

Resource Reduction in Multiparty Quantum Secret Sharing of both Classical and Quantum Information under Noisy Scenario

Nirupam Basak^{1,*} and Goutam Paul^{1,†}

¹*Cryptography and Security Research Unit, Indian Statistical Institute, Kolkata 700108, India*

(Dated: April 24, 2025)

Quantum secret sharing (QSS) enables secure distribution of information among multiple parties but remains vulnerable to noise. We analyze the effects of bit-flip, phase-flip, and amplitude damping noise on the multiparty QSS for classical message (QSSCM) and secret sharing of quantum information (SSQI) protocols proposed by Zhang et al. (Phys. Rev. A, 71:044301, 2005). To scale down these effects, we introduce an efficient quantum error correction (QEC) scheme based on a simplified version of Shor's code. Leveraging the specific structure of the QSS protocols, we reduce the qubit overhead from the standard 9 of Shor's code to as few as 3 while still achieving lower average error rates than existing QEC methods. Thus, our approach can also be adopted for other single-qubit-based quantum protocols. Simulations demonstrate that our approach significantly enhances the protocols' resilience, improving their practicality for real-world deployment.

I. INTRODUCTION

Consider a national government operating a secure server that hosts highly sensitive data vital to national security. Any mishandling or unauthorized access to this information could lead to catastrophic consequences, underscoring the risk of entrusting the server's passkey to a single individual. This prompts a fundamental question: *how can the passkey be stored securely?* A promising solution is to divide the passkey among multiple trusted personnel, such that only a designated subset can collaboratively reconstruct and access it. Implementing this approach necessitates robust protocols for both secure distribution and reliable reconstruction of the key. Secret sharing protocols [1–6] offer a well-established framework to address this challenge.

Traditional secret sharing schemes derive their security from the computational hardness of certain mathematical problems, including polynomial interpolation, integer factorization, and discrete logarithms [4, 5, 7]. However, the advent of quantum computing poses a significant threat to these classical foundations, as quantum algorithms are capable of efficiently solving problems that underpin the security of these schemes [8, 9].

Quantum Secret Sharing (QSS)[10–17], by contrast, harnesses the principles of quantum mechanics—such as superposition and entanglement—to distribute secrets in a fundamentally different manner. Instead of depending on the computational hardness of mathematical problems, QSS leverages intrinsic quantum properties[18, 19] to provide enhanced security. This makes QSS particularly compelling in the emerging quantum era, where conventional cryptographic methods may be rendered ob-

solete by powerful quantum algorithms.

In a QSS protocol, the secret is encoded into multiple quantum bits (qubits) and distributed among participants. Due to the nature of quantum mechanics, a participant holding only one share cannot extract any meaningful information about the secret without disturbing the quantum system, making unauthorized observation or interception detectable [19, 20]. To recover the original secret, a predefined minimum number of participants must collaborate and perform coordinated quantum operations on their respective shares. A QSS scheme that distributes the secret among n parties and requires at least k of them to reconstruct it is referred to as an (n, k) -QSS scheme.

Quantum noise [21–23] poses a major challenge to QSS, as it can disturb the fragile quantum states that the system relies on [22, 24, 25]. Arising from the fundamental principles of quantum mechanics, such as uncertainty and decoherence, quantum noise introduces fluctuations that affect the transmission and measurement of quantum information. In the context of QSS, such noise can degrade the quality of the distributed qubit shares, making it difficult for participants to retrieve a sufficient number of intact shares for successful secret reconstruction. If too many shares are corrupted, the protocol may fail to meet the threshold required, rendering the secret unrecoverable [20].

A key advantage of QSS is its inherent ability to detect eavesdropping: any attempt by an unauthorized party to intercept or measure the quantum shares typically introduces detectable disturbances [20, 26]. However, excessive quantum noise can obscure these disturbances, making it difficult to distinguish between natural errors and deliberate interference [20]. This compromises one of the core security features of QSS and highlights the need for robust noise mitigation strategies.

To mitigate the effects of quantum noise, a range of strategies has been developed [27–30], among which

* nirupambasak2020@iitkalmni.org

† goutam.paul@isical.ac.in

quantum error correction (QEC) techniques play a central role [29, 31–38]. QEC allows a quantum system to detect and correct errors introduced by noise, thereby preserving the integrity of the quantum information. In the context of QSS, these techniques are essential for ensuring that the distributed qubit shares remain usable. By integrating QEC, QSS protocols become significantly more resilient to noise, enabling authorized participants to reliably reconstruct the secret even in the presence of environmental disturbances.

