Sohn et al. *EPJ Quantum Technology* (2025) 12:131
https://doi.org/10.1140/epjqt/s40507-025-00431-5

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Fault-tolerant and secure long-distance quantum communication via uncorrectable-error-injection

IlKwon Sohn[1*], Boseon Kim[1†], Kwangil Bae[1†], Wooyeong Song[1†], Chankyun Lee[1†], Kabgyun Jeong[2,3†] and Wonhyuk Lee[1†]

*Correspondence:
d2estiny@kisti.re.kr
[1]Quantum Network Research Center, Korea Institute of Science and Technology Information, Daejeon, 34141, Republic of Korea
Full list of author information is available at the end of the article
[†]Equal contributors

Abstract

Quantum networks aim to facilitate the fault-tolerant and secure transmission of quantum states across distant devices. The widely adopted quantum teleportation scheme requires multiple rounds of entanglement swapping and purification, leading to significant resource overhead and operational complexity. In this study, we propose a novel fault-tolerant and secure quantum communication scheme based on uncorrectable error injection. Our method exploits a quantum state encoding scheme based on quantum error correction codes, which strategically introduces uncorrectable errors to enhance security. It eliminates the need for entanglement distribution while reducing resource requirements. The injected errors protect against eavesdropping by preventing unauthorized parties from retrieving meaningful information. Security analysis shows that as the data length and encoded message size increase, information leakage becomes negligible relative to the size of the total message. Comparative performance analysis with existing approaches indicates that our method reduces transmission overhead while maintaining comparable fidelity in low-error regimes. These findings suggest that the proposed method offers a scalable and practical alternative for secure long-distance quantum communication, distributed quantum computing, and future quantum internet applications.

Keywords: Fault-tolerant quantum communication; Secure quantum communication; Quantum error correction code; Uncorrectable error injection

1 Introduction

Quantum networks provide a framework for distributing quantum information across physically separated quantum processors, utilizing quantum entanglement [1–5]. To enable secure and efficient quantum communication, it is essential to reliably transmit arbitrary quantum states over long distances.

Quantum teleportation provides the foundation for various quantum communication tasks and serves as a fundamental protocol that utilizes quantum entanglement, as well as quantum and classical links, to transmit arbitrary quantum states [6–8]. However, it requires a pre-shared entangled pair between the sender and receiver. If the distance is

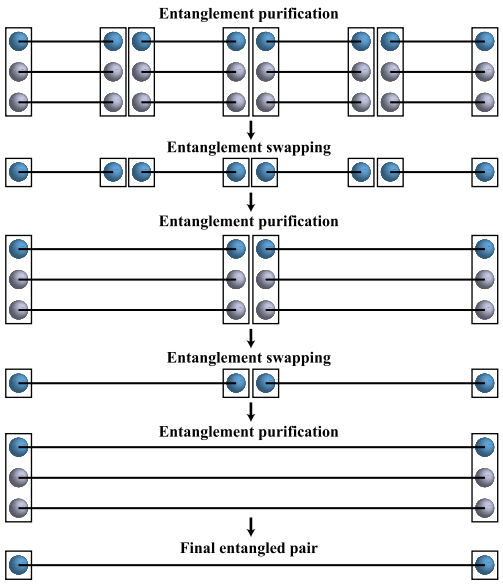

Figure 1 Schematic of the long-distance entanglement distribution Blue spheres represent the entangled pairs and gray spheres represent the ancilla qubits used for purification. By repeatedly performing entanglement purification to enhance fidelity and entanglement swapping, entangled pairs can be shared over long distances

longer than the maximal achievable distance for a single distribution link, entanglement swapping is necessary to extend the distribution range [9, 10]. Additionally, to enhance the fidelity of shared entanglement, entanglement purification must be performed [11–17], as reported in [18].

In a linear optical setup, entanglement swapping has a success probability of only 50% due to the limitations of physical Bell state measurement (BSM), causing the success probability to decrease exponentially with the number of nodes over long distances. To mitigate this, logical BSM using quantum error correction codes (QECCs) can be performed, increasing the success probability to $1 - 1/2^{n_{bsm}}$ based on the code length n_{bsm}, albeit introducing an n_{bsm}-fold overhead [19, 20]. The overhead further increases when purification is considered. Using the purification method described in [17], high fidelity can be achieved with only two ancillary qubits per entangled pair (e.g., approximately 0.995 fidelity with a physical error rate of 0.1). However, when the distance between the sender and receiver is significant and requires multiple stages of entanglement swapping and purification, as illustrated in Fig. 1, the overhead increases exponentially with the number of relay nodes.

Given these challenges, if overhead is inevitable and qubit transmission is necessary for entanglement distribution, an alternative approach is to encode the transmitted information using QECCs and transmit it in a manner similar to classical communication [21–30]. Nevertheless, quantum teleportation inherently possesses a degree of security because entangled pairs do not contain any information about the transmitted quantum states [8]. Thus, for a fair comparison, security must also be ensured when transmitting encoded quantum states.

In this study, we introduce a novel scheme that encodes quantum states with QECCs and injects uncorrectable errors to enable fault-tolerant and secure long-distance transmission

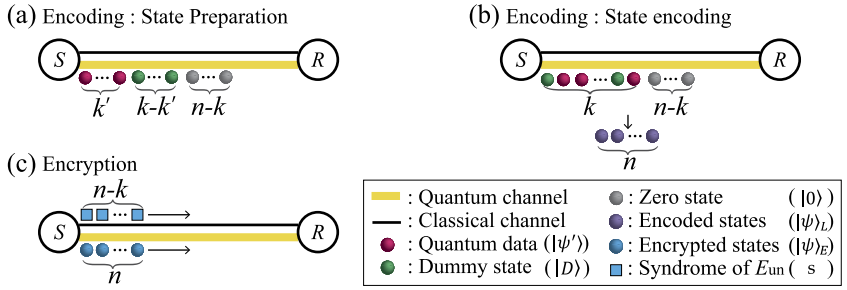

Figure 2 Schematic of the proposed scheme's encoding, and encryption. (a) The sender prepares an arbitrary quantum data $|\psi'\rangle = \sum_{i=0}^{2^{k'}-1} c_i|m_i\rangle$, which is to be transmitted. We assume that the quantum channel is noisy and insecure, while the classical channel is error-free and authenticated. This state is embedded into a larger quantum register by appending mutually unbiased dummy states $|D\rangle = \bigotimes_{i=1}^{k-k'} X^{\boldsymbol{\kappa_i^1}} Z^{\boldsymbol{\kappa_i^2}} H^{\boldsymbol{\kappa_i^3}} |0\rangle^{\otimes k-k'}$ and zero ancillary qubits, yielding $|\psi\rangle = |\psi'\rangle|D\rangle|0\rangle^{\otimes n-k}$. (b) The k' quantum data qubits and $k - k'$ dummy states are randomly shuffled into k slots. This permutation is implemented by the operator $P_{\boldsymbol{\kappa^4}}$, which is determined by a random k-bit key $\boldsymbol{\kappa^4}$ with a Hamming weight of k'. This state is expressed as $|\psi\rangle = U_C|\psi'\rangle|0\rangle^{\otimes n-k'}$, where $U_C = (P_{\boldsymbol{\kappa}^4} \otimes I^{\otimes n-k})(I^{\otimes k'} \otimes U_{MUB} \otimes I^{\otimes n-k})$ denotes the composite operation including permutation and mutually unbiased basis transformation. This state is subsequently encoded using a $[[n, k, d]]$ QECC, yielding the logical state $|\psi\rangle_L = U_E|\psi\rangle$. (c) An uncorrectable error E_{un} is intentionally injected into the logical state to generate the encrypted state $|\psi\rangle_E = E_{un}|\psi\rangle_L$. The sender transmits both the syndrome s corresponding to E_{un} and the encrypted state $|\psi\rangle_E$ to the receiver, who performs syndrome-based decoding and verification to recover the original message

