{\rho}\hat{D}^{\dagger}(\alpha), \tag{D3}$$

where $\hat{D}(\cdot)$ indicates the displacement operator and σ^2 represents the variance of random displacements.

The Gaussian thermal loss channel can be transformed into the Gaussian random displacement channel through a quantum-limited amplifier, denoted as

$$\mathcal{A}[1/\eta]\cdot\mathcal{N}[T,\bar{n}_{th}] = \mathcal{N}_{B_2}\left[\sigma^2_{\eta,\bar{n}_{th}}\right], \tag{D4}$$

where the variance of the Gaussian noise is

$$\sigma^2_{\eta,\bar{n}_{th}} = \left(\frac{1-T}{T}\right)(2\bar{n}_{th}+2) = \left(\frac{1-T}{T}\right)(v+1). \tag{D5}$$

The variance of thermal noises can be converted to the excess noise ε through the relationships of both [29], to obtain the variance $2(1-T)/T+\varepsilon$.

Due to the conversion nature between the channels, it is sufficient to analyze the noises generated by the Gaussian random displacement channel. The essence of this channel is to append Gaussian noises with the variance σ^2 to the two components of the boson state via the displacement operator. Based on stabilizer measurements, the syndrome information $\{q_0, p_0\}$ provided by the GKP state can be gotten. Taking the output q_0 as an illustration, the probability of occurrence of the logical error with a standard deviation of noises σ is [1]:

$$P(\sigma)_{q_0} = \frac{\sum\limits_{n\in\mathbb{Z}}\exp\left[-\left(q_0-(2n+1)\sqrt{\pi}\right)^2/2\sigma^2\right]}{\sum\limits_{n\in\mathbb{Z}}\exp\left[-\left(q_0-n\sqrt{\pi}\right)^2/2\sigma^2\right]}. \tag{D6}$$

At a constant standard deviation, the probability of error will reach a maximum value 0.5 as the syndrome converge to the boundaries, i.e., its absolute value converges to $\sqrt{\pi}/2$. The status of errors introduced after GKP correction can be verified by post selection techniques. In addition, this analog information that the GKP code can provide to the external cascaded DV codes promotes the error correction performance of the external decoding.

Appendix D.2 Syndrome-based iterative decoding

In classical error correction codes, the decoding process is to infer the maximum possible transmit vector based on the receive vector under the establishment of channel characteristics. Relatively, in the protection of quantum information, QEC requires the utilization of ancillary quantum states to accomplish the measurement of stabilizers and to estimate the most likely errors based on the results. In quantum CSS codes, quantum states are perturbed by the noise $[e_X, e_Z]$ after passing through a channel, and the measurement of stabilizers implies verifying the error and obtaining the syndrome

information, denoted $s_X = H_X e_Z^T$ and $s_Z = H_Z e_X^T$, via each row in the parity-check matrices H_X and H_Z. The mission of the decoder is to find a suitable error to match the syndrome information and use the appropriate quantum gate to correct it according to this estimated error.

In terms of decoding, QLDPC codes have the advantage of the existence of iterative decoding algorithms with low complexity to achieve highly accurate error estimation. The message passing iterative decoder can be graphically expressed based on a sparse bipartite graph [30], called Tanner graph, of the parity-check matrix. Since X-type and Z-type errors are independent of each other in the considered channel model, H, s, and e correspond to the parity-check matrix, the measured syndrome, and the error vector, respectively, for the convenience of explaining the process of iterative decoding.

The Tanner graph for the syndrome-based iterative message passing is shown in Figure D1. The error experienced during transmission is represented as a binary vector $e = (e_1, \cdots, e_n)$, and then the measurements yield a syndrome $s = (s_1, \cdots, s_{n-k})$. The target of the decoder is to compute the posterior probability at each iteration, *i.e.*, to estimate the probability of an error or no error based on the measured syndromes $P(e_i \,|s\,)_{i=\{1,\cdots,n\}}$. The computation of this probability relies on the initialization of the message, which is subsequently updated at the node and then propagated in the Tanner graph.