The fundamental principle of QEC is to encode quantum information in a way that distributes it across multiple physical qubits. This redundancy enables the system to detect and correct errors affecting individual qubits without compromising the encoded information. For instance, a single logical qubit, representing a unit of quantum information, can be encoded into a group of physical qubits. If one of these qubits is altered by noise, the error can be identified through specific measurements on the others, allowing the original quantum state to be accurately restored.

One of the most notable quantum error correction codes is Shor’s code [31], which was the first to demonstrate that quantum information could be safeguarded from errors by using ancillary qubits. Shor’s code encodes a single logical qubit into nine physical qubits, allowing it to correct arbitrary errors affecting any one of these qubits.

Our Contributions. In this article, we explore multiparty Quantum Secret Sharing of classical messages (QSSCM) and secret sharing of quantum information (SSQI) protocols [11] proposed by Zhang et al., which utilize single-qubit states. These protocols are straightforward to implement, as they do not involve entanglement generation or multi-qubit quantum operations, except for the teleportation step in the SSQI protocol. In these protocols, each participant performs simple Pauli or Hadamard operations before forwarding the qubit to the next party. However, the transmission channel between parties may introduce noise, potentially corrupting the quantum state. To mitigate this, we employ Shor’s 9-qubit code for error protection. By exploiting the specific structure of the protocol, we demonstrate that certain parts of the code can be bypassed. In particular, we only require the bit-flip and phase-flip error correction codes, reducing the qubit overhead from 9 to 3. In general, such 3-qubit abridged version of Shor’s code does not correct amplitude damping noise. However, here it works due to the structure of the QSS protocol. This modified 3-qubit code can also be used for other single-qubit-based QSS [13, 39, 40], quantum key distribution (QKD) [41–44], quantum secure direct communication (QSDC) [45–48] and quantum authentication (QA) [49–53] protocols. Our results show that this modified code effectively minimizes errors in the reconstructed secret. Moreover, this modified code performs better than the existing QEC codes.

Paper Outline. In Section II, we briefly revisit the multi-

party QSSCM protocol provided by Zhang et al. Then, we discuss the quantum noise models and the QEC codes we considered in Section III. The effect of noise on the above QSSCM protocol has been discussed in Section IV. The reduction of error after using QEC is shown in Section V. In Section VI, we discuss the SSQI protocol under noise and effect of QEC. Finally, in Section VII, we conclude our work.

II. REVISITING MULTIPARTY QSSCM

The QSSCM protocol [11] designed by Zhang et al. is based on a previously developed protocol for quantum secure direct communication by Deng and Long [45]. In this scheme, a sender, Alice, splits her secret into encrypted shares and distributes them to different receivers. Each receiver applies certain quantum operations to ensure security before passing the message along. The receivers can only recover the full message by working together, ensuring that no individual can access it alone. Thus, it is an (n, n) -QSS protocol.

The multiparty QSSCM protocol [11] is provided as Algorithm 1. Note that the states produced by Bob in step 2, are the basis elements of the computational basis and the Hadamard basis. Also, all the operations the participants apply are either commutative or anti-commutative, producing a global phase ± 1 . Therefore, ignoring the global phase, the ordering of the operations may be changed in step 6 to get the Alice’s secret. Thus, after applying the operations, the state of the qubits would become $U_A|0\rangle$ up to global phase ± 1 , where U_A is the operation applied by Alice. Now, by measuring these qubits on a computational basis, Bob and Charlie can get the operation applied by Alice, revealing Alice’s secret. Mathematically, the protocol grows as follows.

$$\begin{aligned} & U_B^\dagger U_C^\dagger \cdots U_Z^\dagger U_A U_Z \cdots U_C U_B |0\rangle \\ &= \pm U_B^\dagger U_C^\dagger \cdots U_A U_Z^\dagger U_Z \cdots U_C U_B |0\rangle \\ &= \cdots = \pm U_B^\dagger U_A U_B |0\rangle \\ &= \pm U_A U_B^\dagger U_B |0\rangle = \pm U_A |0\rangle, \end{aligned} \quad (1)$$

where, U_A, U_B and U_C are the unitary operations by Alice, Bob and Charlie, respectively.