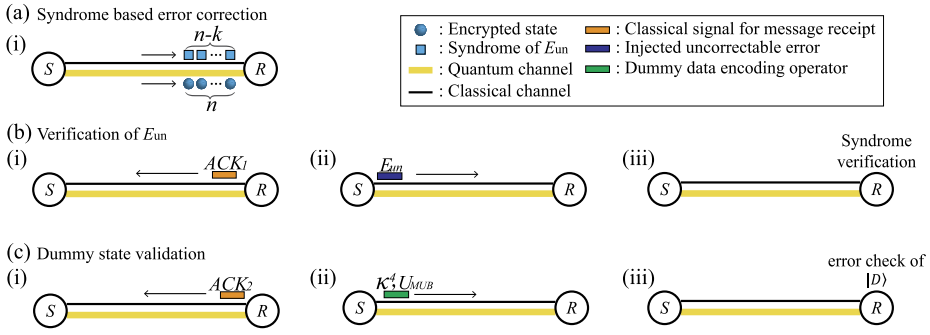

Figure 3 Schematic of the proposed scheme's decryption process: (a-i) The receiver performs syndrome-based error correction on the received encrypted state using the attached syndrome. (b-i) The receiver transmits ACK_1 to notify successful receipt of the state. (b-ii) Upon receiving the acknowledgment, the sender transmits the injected uncorrectable error E_{un} to the receiver. (b-iii) The receiver applies E_{un} and verifies whether an all-zero syndrome is extracted; the protocol is aborted if the syndrome is not a zero vector. (c-i) If verification succeeds, the receiver sends ACK_2 to the sender. (c-ii) The sender then transmits $P_{\boldsymbol{\kappa}^4}$ and U_{MUB}. (c-iii) The receiver uses them to validate the dummy states $|D\rangle$ and check for possible eavesdropping attempts

of arbitrary quantum states. Our approach addresses the limitations of current quantum state transmission methods and provides a scalable solution for quantum communication.

2 Uncorrectable-error-injection-based fault-tolerant and secure quantum communication

In this section, we describe a scheme for transmitting quantum states in a fault-tolerant and secure manner by injecting uncorrectable errors into the encoded states. As illustrated in Fig. 2 and Fig. 3, our proposed scheme consists of four major steps: (1) encoding the

quantum state using a quantum error correction code (QECC), (2) strategically injecting uncorrectable errors to enhance security and fault tolerance, (3) transmitting the encoded state through a noisy and insecure quantum channel, and (4) performing syndrome-based error correction at the receiver to recover the original quantum state while verifying its authenticity.

Additionally, we consider a system model in which an authenticated classical channel is connected between the sender and receiver. The classical channel must be authenticated because the proposed scheme must prevent man-in-the-middle attacks, such as spoofing [31]. We also consider scenarios in which arbitrary quantum states, such as the intermediate results of quantum computing [32], are sent once, rather than repeatedly transmitting the same quantum state. To be precise, this "send-once" constraint applies to the specific combination of a state and the random keys that will be described in the following Sect. 2.1. While the same state $|\psi'\rangle$ cannot be resent using the same set of random keys, re-transmission is permitted with a newly generated set if a verification step fails.

2.1 KeyGen

To transmit arbitrary quantum states, the sender first measures the quantum bit error rate of the quantum channel. Based on this information, the sender determines the error correction capability t of the QECCs and selects an $[[n,k,d]]$ QECC. In this $[[n,k,d]]$ notation, n is the number of physical qubits and k is the number of logical qubits. The code's minimum distance d is selected to provide the required error correction capability t, according to the relation $t = \lfloor (d-1)/2 \rfloor$. To facilitate the security assessment discussed in the Appendix, we consider only non-degenerate quantum codes. A non-degenerate code satisfies the condition that each correctable error yields linearly independent results when applied to elements of the code [25, 28].

Subsequently, the sender generates four bit-strings to create four encryption keys, $\boldsymbol{\kappa^1}$, $\boldsymbol{\kappa^2}$, $\boldsymbol{\kappa^3}$, and $\boldsymbol{\kappa^4}$. The keys $\boldsymbol{\kappa^1}$, $\boldsymbol{\kappa^2}$, and $\boldsymbol{\kappa^3}$ are $(k-k')$-bit strings, each generated independently and uniformly at random. The key $\boldsymbol{\kappa^4}$ is a k-bit string with a Hamming weight of k', generated by selecting k' bit positions uniformly at random and setting them to 1. The roles of these keys are discussed in Sect. 2.2.

2.2 Encoding and encryption

2.2.1 State preparation

The quantum state that the sender wishes to transmit is an arbitrary k'-qubit data $|\psi'\rangle = \sum_{i=0}^{2^{k'}-1} c_i |m_i\rangle$ where $|m_i\rangle$ denotes the computational basis states and c_i are the complex amplitudes associated with the basis states. To prevent an eavesdropper from intercepting the entire quantum state and subsequently transmitting spoofed data—that is, intercept-and-resend attacks—or from extracting information using ancilla states, unitary operations, and measurements, we randomly insert $k-k'$ dummy states $|D\rangle$ into the data sequence. These dummy states are randomly chosen from two sets of mutually unbiased basis (MUB) states: $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$.

At this point, the dummy states $|D\rangle$ are generated using $\boldsymbol{\kappa^1}$, $\boldsymbol{\kappa^2}$, and $\boldsymbol{\kappa^3}$ generated in Sect. 2.1. This can be expressed as

$$|D\rangle = \bigotimes_{i=1}^{k-k'} X^{\boldsymbol{\kappa_i^1}} Z^{\boldsymbol{\kappa_i^2}} H^{\boldsymbol{\kappa_i^3}} |0\rangle^{\otimes k-k'} = U_{MUB} |0\rangle^{\otimes k-k'}, \tag{1}$$

where X and Z are Pauli operators, H is the Hadamard operator, and $X^{\kappa_i^1}$, $Z^{\kappa_i^2}$, and $H^{\kappa_i^3}$ denote operators that apply the respective operation when the corresponding bit in κ^1, κ^2, or κ^3 is 1, and the identity otherwise. For notational simplicity, we define the combined operator as U_{MUB}, which transforms the ancillary zero state into a mutually unbiased basis (MUB) state.