In the decoding process without GKP analog information, each qubit is assigned the same initial value based on the channel characteristics, i.e., the ensemble of probabilities that $e_i = 0$ or $e_i = 1$, denoted by the log-likelihood ratio (LLR) as $\lambda_i = \ln\left(P\left(e_i = 0\right)/P\left(e_i = 1\right)\right)$. In general, the initialization process sets these LLRs to small positive values to favor error-free modes, thus promoting decoder performance. In concatenated GKP-QLDPC codes, the stabilizer measurements of the GKP states provide analog information, so the LLR of each bit is unique. The analog information provided by the GKP state is q_0, then its LLR is expressed as:

$$\lambda_i = \ln \frac{\sum_{n\in\mathbb{Z}} \exp\left[-\left(q_0 - 2n\sqrt{\pi}\right)^2/\left(2\sigma^2\right)\right]}{\sum_{n\in\mathbb{Z}} \exp\left[-\left(q_0 - (2n+1)\sqrt{\pi}\right)^2/(2\sigma^2)\right]}. \tag{D7}$$

There are two types of update functions in the iterative decoder, the variable node update (VNU) function and the check node update (CNU) function. The decoder passes the message through the edges of the Tanner graph, and the passing of extrinsic message from node x to node y in the k-th iteration is denoted as $M_{x\to y}^{(k)}$. All the neighboring nodes of a node x are denoted as N_x, while $N_x/\{y\}$ denotes all other neighboring nodes except the node y. To speed up the computation of the decoding process, the belief propagation (BP) decoding based on the min-sum algorithm [31] is utilized. For every variable node, the VNU function is denoted as:

$$M_{v_i\to c_j} = \Phi\left(\lambda_i, M_{c\to v_i}\right) = \lambda_i + \sum_{c\in N_{v_i}/\{c_j\}} M_{c\to v_i}. \tag{D8}$$

The VNU function is a summing operation that takes the messages from all neighboring nodes except node c_j and passes it to node c_j, while taking into account the LLR of the node itself. The CNU function is expressed as:

$$M_{c_j\to v_i} = \Psi\left(s_j, M_{v\to c_j}\right) = \operatorname{sgn}\left(s_j\right) \cdot \prod_{v\in N_{c_j}/\{v_i\}} \operatorname{sgn}\left(M_{v\to c_j}\right) \cdot \min_{v\in N_{c_j}/\{v_i\}} \left|M_{v\to c_j}\right|, \tag{D9}$$

where the sign function represents $\operatorname{sgn}(a) = 1$ if a is greater than zero and otherwise $\operatorname{sgn}(a) = -1$. The CNU function depends on a continuous multiplication of the symbols obtained from all neighboring nodes except the node v_i, while considering the syndrome of the node itself, and passes the updated value to the node v_i.

At the iteration l less than the maximum iteration l_{max}, each round of the decoding process performs the CNU first, followed by the VNU, and obtains the possible errors for each variable node. Specifically, an error estimate $\hat{e}_i^{(l)} = \left(1 - \operatorname{sgn}\left(\hat{\Phi}\left(\lambda_i, M_{c\to v_i}^{(l)}\right)\right)\right)/2$ is formed using the sign-based decision update function. The decoded output of the round is $\hat{e}^{(l)} = \left(\hat{e}_1^{(l)}, \cdots, \hat{e}_n^{(l)}\right)$, which is used to verify the match with each row of the parity-check matrix, i.e., whether the virtual syndrome $\hat{s}^{(l)} = \hat{e}^{(l)} \cdot H^T$ formed by the estimated error is the same as the measured one. If they are identical, the decoding is successful. Otherwise, the decoding will continue until it is terminated at the maximum iteration l_{max}.

Appendix D.3 System simulation

According to the equations for the secrecy capacity in Sec. Appendix C, it is readily known that the parameters that govern system performances are e_x after the forward transmission and e_z after the two-way transmission. Due to the presence of QEC, it is necessary to focus on the residual errors after two levels of error correction, GKP and QLDPC codes. Considering the symmetry between the logical X operator and the logical Z operator, the probability of the residual error is the same for both and is assumed to be P_{res}. This residual error channel can follow the form of a depolarization channel expressed as

$$D\left(\rho\right) = P_{res}\left(1 - P_{res}\right)\left(X\rho X + Z\rho Z\right) + \left(1 - P_{res}\right)^2\rho + P_{res}^2 Y\rho Y, \tag{D10}$$

where ρ represents the quantum state of the channel input [1]. The error rate of the quantum state in the X- and Z- basis after traveling through this channel is obtained, denoted as $e_x = e_z = P_{res}$. Therefore, the secrecy capacity can be measured via the probability of residual errors P_{res}.