Although the protocol works perfectly in the ideal scenario, the noise in the communication channels corrupts the qubits and makes it hard for the receivers to reconstruct the shared secret. In Section IV and V, we discuss the effect of channel noises on the protocol and how to reduce the error in the reconstructed secret using QEC.

III. QUANTUM NOISE AND ERROR CORRECTION

Quantum noise makes any quantum protocol hard to implement [22]. It changes the state of a qubit and leads

ALGORITHM 1. Multiparty QSSCM Scheme

- 1: **Sender:** Alice, **Receiver:** Bob, Charlie, Dave, . . . , Zach.
- 2: Bob prepares a batch of single qubits $\{|\psi_i\rangle\}_i$ randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends the qubits to the next receiver, Charlie.

$$|\psi_i\rangle = U_B|0\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}.$$

- 3: After receiving these qubits, for each qubit, Charlie randomly chooses a unitary operator U_C from $\{I, \sigma_y, H\}$ and applies this operator to the qubit. Here, I is the identity operator $|0\rangle\langle 0| + |1\rangle\langle 1|$, σ_y is Pauli Y operator $|0\rangle\langle 1| - |1\rangle\langle 0|$ and H is the Hadamard operator $\frac{1}{\sqrt{2}}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|]$. After this encryption, she sends the batch to Dave.

$$|\psi_i\rangle \rightarrow U_C|\psi_i\rangle, U_C \in \{I, \sigma_y, H\}.$$

- 4: Dave randomly encrypts the encoded photons using the same method as Charlie, then forwards them to the next receiver. Each participant repeats this process until Zach completes his encryption. Once finished, Zach sends the fully encrypted photons to Alice.

$$U_C|\psi_i\rangle \rightarrow U_Z \cdots U_D U_C|\psi_i\rangle, U_Z, \cdots, U_D \in \{I, \sigma_y, H\}.$$

- 5: Alice performs some security check. Upon success, she discards the qubits used in security checking, and encodes her secret by applying unitary U_A , which is either I (for 0) or σ_y (for 1), on the remaining qubits. Finally, she forwards these qubits to Charlie.

$$U_D \cdots U_C|\psi_i\rangle \rightarrow U_A U_D \cdots U_C|\psi_i\rangle, U_A \in \{I, \sigma_y\}.$$

- 6: If Bob and Charlie collaborate, they can reconstruct the secret. First, they apply the inverse of their respective operations in step 2, 3 and 4. Then they measure the state in computational basis $\{|0\rangle, |1\rangle\}$ to get the secret.

$$U_A U_D \cdots U_C|\psi_i\rangle \rightarrow U_B^\dagger U_C^\dagger \cdots U_Z^\dagger U_A U_Z \cdots U_C U_B|0\rangle = U_A|0\rangle.$$

to an erroneous result at the end. Several QEC codes [31, 36, 54–64] to protect quantum information from noise.

A. Noise Models

There are several noise models [20, 22, 65, 66] available for quantum channels. However, as Pauli X ($\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$) and Pauli Z ($\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$), along with I and $i\sigma_y = i\sigma_z\sigma_x$, form a basis for single qubit states, most of the single qubit noises, including depolarizing noise, can be easily transformed into a combination of bit-flip and phase-flip noise [22]. So, in this work, we are going to consider three common noises: bit-flip, phase-flip and amplitude damping.

a. Bit-flip Noise A bit-flip noise flips a state in the computational basis, i.e., it interchanges $|0\rangle$ and $|1\rangle$ up to some probability, called *bit-flip error probability*. The Kraus operators [67] of a bit-flip channel \mathcal{C}_b with bit-flip error probability p_b^c is given by $\{\sqrt{1-p_b^c}I, \sqrt{p_b^c}\sigma_x\}$. The action of the channel on some density matrix ρ is as follows

$$\mathcal{C}_b(\rho) = (1-p_b^c)\rho + p_b^c\sigma_x\rho\sigma_x. \quad (2)$$

b. Phase-flip Noise A phase-flip noise flips the relative phase of a state in computational basis up to some probability, called *phase-flip error probability*. This error interchanges the states $|+\rangle$ and $|-\rangle$. The Kraus operators of a phase-flip channel \mathcal{C}_p with phase-flip error probability p_p^c is given by $\{\sqrt{1-p_p^c}I, \sqrt{p_p^c}\sigma_z\}$ and the corresponding channel action on some density matrix ρ