2.2.2 State encoding

The prepared states must be encoded using QECCs to transmit the quantum state reliably. Thus, the n-qubit state $|\psi\rangle$ prepared by the sender for $[[n, k, d]]$ QECC encoding can be expressed as

$$\begin{aligned} |\psi\rangle &= (P_{\boldsymbol{\kappa^4}} \otimes I^{\otimes n-k})|\psi'\rangle U_{MUB}|0\rangle^{\otimes k-k'}|0\rangle^{\otimes n-k}, \\ &= (P_{\boldsymbol{\kappa^4}} \otimes I^{\otimes n-k})(I^{\otimes k'} \otimes U_{MUB} \otimes I^{\otimes n-k})|\psi'\rangle|0\rangle^{\otimes n-k'}, \\ &= U_c|\psi'\rangle|0\rangle^{\otimes n-k'}, \end{aligned} \tag{2}$$

where $P_{\boldsymbol{\kappa^4}}$ is the permutation operator, determined by the key $\boldsymbol{\kappa^4}$ described in Sect. 2.1, that shuffles the k' data and $k - k'$-qubit dummy states $|D\rangle$. U_c denotes the composite operation that combines the permutation $P_{\boldsymbol{\kappa^4}}$ with the MUB transformation U_{MUB}.

The sender encodes the state $|\psi\rangle$ into a logical state using the encoding operator U_E associated with the selected QECC

$$|\psi\rangle_L = U_E|\psi\rangle. \tag{3}$$

2.2.3 State encryption

To perform encryption, a random Pauli error operator E_{un}, which the chosen QECC cannot correct, is injected into the encoded logical state $|\psi\rangle_L$. The uncorrectable error E_{un} is injected into the transmitted state, preventing eavesdroppers or intermediate nodes from obtaining information about the state. Additionally, after receiving the state, the receiver uses it to verify whether the received state is indeed the one sent by the sender, functioning as a signature. These functionalities will be elaborated in Sect. 2.3 and the set of E_{un} that the sender can choose is detailed in the Appendix.

The resulting encoded and encrypted state $|\psi\rangle_E$ is as follows:

$$|\psi\rangle_E = E_{un}|\psi\rangle_L. \tag{4}$$

The sender calculates the syndrome s of the injected E_{un}, then transmits the encoded state $|\psi\rangle_E$ through the quantum channel and transmits the syndrome s through the classical channel to the receiver. We assume that the quantum channel is noisy and insecure, while the classical channel is error-free and authenticated.

2.3 Decryption

2.3.1 Syndrome-based error correction before verification

Upon receiving $|\psi\rangle_E$ and s, the receiver extracts the syndrome of $|\psi\rangle_E$ and performs error correction based on s. Generally, error correction using syndromes is performed based on the all-zero syndrome to revert to an error-free state. However, because the difference between syndromes represents the channel error that has occurred, error correction based on the syndrome s can correct the channel error [33].

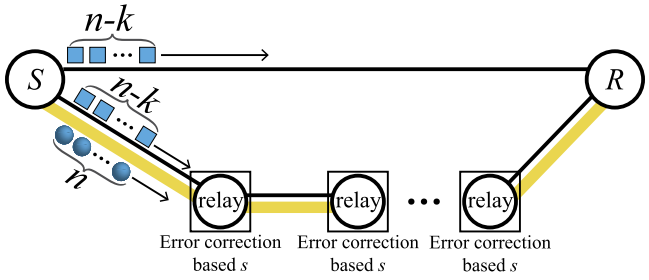

Figure 4 Distance extension of the proposed scheme Relay nodes can perform error correction based on s, ensuring that relay nodes cannot obtain any information about the quantum states

2.3.2 *Verification of E_{un}*

Thereafter, the receiver transmits an ACK_1 to inform the sender that $|\psi\rangle_E$ has been received, where *ACK* (acknowledgment) refers to a signal in data networking that confirms the successful receipt of a transmitted message [34]. Upon receiving the ACK_1, the sender transmits E_{un} to the receiver via a classical channel. The receiver applies E_{un} to $|\psi\rangle_E$ and performs syndrome extraction again to verify if an all-zero syndrome is obtained. If the syndrome is not all-zero, the receiver assumes a potential eavesdropping attack and aborts the process.

2.3.3 *Dummy states validation*

If an all-zero syndrome is extracted, the receiver transmits an ACK_2 to the sender again indicating the extraction of an all-zero syndrome. Upon receiving the ACK_2, the sender transmits a random permutation operator $P_{\kappa 4}$ and U_{MUB} through the classical channel. Subsequently, the receiver measures each mutually unbiased state in the corresponding U_{MUB} to verify the consistency between the results encoded by U_{MUB} and the measurement outcomes. If errors are detected, it is assumed that an eavesdropper attempts to extract information, and the process is aborted.

2.4 Distance extension

The advantage of the proposed approach lies in its ability to extend distance despite encryption, as error correction is still feasible. As illustrated in Fig. 4, similar to the same process that the receiver performs in Sect. 2.3, relay nodes perform error correction based on s, and thereafter pass it to the next node, enabling fault-tolerant transmission. Furthermore, because E_{un} is injected, relay nodes cannot obtain any information regarding the quantum states through syndrome extraction [28].

3 Security analysis

In this section, we analyze the security of the proposed scheme. The only operators that do not affect the syndrome of a quantum state encoded with a quantum error-correcting code are stabilizers and logical operators [28]. Additionally, the dummy states $|D\rangle$ introduced during the state preparation in the proposed scheme can be modified by logical operators. Therefore, if an eavesdropper attempts to extract information using a specific operation or a measurement involving logical ancilla states, the syndrome s of E_{un} or $|D\rangle$ may become corrupted, making such attempts detectable. In other words, even if Eve is assumed to be a computationally unbounded quantum adversary [35], the inability of stabilizers to

reveal logical information ensures that no data can be extracted without disturbing the syndrome or the dummy states. The only case where neither is affected is an attack using stabilizers, but it is well known that such attacks cannot extract information about the quantum state [28]. Therefore, to demonstrate that such forms of attacks can be detected, we first examine countermeasures against *intercept-and-resend attacks*, which serve as an example where the syndrome s alone cannot detect the attack, but $|D\rangle$ enables detection. Additionally, we analyze the accessible information in the proposed scheme to evaluate its security in terms of potential information leakage [36–38]. We demonstrate that as the length of the message k' increases, the potential information leakage can be sufficiently minimized.

3.1 Intercept-and-resend attacks

Intercept-and-resend attacks involve an eavesdropper intercepting the transmitted quantum state $|\psi\rangle_E$ and sending a spoofed quantum state with a spoofed injected error E'_{un} that matches the syndrome s to the receiver, masquerading as the sender. Thereafter, the eavesdropper intercepts the E_{un} sent by the legitimate sender to extract information from $|\psi\rangle_E$.

This attack can be detected because when the receiver applies the received E_{un} to the spoofed quantum state of the eavesdropper, the difference between E_{un} and E'_{un} results in a non-zero syndrome during the subsequent syndrome extraction. In this case, it could be problematic if the eavesdropper retains the information of $|\psi'\rangle$ using the intercepted quantum state and E_{un}.