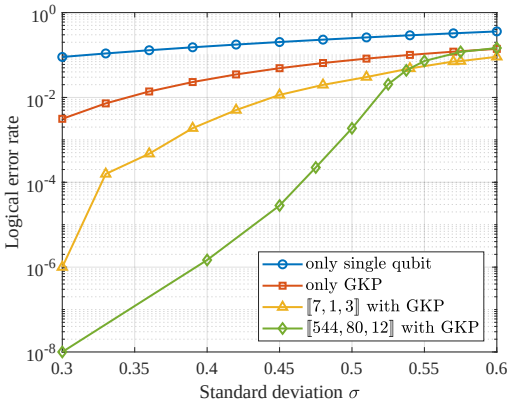

Figure D2 The logical error rate graph under different conditions. The blue and orange data points indicate the use of only single qubits and GKP states, respectively. The yellow and green data points correspond to the $[\![7,1,3]\!]$ Steane code and $[\![544,80,12]\!]$ LP-QLDPC code, respectively, which have a close code rate. The intersection point of two curves indicates an error threshold. At σ less than the error threshold, the long code obtains a lower logical error rate compared to the short code. This advantage of the long code becomes a drawback after σ is greater than the error threshold.

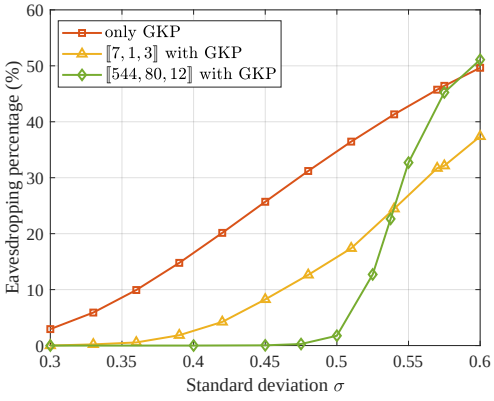

Figure D3 Eavesdropping percentage as a function of standard deviation at different codes. The orange data points indicate that only GKP error correction is utilized without the outer layer code. The yellow and green data points indicate that the $[\![7,1,3]\!]$ Steane code and $[\![544,80,12]\!]$ code are served as the outer layer of the GKP code, respectively.

Due to technological limitations, the probability P_{res} is acquired by means of the numerical Monte Carlo simulation. Meanwhile, the focus of this article is on the achievable performance of communication systems aided by quantum CSS codes, so the assumptions of ideal GKP states and perfect operators are employed throughout the analysis. There are two quantum codes chosen as external codes for the system. One is the $[\![7,1,3]\!]$ Steane code [32], which is expanded from the classical $[7,4,3]$ Hamming code. The other is the $[\![544,80,12]\!]$ lifted product (LP) QLDPC code [33,34], which belongs to the quasi-cyclic (QC) QLDPC codes. Long codes provide better error-correction performance as they have larger d compared to short codes. Our aim is to quantify the degree of improvement in system performance.

To compare the performance of the above two codes with the assistance of GKP codes, the logical error rate is plotted as a function of the standard deviation σ of the Gaussian random displacement noise in Figure D2. In particular, the standard deviation can be conveniently converted to the transmittance and excess noise through the relationship $\sigma = \sqrt{2\,(1-T)/T+\varepsilon}$. For an $[\![n,k,d]\!]$ quantum code, a logical error refers to the fact that one of the n physical qubits is different from the original state after passing through the channel. In our simulations, the decoder utilizes the syndrome-based min-sum algorithm and the sequential update schedule, with the maximum number of iterations $l_{max} = 100$. The close code rate of the two codes indicates that the proportion of errors generated is similar for the code length under the same noise variance σ^2. The intersection of the two curves represents an error threshold that reflects the transition from error suppression to error enhancement. Below the threshold, the effect of the long code on reducing the logical error rate is remarkable. On the contrary, the short code shows a lower logical error rate compared to the long code.