is as follows

$$\mathcal{C}_b(\rho) = (1-p_b^c)\rho + p_b^c\sigma_z\rho\sigma_z. \quad (3)$$

c. Amplitude Damping Noise Amplitude damping noise represents energy loss in a quantum system. It models the process where a qubit interacts with its environment and loses energy. This type of noise is particularly relevant in systems like superconducting qubits and optical quantum communication, where energy dissipation is a major concern [68, 69]. Mathematically, the action of an amplitude damping channel \mathcal{C}_a with damping strength $\gamma \in [0, 1]$ on some density matrix ρ can be written as

$$\mathcal{C}_a(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger, \quad (4)$$

where the Kraus operators are given by

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}. \quad (5)$$

Amplitude damping noise is crucial in quantum error correction and fault-tolerant quantum computing as it represents a primary source of decoherence in real-world quantum devices [68].

B. Error-correcting Codes

For perfect protection of a qubit from an arbitrary noise, we require at least five qubits, due to quantum singleton bound [70]. Although, some four- and three-qubit codes have been proposed [56, 57] to protect a qubit from

amplitude damping noise, they are classified as approximate code, where error correction happens up to some threshold. Here we use the Shor's code [8], five-qubit perfect code [54] and four-qubit approximate code [56]. By exploiting the structure of the QSSCM protocol, we show that we can use the bit-flip and phase-flip codes separately to get 3-qubit repetition code for perfect protection of single qubit error. We also show that this 3-qubit repetition code outperforms the 4-qubit approximate code and the smallest perfect code of 5 qubits.

a. Shor's Code Shor's code [31], introduced by Peter Shor in 1995, was one of the first quantum error correction codes. It protects a single logical qubit from arbitrary errors (bit-flip, phase-flip, and combinations of both) by encoding it into nine physical qubits. The code is composed of two parts as follows.

Bit-flip error correction: The first step of Shor's code involves encoding the logical qubit into three physical qubits. These qubits are encoded using a repetition code, where each qubit is copied three times to correct

for bit-flip errors.

Phase-flip error correction: After the bit-flip error correction, the next step involves encoding each of the three qubits into another set of three physical qubits, using a three-qubit phase-flip code, which consists of a layer of Hadamard operation for change of basis, then copying the states three times, and finally another layer of Hadamard operation to go back to the original basis (or, in other words, copying each qubit three times in Hadamard basis). This helps to protect the information from phase-flip errors.

Together, these two layers of encoding (bit-flip and phase-flip corrections) allow Shor's code to protect a logical qubit from errors in both the bit and phase, as well as combinations of both, making it more robust against noise.

b. Five-qubit Perfect Code Five-qubit code [54] is the smallest QEC code for perfect error correction. As the name suggests, the five-qubit code [36] encodes a single logical qubit using five physical qubits. The encoded logical qubits are as follows.

$$\begin{aligned} |0_L\rangle &= \frac{1}{2\sqrt{2}}(-|00000\rangle + |00110\rangle + |01001\rangle + |01111\rangle - |10011\rangle + |10101\rangle + |11010\rangle + |11100\rangle), \\ |1_L\rangle &= \frac{1}{2\sqrt{2}}(-|11111\rangle + |11001\rangle + |10110\rangle + |10000\rangle + |01100\rangle - |01010\rangle - |00101\rangle - |00011\rangle). \end{aligned} \quad (6)$$

For QSSCM protocol, Bob performs this encoding operation on his qubits and sends the encoded states to Charlie. Charlie applies random logical operators from $\{I_L, \sigma_{yL}, H_L\}$ corresponding to the physical operators $\{I, \sigma_y, H\}$. Then Charlie sends the sequence to the next party. Finally, after performing security checks, Alice applies logical identity I_L for secret bit 0 and logical Pauli- Y

σ_{yL} for secret bit 1 and sends the sequence to Charlie. Upon receiving the sequence, all the receivers apply the logical operations they applied before Alice's encoding.