To prevent this, dummy states $|D\rangle$ defined in MUBs are mixed with $|\psi'\rangle$, and this information is only disclosed when the sender receives the ACK_1 indicating an all-zero syndrome. This permutation-based security relies on P_{κ^4}, that is, the number of all possible combinations of the key κ^4, denoted as $|\kappa^4|$ [39, 40]. In the proposed scheme, the probability that an eavesdropper can extract $|\psi'\rangle$ is $\binom{k}{k'}^{-1}$.

3.2 Accessible information available to the eavesdropper

To derive accessible information, we adopt the perspective of the eavesdropper. Since the eavesdropper knows neither the arbitrary quantum data being sent nor the random keys used for encryption, the state is indistinguishable from a uniform mixture of all possible data. This modeling clarifies that the security relies on the randomness of the encryption keys, not on any assumption that the message itself must be random. In addition, because of the influence of the data and randomly permuted dummy states $|D\rangle$ defined in MUBs, E_{un} appears as a state in which all possible Pauli error patterns are mixed. Thus, when considering only the data, uncorrectable error applied to the state differs from the actual injected E_{un}. This can be mathematically verified as

$$\begin{aligned} |\psi\rangle_E &= E_{un}U_E U_c|\psi'\rangle|0\rangle^{\otimes n-k'}, \\ &= E_{un}U'_c U_E|\psi'\rangle|0\rangle^{\otimes n-k'}, \end{aligned} \tag{5}$$

where $U'_c = U_E U_c U_E^{-1}$. Thus, although the eavesdropper can narrow down the candidate E_{un} based on the syndrome information s, they must identify $E_{un}U'_c$, which necessitates the consideration of all possible Pauli error patterns [39, 40].

Consequently, the description of the quantum state after the receiver's error correction process perceived by the eavesdropper, ρ_E,

$$\rho_E = \frac{1}{2^{k'}} \frac{1}{4^n} \sum_{i=0}^{2^{k'}-1} \sum_{\mathbf{j},\mathbf{k}\in\{0,1\}^n} X^{\mathbf{j}} Z^{\mathbf{k}} |\psi\rangle_{L,i} \langle\psi|_{L,i} Z^{\mathbf{k}} X^{\mathbf{j}}, \tag{6}$$

where $|\psi\rangle_{L,i}$ denotes the logical basis for $|m_i\rangle$, and the vectors $\mathbf{j}, \mathbf{k} \in \{0,1\}^n$ are n-bit binary strings that specify the locations of the Pauli X and Z operators, respectively.

The accessible information is defined as the maximum mutual information, $I_{acc}(M;E)$,

$$I_{acc}(M;E) = \max_{\Lambda} I(M;Y). \tag{7}$$

where M is the message of the sender, E is system of the eavesdropper, and Y is a random variable obtained from the measurements Λ of the eavesdropper. According to the convexity of mutual information, the maximum can be achieved through a positive operator-valued measure, $\{\Lambda_y\}$ with rank-one elements, such that $\Lambda_y \geq 0$, $\sum_y \Lambda_y = \mathbb{I}$ [37, 41],

$$\Lambda_y = \mu_y |\phi_y\rangle\langle\phi_y|, \tag{8}$$

where $|\phi_y\rangle$ are unit vectors and μ_y are positive numbers such that $\sum_y \mu_y = 2^n$.

The measurement results follow the probability distribution:

$$p_Y(y) = \mu_y \langle\phi_y|\rho_E|\phi_y\rangle. \tag{9}$$

For a given m, one of the entire basis of $|\psi'\rangle$, the conditional probability of a measurement outcome is

$$p_{Y|M=m}(y) = \mu_y \langle\phi_y|\rho_E^m|\phi_y\rangle. \tag{10}$$

with

$$\rho_E^m = \frac{1}{4^n} \sum_{\mathbf{j},\mathbf{k}\in\{0,1\}^n} X^{\mathbf{j}} Z^{\mathbf{k}} |\psi\rangle_L \langle\psi|_L Z^{\mathbf{k}} X^{\mathbf{j}}. \tag{11}$$

The accessible information is given by

$$\begin{aligned} I_{acc}(M;E) &= \max_{\Lambda} \{ -\sum_y p_Y(y) \log p_Y(y) \\ &\quad + \frac{1}{2^{k'}} \sum_{y,m} p_{Y|M=m}(y) \log p_{Y|M=m}(y) \}, \\ &= \max_{\Lambda} \sum_y \mu_y \{ -\langle\phi_y|\rho_E|\phi_y\rangle \log \langle\phi_y|\rho_E|\phi_y\rangle \\ &\quad + \frac{1}{2^{k'}} \sum_m \langle\phi_y|\rho_E^m|\phi_y\rangle \log \langle\phi_y|\rho_E^m|\phi_y\rangle \}, \end{aligned} \tag{12}$$

where the term μ_y inside the logarithm in equation (12) can be canceled out using the relationship between equations (9) and (10).

From the perspective of an eavesdropper, errors are perceived as maximally mixed. Therefore, the higher the effective code rate, $R_{\text{eff}} = k'/n$—which can differ from the code rate $R = k/n$ due to the presence of $k - k'$ dummy qubits—the closer ρ_E and ρ_E^m approach maximally mixed states (MMSs).

By applying the results in [38] with the matrix Chernoff bound and Maurer bound,

$$\langle\phi|\rho_E|\phi\rangle \leq (1+\epsilon)2^{-n}, \tag{13}$$

$$\langle\phi|\rho_E^m|\phi\rangle \geq (1-\epsilon)2^{-n}. \tag{14}$$

Then, by substituting equation (13) and (14) into equation (12), the accessible information can be obtained as

$$I_{acc}(M;E) \leq 2\epsilon n, \tag{15}$$

where $\epsilon > 0$. As k' and n increase, ρ_E and ρ_E^m asymptotically approach MMSs, ensuring that any accessible information for an eavesdropper becomes increasingly randomized. This strengthens security by making the extracted information less distinguishable from noise. However, since the total message length scales with n, the absolute amount of leaked information also increases. This is an inherent effect of encoding a larger message rather than a weakness of the scheme, as the fraction of leaked information relative to the total message content continues to decrease. Therefore, the quantum state can be transmitted using the proposed scheme while ensuring that the information leaked to the eavesdropper remains sufficiently negligible.

4 Resource and fidelity analysis

In this section, we present a comparative analysis of the resource overhead and fidelity between a long-distance entanglement distribution (LDED) scheme and the proposed scheme. We acknowledge that both channel errors and qubit loss are major sources of error in long-distance quantum communication. The proposed scheme, based on QECCs, is capable of correcting both types of errors. A general $[[n,k,d]]$ code can correct up to $t = \lfloor (d-1)/2 \rfloor$ Pauli errors with unknown locations. Alternatively, it can correct up to $d-1$ erasure errors (losses) whose locations are known [42]. For a channel with both, it can correct a combination of t Pauli errors and r erasures provided that $2t + r < d$ [43]. However, from a security standpoint, the most relevant threat model involves an eavesdropper's attack, which more closely resembles a channel characterized by Pauli errors. For this reason, our primary comparative analysis focuses on the depolarizing channel. A specific analysis of our scheme's logical error rate in a channel with both depolarizing errors and qubit loss is provided in the Appendix B.