This threshold illustrates that neither an increase in code length nor an increase in the number of iterations improves the logical error rate as the channel noise exceeds a certain value. In other words, while the error rate of physical qubits is less than the error threshold, the logical error rate can be infinitely low as the code length increases, which is also one of the thresholds for fault-tolerant quantum computation. For a given family or similar code rate of QLDPC codes, there exists a theoretical threshold to limit the probability of successful decoding [35], which also reflects the upper bound of error correction capability. To get the threshold of QEC codes, some statistical mechanical models have been used to make indirect estimations [36]. Without taking into account the specific hardware architecture as well as the actual implementation of quantum gates, the error threshold depends mainly on the algorithm used for syndrome-based decoding. Consequently, the

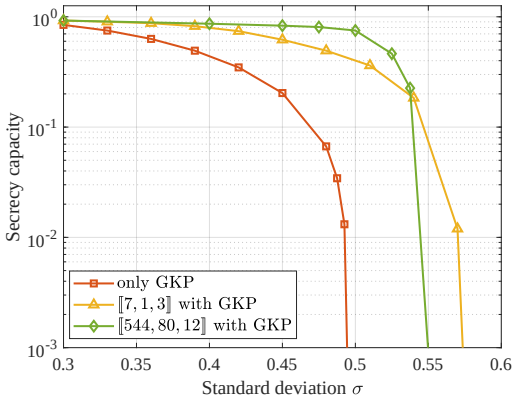

Figure D4 Secrecy capacity as a function of standard deviation at different codes. The orange data points indicate that only GKP error correction is utilized without the outer layer code. The yellow and green data points indicate that the $[\![7,1,3]\!]$ Steane code and $[\![544,80,12]\!]$ code are served as the outer layer of the GKP code, respectively. The intersection point of these two curves represents an error threshold.

appropriate adjustment and improvement of the decoding algorithm is favorable to increase error threshold [37]. Besides, it is possible to design QLDPC codes with high thresholds by analyzing the factors of non-convergence of decoding.

In addition, in order to demonstrate the effect of the second level QEC, the secrecy capacity with only GKP error correction is analyzed by numerical evaluation. For ideal GKP states, the probability of X logical error and Z logical error after error correction is equivalent [1], is given by

$$P_{err}(\sigma) = \frac{1}{\sqrt{2\pi}\sigma} \int_{|x|>\frac{\sqrt{\pi}}{2}} dx \exp\left(-\frac{x^2}{2\sigma^2}\right) = \operatorname{erfc}\left(\sqrt{\frac{\pi}{8\sigma^2}}\right), \tag{D11}$$

where the error function is $\operatorname{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^\infty e^{-t^2} dt$. Large random displacements on quadrature components that lie in even multiples of the interval $\left[-\sqrt{\pi}/2, \sqrt{\pi}/2\right)$ can be corrected, but the probability of this component is negligibly small given the range of σ. Here, the considered range of the noise variance is shown on the horizontal axis. The orange data points respond to the error correction capability of the GKP code, while the degree of decrease in the logical error rate of the yellow and green data points reflects the error correction capability of the respective quantum codes. Obviously, a cascade of GKP codes and QLDPC codes yields a better error correction capability. Notably, the green data points are above the orange data points at larger variances, which indicates that the second level of error correction produces negative gains. Moreover, the blue data points indicate the logical error rate of single qubits at different standard deviations of noises [1], and have a higher logical error rate compared to orange data points. The reason is the robustness of GKP states to the noise compared to single qubits.

After mastering the performance of the two codes, the channel parameter e_x for evaluating the eavesdropping capacity are derived through the simulation approach. The eavesdropping percentage, which represents the ratio of the estimated and maximum eavesdropping channel capacity, is used to demonstrate the extent of eavesdropping, as shown in Figure D3. The yellow data points and the green data points are almost always below the orange data points, indicating that the employment of QLDPC codes effectively suppresses the eavesdropper's abilities. Green data points have a very low eavesdropping percentage compared to yellow data points over most of the noise range, indicating that eavesdroppers have little access to valid information. Therefore, long codes are essential for building a secure quantum channel.