At the end, the receivers perform the decoding, which is simply the inverse of the initial encoding (6), followed by the state recovery operation, whose Kraus operators $\{\mathcal{R}_k\}_k$ [71] are given by

$$\begin{aligned} R_0 &= |00\rangle\langle 00| \otimes \sigma_0 \otimes |00\rangle\langle 00|, & R_1 &= |00\rangle\langle 00| \otimes \sigma_z \otimes |00\rangle\langle 01|, \\ R_2 &= |00\rangle\langle 00| \otimes \sigma_0 \otimes |00\rangle\langle 10|, & R_3 &= |00\rangle\langle 00| \otimes \sigma_0 \otimes |00\rangle\langle 11|, \\ R_4 &= |00\rangle\langle 01| \otimes \sigma_0 \otimes |00\rangle\langle 00|, & R_5 &= |00\rangle\langle 01| \otimes \sigma_z \otimes |00\rangle\langle 01|, \\ R_6 &= |00\rangle\langle 01| \otimes \sigma_x \otimes |00\rangle\langle 10|, & R_7 &= |00\rangle\langle 01| \otimes \sigma_x \otimes |00\rangle\langle 11|, \\ R_8 &= |00\rangle\langle 10| \otimes \sigma_0 \otimes |00\rangle\langle 00|, & R_9 &= |00\rangle\langle 10| \otimes \sigma_x \otimes |00\rangle\langle 01|, \\ R_{10} &= |00\rangle\langle 10| \otimes \sigma_z \otimes |00\rangle\langle 10|, & R_{11} &= |00\rangle\langle 10| \otimes \sigma_x \otimes |00\rangle\langle 11|, \\ R_{12} &= |00\rangle\langle 11| \otimes \sigma_z \otimes |00\rangle\langle 00|, & R_{13} &= |00\rangle\langle 11| \otimes \sigma_x \sigma_z \otimes |00\rangle\langle 01|, \\ R_{14} &= |00\rangle\langle 11| \otimes \sigma_x \otimes |00\rangle\langle 10|, & R_{15} &= |00\rangle\langle 11| \otimes \sigma_z \otimes |00\rangle\langle 11|, \end{aligned}$$

where σ_0 is the identity operator and σ_x, σ_z are the Pauli- X and Pauli- Z operators, respectively. After discarding the ancillary qubits and measuring the main qubit in the

computational basis, they get the secret shared by Alice.

c. Four-qubit Approximate Code The four-qubit approximate quantum error-correcting code [56] introduced

by Leung et al. is designed to protect against amplitude damping errors, which commonly occur in realistic quantum systems due to energy loss. It encodes a single logical qubit into four physical qubits as

$$\begin{aligned} |0_L\rangle &= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle), \\ |1_L\rangle &= \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle). \end{aligned} \quad (7)$$

Unlike conventional perfect QEC codes, this code does not correct all possible single-qubit errors exactly, but instead offers *approximate correction* optimized for amplitude damping noise. The recovery process involves detecting which qubit experienced a damping event and applying a conditional unitary to restore the state, resulting in high-fidelity recovery despite the approximate nature. This demonstrates that relaxing the strict criteria of perfect quantum error correction can lead to more efficient codes for specific noise models.

IV. EFFECTS OF NOISE ON MULTIPARTY QSSCM PROTOCOL

Quantum states are fragile to noise. Therefore, studying noises and investigating their actual effect on a protocol is crucial for implementing the protocol.

A. Effect of noise on 3-party QSSCM Protocol

There are three different channels, namely, Bob to Charlie, Charlie to Alice and Alice to Charlie, in the

QSSCM protocol we are considering here. Any of these three channels may get affected by the noise. Here, we consider the bit-flip, phase-flip and amplitude damping noise.

a. Bit-flip and Phase-flip Noise If a state is prepared on a computational (Hadamard respectively) basis, from the discussion in Section III A, we can easily see that the phase-flip (bit-flip respectively) noise does not affect it. Therefore, over each channel, depending on the transmitted state, there is only one effective error, either bit-flip or phase-flip. Let us assume p_*^B, p_*^C and p_*^A are the error probabilities for the channels \mathcal{C}^B from Bob to Charlie, \mathcal{C}^C from Charlie to Alice and \mathcal{C}^A from Alice to Charlie, respectively. Here, * in the suffix denotes the bit-flip or phase-flip (whichever is applicable). Therefore, a state ρ becomes