4.1 Resource overhead modeling

This section presents a modeling-based analysis of the resource overhead incurred by the LDED, focusing on entanglement swapping and purification over a linear chain network. We subsequently apply the derived overhead to evaluate the performance of the proposed scheme in terms of fidelity under comparable resource conditions. We consider the LDED

over a linear chain network consisting of $2^N + 1$ nodes. This architecture requires entanglement swapping and purification to maintain high fidelity.

Let N_{EP} denote the number of ancillary qubits required for entanglement purification. Assuming all entanglement swapping operations succeed, the purification overhead is given by:

$$N_{EP} = \sum_{i=0}^{N} N_A 2^{N-i} \times 2, \tag{16}$$

where N_A is the number of ancilla qubits for a single purification step.

The number of BSMs required for entanglement swapping is:

$$O_{ES} = \sum_{i=1}^{N} 2^{N-i}. \tag{17}$$

To increase the BSM success probability, $P_{ES} = 1 - 1/2^{n_{bsm}}$, we employ logical BSMs. The probability that all O_{ES} BSMs succeed is $(1 - 1/2^{n_{bsm}})^{O_{ES}}$, and the number of repetitions required for at least one successful attempt is:

$$\left\lceil \left(\frac{2^{n_{bsm}}}{2^{n_{bsm}} - 1} \right)^{O_{ES}} \right\rceil. \tag{18}$$

The total number of qubits N_T required for one successful LDED is:

$$N_T = (N_{EP} + 2O_{ES}(n_{bsm} - 1)) \times \left\lceil \left(\frac{2^{n_{bsm}}}{2^{n_{bsm}} - 1} \right)^{O_{ES}} \right\rceil. \tag{19}$$

4.2 Fidelity estimation

Using the resource overhead analyzed in the previous section, we evaluate the transmission fidelity achieved by the proposed scheme and compare it with that of the LDED involving entanglement swapping and purification.

We consider a noise model in which only depolarizing noise is applied at the final purification stage. All preceding steps in the LDED scheme—such as entanglement generation, entanglement swapping, intermediate purification, and state preparation—are assumed to be noiseless. Likewise, gate operations and measurements in both schemes are also treated as ideal. These assumptions are introduced to enable a direct comparison between the two schemes under a controlled setting.

For the proposed scheme, the fidelity is approximated based on the logical error probability p_L of a quantum stabilizer code. Under a depolarizing channel with physical error rate p, the logical error probability is given by [44]:

$$p_L = 1 - \sum_{i=0}^{t} \binom{N_T}{i} p^i (1-p)^{N_T - i}. \tag{20}$$

To estimate t, we apply the quantum Singleton bound [45],

$$N_T - k \geq 2(d-1), \tag{21}$$

which we reformulate as:

$$\frac{N_T - k}{4} \geq t. \tag{22}$$

Assuming a code rate $R = 1/2$, the lower bound on p_L becomes:

$$p_L \geq 1 - \sum_{i=0}^{\lfloor N_T/8 \rfloor} \binom{N_T}{i} p^i (1-p)^{N_T - i}, \tag{23}$$

and the fidelity of the proposed scheme is accordingly approximated as:

$$F_{\text{our}} \approx \sum_{i=0}^{\lfloor N_T/8 \rfloor} \binom{N_T}{i} p^i (1-p)^{N_T - i}. \tag{24}$$

For the LDED, assuming that the initial Bell state is prepared as the $|\Phi^+\rangle$ state and each qubit is independently subject to depolarizing noise, the resulting initial fidelity is given by $F_{\text{ini}} = (1-p)^2 + \frac{p^2}{3}$, where p denotes the physical error rate. The fidelity expression is derived based on the model in Ref. [17], which demonstrates high purification performance even with a small number of ancilla qubits, and is given by:

$$F_{\text{LDED}} = \frac{(F_{\text{ini}})^{N_A+1}}{(F_{\text{ini}})^{N_A+1} + (1 - F_{\text{ini}})^{N_A+1}}. \tag{25}$$

4.3 Comparative performance analysis

To provide a practical and quantitative comparison between the proposed scheme and the LDED scheme, we evaluate their fidelity performance using the analytic models derived in Sect. 4.2. We assume a network consisting of five nodes (i.e., $N = 2$), and consider LDED configurations with $N_A = 2$, 3, and 4 ancillary Bell states per end node. The fidelity of each configuration is computed using the closed-form expressions for F_{our} and F_{LDED}, and the resulting fidelity trends across different physical error rates p are shown in Fig. 5.

To further investigate the trade-off between fidelity and total qubit overhead, we fix the physical error rate p and evaluate how the fidelity scales with N_T. Figure 6 presents the results for three representative values of p (0.01, 0.03, and 0.05), illustrating the behavior of both schemes across different noise levels. At lower error rates (e.g., $p = 0.01$ or 0.03), the proposed scheme achieves high fidelity with substantially fewer qubits than LDED. As p increases, the required overhead to maintain comparable fidelity also increases, narrowing the performance gap between the two schemes. These results indicate that the proposed approach is particularly advantageous in low-noise regimes, offering strong fidelity with reduced resource requirements.

As a simple example, consider the case where $N_A = 2$, $p = 0.01$, $n_{\text{bsm}} = 2$, and the total number of nodes is 5. In this setting, the number of qubits required for entanglement purification is $N_{\text{EP}} = 28$, resulting in a total resource count of $N_T = 102$. The fidelity achieved by our scheme is $F_{\text{our}} \approx 1 - 4.08 \times 10^{-11}$, while the LDED achieves $F_{\text{LDED}} \approx 1 - 8.33 \times 10^{-6}$. Notably, even with just $N_T = 40$ qubits, the proposed scheme achieves $F_{\text{our}} \approx 1 - 2.87 \times 10^{-6}$, surpassing the LDED in fidelity. Table 1 summarizes a set of representative scenarios comparing the proposed scheme and the LDED under various