In our protocol, $e_x = P_{err}$, while the value e_z requires further estimation due to the influence of noises in the forward and backward channels. With the two channels independent of each other, the total probability of logical errors can be obtained from the accumulation of two errors. The secrecy capacity with only GKP error correction is shown as orange data points in Figure D4. Due to the robustness of GKP states for noise-induced random displacements in the interval $\left[-\sqrt{\pi}/2, \sqrt{\pi}/2\right)$, the secrecy capacity decreases smoothly with the standard deviation. As the standard deviation increases further, the secrecy capacity rapidly decreases.

In the cascaded GKP-QLDPC structure, the processes of encoding and decoding of the two codes are simulated to get the probability of remaining logical errors. The performance of $[\![7,1,3]\!]$ Steane code and $[\![544,80,12]\!]$ LP-QLDPC code in the QSDC system is presented as the yellow and green data points. Compared to the orange data points, the extra outer code is significant for maintaining a high level of secrecy capacity, so the transmission distance increases slightly as well. The long code has an advantage over the short code in maintaining high secrecy capacity. However, due to the presence of an error threshold, the advantage of the long code in secrecy capacity converts into a disadvantage as the noise variance increases and shows a higher logical error rate. Nevertheless, the high fidelity provided by the long code in the corresponding standard deviation below the threshold is indispensable for the protocols with highly reliable communication requirements.

As for potential experimental realizations, the possibilities and challenges of our scheme naturally depend on its physical realization. To accommodate multiple error corrections, a possible implementation is to accomplish the preparation of auxiliary GKP states and quantum gate operations via the CV quantum memory. Although high-quality GKP states have been realized in ion trap and superconducting circuit platforms, there are barriers to efficient transduction between optical field and these regions. Owing to the recent experimental realization of optical GKP states [38], all-optical implementation is

an alternative option that can avoid the requirement of quantum memory. Such an implementation performs QEC through the measurement-based approach, which is usually easier than the quantum circuit model based on the quantum gate in the optical setup. To facilitate the practicability, the designed quantum circuits based on the quantum gate need to be mapped into the form of cluster state representations [39] for the adaptation of all-optical implementations. Furthermore, many non-ideal factors, such as GKP states with finite squeezing, lossy linear optical transformations, and noisy heterodyne detectors, can be taken into account in the simulation analysis process. In this optical architecture, the weight optimization of QLDPC codes to improve the noise tolerance performance also deserves further exploration. Finally, the extension of our scheme to all-optical repeater structures will be an attractive research direction.