$$\mathcal{C}(\rho) = (1 - p_*^C)\rho + p_*^C\rho' \quad (8)$$

under the channel \mathcal{C} , where ρ' is the state obtained by a bit-flip or phase-flip (whichever is applicable) error on the state ρ . Note that, for any operator U applied by Bob, Charlie or Alice on a prepared state ρ ,

$$U\rho' = (U\rho)' \quad (9)$$

holds, up to some global phase ± 1 . Thus, if Bob prepares a state as ρ , after going through all three channels, the final state (up to some global phase) would be

$$\begin{aligned} \mathcal{C}^A(\mathcal{C}^C(\mathcal{C}^B(\rho))) &= \mathcal{C}^A(\mathcal{C}^C((1 - p_*^B)\rho + p_*^B\rho')) = \mathcal{C}^A((1 - p_*^C)[(1 - p_*^B)\rho + p_*^B\rho'] + p_*^C[(1 - p_*^B)\rho' + p_*^B(\rho')']) \\ &= \mathcal{C}^A((1 - p_*^C)[(1 - p_*^B)\rho + p_*^B\rho'] + p_*^C[(1 - p_*^B)\rho' + p_*^B\rho]) \\ &= \mathcal{C}^A([(1 - p_*^C)(1 - p_*^B) + p_*^C p_*^B]\rho + [(1 - p_*^C)p_*^B + p_*^C(1 - p_*^B)]\rho') \\ &= [(1 - p_*^A)(1 - p_*^C)(1 - p_*^B) + (1 - p_*^A)p_*^C p_*^B + p_*^A(1 - p_*^C)p_*^B + p_*^A p_*^C(1 - p_*^B)]\rho \\ &\quad + [(1 - p_*^A)(1 - p_*^C)p_*^B + (1 - p_*^A)p_*^C(1 - p_*^B) + p_*^A(1 - p_*^C)(1 - p_*^B) + p_*^A p_*^C p_*^B]\rho'. \end{aligned} \quad (10)$$

Here, the operations by Bob, Charlie and Alice have been ignored due to (9), we can think that all the noise acts before the unitary operations. Note that (10) is symmetric for p_*^A, p_*^B and p_*^C . This implies that all three channels $\mathcal{C}^A, \mathcal{C}^B$ and \mathcal{C}^C act similarly under bit-flip and phase-flip noise.

For simplicity, let us assume $p_*^A = p_*^C = p_*^B = p$. Then, from (10), the probability of error for a single state will be

$$e_1 = 3p(1 - p)^2 + p^3 = 3p(1 - 2p) + \mathcal{O}(p^3). \quad (11)$$

b. Effect of Amplitude Damping Noise We can see that the amplitude damping channel \mathcal{C}_a does not commute or anticommute with the operations U_A, U_B and U_C . In this case, the final state would be

$$U_B^\dagger U_C^\dagger \mathcal{C}_a^A \left(U_A \mathcal{C}_a^C \left(U_C \mathcal{C}_a^B \left(U_B |0\rangle\langle 0| U_B^\dagger \right) U_C^\dagger \right) U_A^\dagger \right) U_C U_B. \quad (12)$$

There are 4 choices for U_B , 3 choices for U_C and 2 choices for U_A , producing $4*3*2 = 24$ different final states, each with probability $\frac{1}{24}$. Note that if the channels are considered as noise-free, these states would be either $|0\rangle\langle 0|$

or $\sigma_y|0\rangle\langle 0|\sigma_y = |1\rangle\langle 1|$.

The probability of average error under the amplitude damping channel is thus given by

$$\begin{aligned} e_1^a &= \frac{1}{12} \left(3 + 8\gamma - 7\gamma^2 + 2\gamma^3 - 2(1-\gamma)^{3/2} - (1-\gamma)^{5/2} \right) \\ &= \frac{27}{24}\gamma - \frac{77}{96}\gamma^2 + \mathcal{O}(\gamma^3). \end{aligned} \quad (13)$$

The probabilities of errors for all 24 cases are explicitly mentioned in Table I.