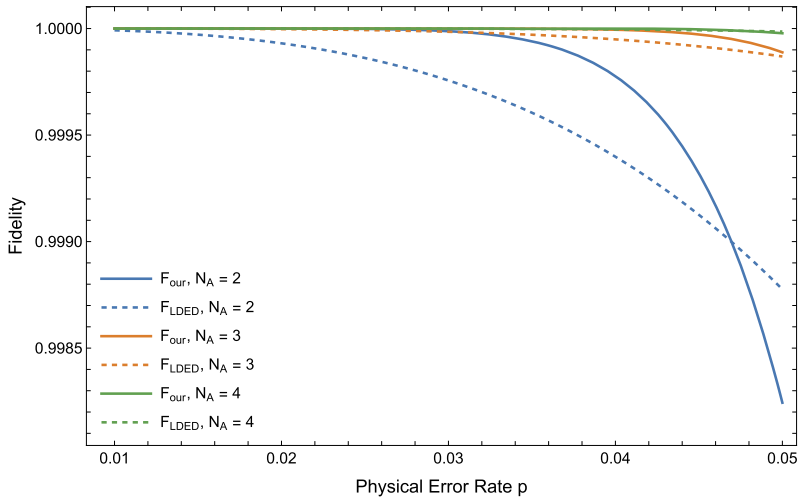

Figure 5 Fidelity comparison between $F_{\mathbf{our}}$ and F_{LDED} with varying purification resource levels ($N_A = 2$, 3, and 4). The network consists of five nodes (i.e., $N = 2$), and the Bell state measurement parameter is $n_{\mathbf{bsm}} = 2$. Solid lines indicate $F_{\mathbf{our}}$, and dashed lines indicate F_{LDED}. The results show that in the low-error regime, the proposed scheme achieves higher fidelity

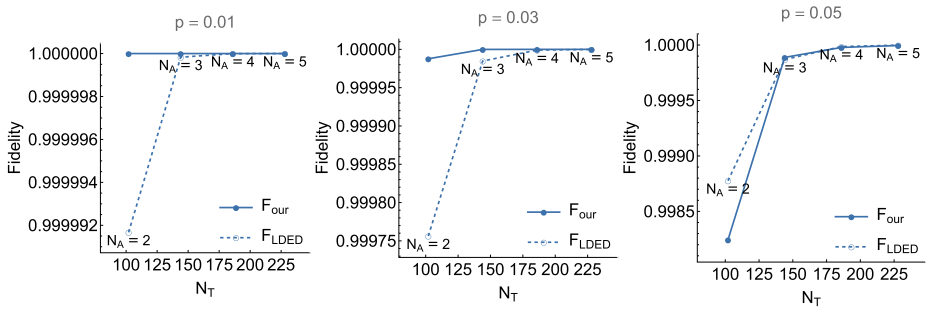

Figure 6 Fidelity as a function of total qubit overhead (N_T with $N_A = 2, 3, 4, 5$) for $F_{\mathbf{our}}$ and F_{LDED} under various physical error rates ($p = 0.01$, 0.03, and 0.05). The results illustrate that the proposed scheme achieves high fidelity with lower overhead in low-noise regimes

values of p, N_A and network size N. In each case, the proposed method achieves comparable or superior fidelity while requiring significantly fewer physical qubits. The last column quantifies this advantage, showing that our scheme can reduce qubit requirements by more than 60% to 90% in low-error regimes, with minimal or even improved fidelity loss. Such results highlight the resource-efficiency of our approach, requiring substantially fewer physical qubits in low-error regimes.

5 Conclusion

In this study, we proposed a novel fault-tolerant and secure quantum communication scheme leveraging uncorrectable error injection. Unlike conventional quantum teleportation-based approaches, which require entanglement distribution, entanglement swapping, and purification, our method eliminates the need for pre-distributed entanglement while ensuring secure and fault-tolerant quantum state transmission. By encoding quantum states with QECCs and introducing uncorrectable errors, we enhanced both

Table 1 Comparison of fidelity and resource overhead between the proposed scheme and the LDED under $n_{\mathrm{bsm}} = 2$ and different parameter settings. "Enhanced efficiency" refers to configurations where the proposed scheme achieves slightly higher fidelity than the LDED while using the minimum number of qubits. "Resource reduction" denotes the percentage of qubit savings achieved relative to the LDED baseline

Scheme	p	N	N_T	Fidelity	Resource reduction (%)
LDED (baseline)	0.01	2	102	$1 - 8.33 \times 10^{-6}$	60.78
Proposed (matched resource)			102	$1 - 4.08 \times 10^{-11}$	
Proposed (enhanced efficiency)			40	$1 - 2.87 \times 10^{-6}$	
LDED (baseline)	0.02	3	779	$1 - 2.85 \times 10^{-6}$	90.76
Proposed (matched resource)			779	$1 - 1.32 \times 10^{-14}$	
Proposed (enhanced efficiency)			72	$1 - 1.77 \times 10^{-6}$	
LDED (baseline)	0.03	2	113	$1 - 1.52 \times 10^{-5}$	22.12
Proposed (matched resource)			113	$1 - 1.61 \times 10^{-6}$	
Proposed (enhanced efficiency)			88	$1 - 1.31 \times 10^{-5}$	
LDED (baseline)	0.03	3	1003	$1 - 9.52 \times 10^{-7}$	88.04
Proposed (matched resource)			1003	$1 - 2.81 \times 10^{-14}$	
Proposed (enhanced efficiency)			120	$1 - 6.92 \times 10^{-7}$	

the fault tolerance and security of the transmission process while reducing the resource overhead associated with entanglement management.

Our security analysis demonstrated that the proposed scheme is resilient against intercept-and-resend attacks, as unauthorized modifications to the transmitted state can be detected through syndrome extraction and verification. Furthermore, the presence of uncorrectable errors prevents an eavesdropper from extracting meaningful information from an intercepted state. The comparative performance analysis confirmed that the proposed scheme effectively reduces the overhead associated with quantum state transmission while maintaining high fidelity in low physical error regimes. By eliminating the complexities of entanglement distribution and minimizing the number of required quantum operations, our approach provides a resource-efficient solution for long-distance quantum communication. These findings indicate that the proposed approach offers a scalable and practical alternative to conventional quantum state transmission methods, particularly in large-scale quantum networks.

Future research could focus on experimentally validating the proposed scheme using near-term quantum hardware or by employing existing quantum network simulation tools, as well as integrating it into emerging quantum communication frameworks, including quantum key distribution and quantum repeaters. While the current security analysis addresses representative attack scenarios, extending the evaluation to include more sophisticated quantum adversaries will further strengthen the protocol's robustness. In addition, exploring optimization strategies for encoding efficiency and analyzing the trade-offs between security and fidelity across diverse quantum network configurations will be valuable for enhancing practical deployment. A comprehensive comparative analysis against LDED schemes including qubit loss also remains a crucial future work. Moreover, investigating the interplay between our scheme and high-throughput frameworks, such as multicarrier CV-QKD systems, presents a promising research avenue [46, 47]. By further refining the method and broadening its applicability, this research can contribute to the advancement of secure, scalable, and fault-tolerant quantum networking technologies.