References

1 Rozpędek F, Noh K, Xu Q, et al. Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes. npj Quantum Information, 2021, 7: 102
2 Wu B H, Zhang Z, Zhuang Q. Continuous-variable quantum repeaters based on bosonic error-correction and teleportation: architecture and applications. Quantum Science and Technology, 2022, 7: 025018
3 Brady A J, Eickbusch A, Singh S, et al. Advances in bosonic quantum error correction with Gottesman-Kitaev-Preskill codes: Theory, engineering and applications. Progress in Quantum Electronics, 2024, 93: 100496
4 Fukui K, Takeda S. Building a large-scale quantum computer with continuous-variable optical technologies. Journal of Physics B: Atomic, Molecular and Optical Physics, 2022, 55: 012001
5 Noh K. Quantum computation and communication in bosonic systems. Ph.D. thesis, Yale University, 2020
6 Fukui K, Alexander R N, van Loock P. All-optical long-distance quantum communication with Gottesman-Kitaev-Preskill qubits. Phys Rev Res, 2021, 3: 033118
7 Walshe B W, Baragiola B Q, Alexander R N, et al. Continuous-variable gate teleportation and bosonic-code error correction. Phys Rev A, 2020, 102: 062411
8 Bharti K, Cervera-Lierta A, Kyaw T H, et al. Noisy intermediate-scale quantum algorithms. Rev Mod Phys, 2022, 94: 015004
9 Gottesman D. Stabilizer codes and quantum error correction. California Institute of Technology, 1997
10 Gallager R. Low-density parity-check codes. IRE Transactions on Information Theory, 1962, 8: 21–28
11 Breuckmann N P, Eberhardt J N. Quantum low-density parity-check codes. PRX Quantum, 2021, 2: 040101
12 Calderbank A R, Shor P W. Good quantum error-correcting codes exist. Phys Rev A, 1996, 54: 1098–1105
13 Steane A. Multiple-particle interference and quantum error correction. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 1996, 452: 2551–2577
14 Martinez J E, Fuentes P, Crespo P M, et al. Approximating decoherence processes for the design and simulation of quantum error correction codes on classical computers. IEEE Access, 2020, 8: 172623–172643
15 Rozpędek F, Seshadreesan K P, Polakos P, et al. All-photonic Gottesman-Kitaev-Preskill-qubit repeater using analog-information-assisted multiplexed entanglement ranking. Phys Rev Res, 2023, 5: 043056
16 Fukui K, Tomita A, Okamoto A. Analog quantum error correction with encoding a qubit into an oscillator. Phys Rev Lett, 2017, 119: 180507
17 Zhang J, Wu Y C, Guo G P. Concatenation of the Gottesman-Kitaev-Preskill code with the XZZX surface code. Phys Rev A, 2023, 107: 062408
18 Xu Q, Bonilla Ataides J P, Pattison C A, et al. Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays. Nature Physics, 2024, 20: 1084–1090
19 Xu Y, Wang Y, Kuo E J, et al. Qubit-oscillator concatenated codes: Decoding formalism and code comparison. PRX Quantum, 2023, 4: 020342
20 Devitt S J, Munro W J, Nemoto K. Quantum error correction for beginners. Reports on Progress in Physics, 2013, 76: 076001
21 Nielsen M A, Chuang I L. Quantum computation and quantum information. Cambridge university press, 2010
22 Wu J, Lin Z, Yin L, et al. Security of quantum secure direct communication based on wyner's wiretap channel theory. Quantum Engineer, 1: e26
23 Qi R, Sun Z, Lin Z, et al. Implementation and security analysis of practical quantum secure direct communication. Light Sci Appl, 2019, 8: 1–8
24 Wu J, Long G L, Hayashi M. Quantum secure direct communication with private dense coding using a general preshared quantum state. Phys Rev Appl, 2022, 17: 064011
25 Jozsa R, Schlienz J. Distinguishability of states and von neumann entropy. Phys Rev A, 2000, 62: 012301
26 Henao C I, Serra R M. Practical security analysis of two-way quantum-key-distribution protocols based on nonorthogonal states. Phys Rev A, 2015, 92: 052317
27 Noh K, Albert V V, Jiang L. Quantum capacity bounds of gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes. IEEE Transactions on Information Theory, 2019, 65: 2563-2582
28 Weedbrook C, Pirandola S, García-Patrón R, et al. Gaussian quantum information. Rev Mod Phys, 2012, 84: 621–669
29 Weedbrook C, Pirandola S, Ralph T C. Continuous-variable quantum key distribution using thermal states. Phys Rev A, 2012, 86: 022318
30 MacKay D, Mitchison G, McFadden P. Sparse-graph codes for quantum error correction. IEEE Transactions on Information Theory, 2004, 50: 2315–2330
31 Hocevar D. A reduced complexity decoder architecture via layered decoding of LDPC codes. In: IEEE Workshop on Signal Processing Systems, Texas, 2004. 107–112
32 Steane A M. Error correcting codes in quantum theory. Phys Rev Lett, 1996, 77: 793–797
33 Panteleev P, Kalachev G. Quantum LDPC codes with almost linear minimum distance. IEEE Transactions on Information Theory, 2022, 68: 213–229
34 Rengaswamy N, Raveendran N, Raina A, et al. Entanglement Purification with Quantum LDPC Codes and Iterative Decoding. Quantum, 2024, 8: 1233
35 Kovalev A A, Pryadko L P. Fault tolerance of quantum low-density parity check codes with sublinear distance scaling. Phys Rev A, 2013, 87: 020304
36 Dumer I, Kovalev A A, Pryadko L P. Thresholds for correcting errors, erasures, and faulty syndrome measurements in degenerate quantum codes. Phys Rev Lett., 2015, 115: 050502
37 Grospellier A, Grouès L, Krishna A, et al. Combining hard and soft decoders for hypergraph product codes. Quantum, 2021, 5: 432
38 Larsen M V, Bourassa J E, Kocsis S, et al. Integrated photonic source of Gottesman-Kitaev-Preskill qubits. Nature, 2025, 642: 587–592
39 Walshe B W, Baragiola B Q, Ferretti H, et al. Linear-optical quantum computation with arbitrary error-correcting codes. Phys Rev Lett, 2025, 134: 100602