Appendix A: Analysis of number of uncorrectable errors

In this section, we discuss the number of uncorrectable errors for encryption. The security of the proposed scheme is primarily determined by the number of uncorrectable errors assigned to each syndrome. The number of uncorrectable errors assigned to a syndrome, N_u, can be estimated as follows:

$$N_u \sim \frac{4^n - \sum_{i=0}^{t} 3^i \binom{n}{i}(2^{n-k} + 2^{2k})}{2^{n-k}} \times \frac{1}{2^{n-k}}. \tag{A.1}$$

where 4^n of equation (A.1) represents the number of all Pauli error patterns of length n, and $\sum_{i=0}^{t} 3^i \binom{n}{i}$ denotes the number of all errors that the QECCs can correct. For simplicity, we refer to this as N_c. The subsequent terms multiplied by N_c represents the number of errors with different weights sharing the same syndrome as correctable errors within N_c. Between these terms, 2^{n-k} represents the total number of stabilizers. When multiplied by N_c, it represents errors that share the same syndrome and behavior as correctable errors within N_c. The value 2^{2k} represents the total number of logical Pauli operators. When it is multiplied by N_c, it represents errors that share the same syndrome but have different behaviors because of logical operators, thereby being uncorrectable. In other words, the numerator represents the total number of errors associated with uncorrectable syndromes. Errors with uncorrectable syndromes, even when multiplied by stabilizers, exhibit the same behavior and syndrome. Therefore, they should be considered as single errors. To account for this, we adjusted by dividing by the total number of stabilizers, 2^{n-k}, which served as the denominator. The final $\frac{1}{2^{n-k}}$ term was used to calculate the average number of uncorrectable errors allocated to each syndrome. Here, 2^{n-k} represents the total number of syndromes which are bit strings of length $n-k$. Using this information, the approximate number of completely different errors, denoted as N_u, that share the same syndrome as any given uncorrectable error could be determined. N_c was substituted with a term containing n and k using the Hamming bound for QECCs [48]. The quantum Hamming bound is expressed as

$$\begin{aligned} n - k &\geq \log \sum_{i=0}^{t} 3^i \binom{n}{i}, \\ 2^{n-k} &\geq \sum_{i=0}^{t} 3^i \binom{n}{i}. \end{aligned} \tag{A.2}$$

Rearranging equation (A.1) yields

$$\begin{aligned} N_u &\geq \frac{4^n - 2^{n-k}(2^{n-k} + 2^{2k})}{2^{n-k}} \times \frac{1}{2^{n-k}} \\ &\geq 2^{2k} - 2^{n-k}(2^{k-n} + 2^{4k-2n}). \end{aligned} \tag{A.3}$$

By substituting the code rate $k/n = R$, equation (A.3) can be revised as,

$$N_u \geq 2^{2Rn}(1 - (\frac{1}{2})^{(1-R)n}) - 1. \tag{A.4}$$

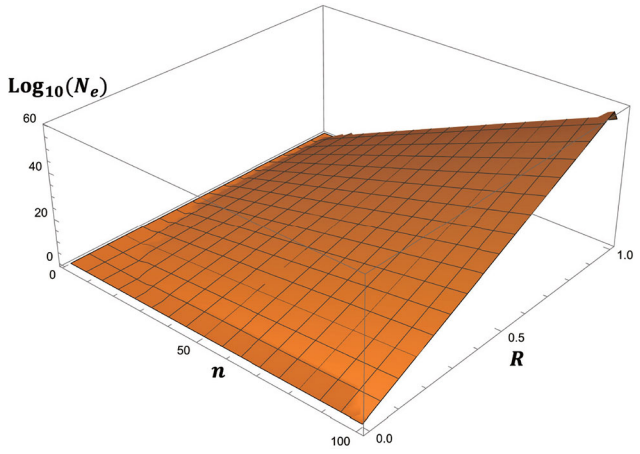

Figure 7 Security analysis graph This graph illustrates the order of the average number of distinct uncorrectable errors N_u with the same syndrome as equation (A.5)

When n is sufficiently large, equation (A.4) can be approximated as follows:

$$N_u = \begin{cases} \lfloor 2^{2Rn} - 1 \rfloor, & \text{if } 2^{2Rn} \geq 1, \\ 0, & \text{if } 2^{2Rn} < 1. \end{cases} \tag{A.5}$$

As expressed in equation (A.5), the graph of N_u over the range $1 \leq n \leq 100$ is shown in Fig. 7. To ensure adequate security, QECCs with sufficiently large n, R should be used. As mentioned in Sect. 4.3, for the case with a total of 5 nodes and 102 required qubits, the number of N_u when $R = 0.5$ is approximately 5.0706×10^{30}.

Appendix B: Analysis of logical error rate with errors and qubit losses

In this section, we discuss the logical error rate for the proposed scheme under a channel with both Pauli errors and qubit losses, as mentioned in Sect. 4. Let the physical error rate be denoted by p and the probability of a qubit loss (erasure) by l. Then the logical error rate, P_L, for an $[[n,k,d]]$ code under these conditions is given by:

$$\begin{aligned} p_L &= \sum_{r=0}^{n} \sum_{t=t_{\min}(r)}^{n-r} \binom{n}{r} \binom{n-r}{t} l^r (1-l)^{n-r} \left(\frac{p}{1-l}\right)^t \left(1 - \frac{p}{1-l}\right)^{n-r-t}, \\ &= \sum_{r=0}^{n} \sum_{t=t_{\min}(r)}^{n-r} \binom{n}{r} \binom{n-r}{t} l^r p^t (1-l-p)^{n-r-t}, \end{aligned} \tag{B.1}$$

where the minimum number of Pauli errors required to cause a logical error, $t_{\min}(r)$, depends on the number of qubit losses r and is given by $t_{\min}(r) = \max\left(0, \left\lceil \frac{d-r}{2} \right\rceil\right)$. This formula calculates the total logical error rate by summing the probabilities of all possible uncorrectable error events. The summation over r considers all possible numbers of qubit losses, from 0 to n. For a fixed number of losses r, the term $\binom{n}{r} l^r (1-l)^{n-r}$ gives the binomial probability of exactly r losses occurring. The summation over t then computes the probability of an uncorrectable error on the remaining $n-r$ qubits. An uncorrectable error occurs if

the number of Pauli errors t meets or exceeds the required threshold $t_{\min}(r)$. This probability is given by the second binomial term, which uses the conditional probability $p/(1-l)$ for a Pauli error to occur on a qubit given that it was not erased.

Acknowledgements
This research was supported by Korea Institute of Science and Technology Information (KISTI). (No. K25L5M2C2). This research was supported by the National Research Council of Science & Technology (NST) grant by the Korea government (MSIT) (No. CAP22053-000). K.J. acknowledges support by the National Research Foundation of Korea (NRF) through a grant funded by the Ministry of Science and ICT (Grant No. RS-2025-00515537), the Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korean government (MSIP) (Grant No. RS-2025-02304540), and the National Research Council of Science & Technology (NST) (Grant No. GTL25011-401).

Author contributions
These authors contributed equally to this work.

Funding information
Not applicable.

Data availability
No datasets were generated or analysed during the current study.

Materials availability
Not applicable.

Code availability
Not applicable.

Declarations

Ethics approval and consent to participate
This work poses no ethical issues or challenges and is rightfully in line with the format for writing manuscripts or articles. All authors consent to participate in this research or paper.

Consent for publication
All authors consent to publish this research or paper.

Competing interests
The authors declare no competing interests.

Author details
[1]Quantum Network Research Center, Korea Institute of Science and Technology Information, Daejeon, 34141, Republic of Korea. [2]Research Institute of Mathematics, Seoul National University, Seoul, 08826, Republic of Korea. [3]School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 02455, Republic of Korea.

Received: 19 April 2025 Accepted: 13 October 2025 Published online: 11 November 2025

References

1. Kimble HJ. The quantum Internet. Nature. 2008;453(7198):1023–30.
2. Wehner S, Elkouss D, Hanson R. Quantum Internet: a vision for the road ahead. Science. 2018;362(6412):9288.
3. Cacciapuoti AS, Caleffi M, Tafuri F, Cataliotti FS, Gherardini S, Bianchi G. Quantum Internet: networking challenges in distributed quantum computing. IEEE Netw. 2019;34(1):137–43.
4. Gyongyosi L, Imre S. Advances in the quantum Internet. Commun ACM. 2022;65(8):52–63.
5. Gyongyosi L, Imre S. Networked quantum services. Quantum Inf Comput. 2025;25(2025):97–140.
6. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett. 1993;70(13):1895.
7. Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurter H, Zeilinger A. Experimental quantum teleportation. Nature. 1997;390(6660):575–9.
8. Pirandola S, Eisert J, Weedbrook C, Furusawa A, Braunstein SL. Advances in quantum teleportation. Nat Photonics. 2015;9(10):641–52.
9. Zukowski M, Zeilinger A, Horne M, Ekert A. "event-ready-detectors" bell experiment via entanglement swapping. Phys Rev Lett. 1993;71(26):4287.
10. Goebel AM, Wagenknecht C, Zhang Q, Chen Y-A, Chen K, Schmiedmayer J, Pan J-W. Multistage entanglement swapping. Phys Rev Lett. 2008;101(8):080403.
11. Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett. 1996;76(5):722.
12. Bennett CH, Bernstein HJ, Popescu S, Schumacher B. Concentrating partial entanglement by local operations. Phys Rev A. 1996;53(4):2046.
13. Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A. Quantum privacy amplification and the security of quantum cryptography over noisy channels. Phys Rev Lett. 1996;77(13):2818.

14. Rozpedek F, Schiet T, Thinh LP, Elkouss D, Doherty AC, Wehner S. Optimizing practical entanglement distillation. Phys Rev A. 2018;97(6):062333.
15. Zhao X, Zhao B, Wang Z, Song Z, Wang X. Practical distributed quantum information processing with loccnet. npj Quantum Inf. 2021;7(1):159.
16. Jansen S, Goodenough K, Bone S, Gijswijt D, Elkouss D. Enumerating all bilocal Clifford distillation protocols through symmetry reduction. Quantum. 2022;6:715.
17. Kim J, Seo S, Yun J, Bae J. Static quantum errors and purification. 2024. arXiv preprint. arXiv:2405.06291.
18. Weber M. Experimental quantum memory applications and demonstration of an elementary quantum repeater link with entangled light-matter interfaces. München: Ludwig-Maximilians-Universität; 2012.
19. Lee S-W, Ralph TC, Jeong H. Fundamental building block for all-optical scalable quantum networks. Phys Rev A. 2019;100(5):052303.
20. Lee S-H, Lee S-W, Jeong H. Loss-tolerant concatenated bell-state measurement with encoded coherent-state qubits for long-range quantum communication. Phys Rev Res. 2021;3(4):043205.
21. Shor PW. Scheme for reducing decoherence in quantum computer memory. Phys Rev A. 1995;52(4):2493.
22. Calderbank AR, Shor PW. Good quantum error-correcting codes exist. Phys Rev A. 1996;54(2):1098.
23. Steane AM. Simple quantum error-correcting codes. Phys Rev A. 1996;54(6):4741.
24. Steane AM. Active stabilization, quantum computation, and quantum state synthesis. Phys Rev Lett. 1997;78(11):2252.
25. Calderbank AR, Rains EM, Shor PM, Sloane NJ. Quantum error correction via codes over gf (4). IEEE Trans Inf Theory. 1998;44(4):1369–87.
26. Knill E, Laflamme R, Zurek WH. Resilient quantum computation: error models and thresholds. Proc R Soc Lond, Ser A, Math Phys Eng Sci. 1998;454(1969):365–84.
27. Knill E. Quantum computing with realistically noisy devices. Nature. 2005;434(7029):39–44.
28. Gottesman D. An introduction to quantum error correction and fault-tolerant quantum computation. In: Quantum information science and its contributions to mathematics, proceedings of symposia in applied mathematics. vol. 68. 2010. p. 13–58.
29. Terhal BM. Quantum error correction for quantum memories. Rev Mod Phys. 2015;87(2):307–46.
30. Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. IEEE Commun Surv Tutor. 2018;20(2):1149–205.
31. Abidin A. Authentication in quantum key distribution: security proof and universal hash functions. PhD thesis. Linköping University Electronic Press; 2013.
32. Gyongyosi L, Imre S. Scalable distributed gate-model quantum computers. Sci Rep. 2021;11(1):5172.
33. Beutelspacher A, Rosenbaum U. Projective geometry: from foundations to applications. Cambridge: Cambridge University Press; 1998.
34. Lin S, Costello DJ, Miller MJ. Automatic-repeat-request error-control schemes. IEEE Commun Mag. 1984;22(12):5–17.
35. Watrous J. The theory of quantum information. Cambridge university press; 2018.
36. Schumacher B. Information from quantum measurements. In: Complexity, entropy and the physics of information. 1990. p. 29–37.
37. DiVincenzo DP, Horodecki M, Leung DW, Smolin JA, Terhal BM. Locking classical correlations in quantum states. Phys Rev Lett. 2004;92(6):067902.
38. Huang Z, Kok P, Lupo C. Fault-tolerant quantum data locking. Phys Rev A. 2021;103(5):052611.
39. Ouyang Y, Rohde PP. A general framework for the composition of quantum homomorphic encryption & quantum error correction. 2022. arXiv preprint. arXiv:2204.10471.
40. Sohn I, Kim B, Bae K, Song W, Lee W. Error-correctable efficient quantum homomorphic encryption using calderbank–shor–steane codes. Quantum Inf Process. 2025;24(2):28.
41. Peres A. Quantum theory: concepts and methods. vol. 72. Berlin: Springer; 1997.
42. Grassl M, Beth T, Pellizzari T. Codes for the quantum erasure channel. Phys Rev A. 1997;56(1):33.
43. Delfosse N, Nickerson NH. Almost-linear time decoding algorithm for topological codes. Quantum. 2021;5:595.
44. Forlivesi D, Valentini L, Chiani M. Performance analysis of quantum css error-correcting codes via macwilliams identities. 2023. arXiv preprint. arXiv:2305.01301.
45. Knill E, Laflamme R. Theory of quantum error-correcting codes. Phys Rev A. 1997;55(2):900.
46. Gyongyosi L, Imre S. Multiple access multicarrier continuous-variable quantum key distribution. Chaos Solitons Fractals. 2018;114:491–505.
47. Gyongyosi L. Multicarrier continuous-variable quantum key distribution. Theor Comput Sci. 2020;816:67–95.
48. Ekert A, Macchiavello C. Quantum error correction for communication. Phys Rev Lett. 1996;77(12):2585.

Publisher's note