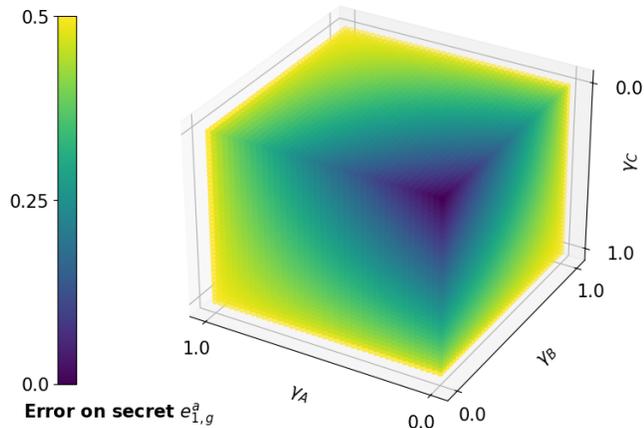


FIG. 1. Error on secret $e_{1,g}^a$ as function (14) of damping strengths γ_A, γ_B and γ_C for channels from Alice to Charlie, from Bob to Charlie and from Charlie to Alice, respectively. Observe that γ_A and γ_C affect similarly, while γ_B effects differently.

For a more general case, when the damping strengths of the channels $\mathcal{C}^A, \mathcal{C}^B$ and \mathcal{C}^C are given by γ_A, γ_B and γ_C , respectively, the probabilities of errors are given by

$$\begin{aligned} e_{1,g}^a &= \left(4 + 2(\gamma_A + \gamma_B + \gamma_C) - 2(\gamma_A\gamma_B + \gamma_B\gamma_C + \gamma_C\gamma_A) \right. \\ &\quad + 2\gamma_A\gamma_B\gamma_C - (1-\gamma_A)(1-\gamma_C)\sqrt{1-\gamma_B} \\ &\quad - (1-\gamma_B)\sqrt{(1-\gamma_A)(1-\gamma_C)} \\ &\quad \left. - 2\sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)} \right) / 12. \end{aligned} \quad (14)$$

The probabilities of errors for different cases can be found in Table II. From (14), we can see that the effects of γ_A and γ_C are the same. However, γ_B creates more error than γ_A and γ_C . The effect of γ_A, γ_B and γ_C can be seen in Fig. 1.

B. Effect of noise on n -party QSSCM Protocol

There are n different channels in n -party QSSCM protocol. As we have already seen, all of these n channels act similarly under bit-flip and phase-flip noise; for simplicity, let us consider that they all have the same error

probability p . Then generalizing (10) and (11), we get the error for a single qubit as

$$\begin{aligned} e_1^g &= \sum_{i \text{ is odd } \leq n} \binom{n}{i} p^i (1-p)^{n-i} \\ &= \frac{1}{2} \left((1-p+p)^n - (1-p-p)^n \right) \\ &= \frac{1}{2} (1 - (1-2p)^n). \end{aligned} \quad (15)$$

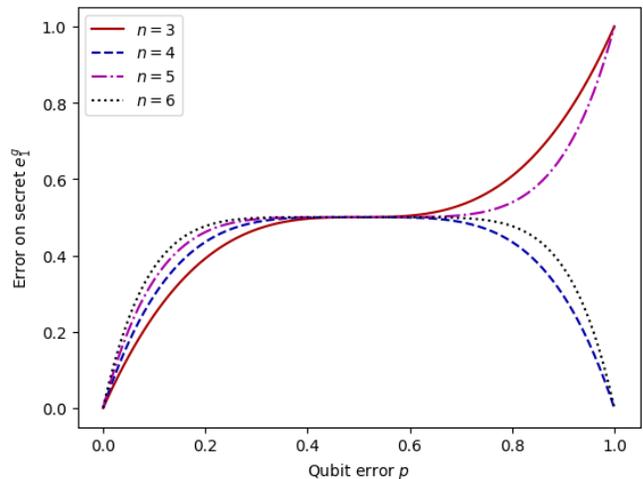


FIG. 2. The plots of the error e_1^g as a function (15) of the qubit error probability p are shown for $n = 3, 4, 5$, and 6 . For protocols involving an even number of channels, a higher error probability increases the likelihood of an even number of flips, which can paradoxically lead to a reduction in the overall error. However, this does not happen for odd number of channels, leading the error on secret to 1, as qubit error probability reaches to 1.

Fig. 2 shows the plots of the error e_1^g against error probability p for $n = 3, 4, 5$ and 6 . Note that even number of flips result in *no error*. Therefore, if the error probability is high, the probability of even number of flips is also high for even numbers of channels, reducing the overall error.

V. IMPROVEMENT OF RESULT USING QEC

Quantum error correction (QEC) is a crucial technique in quantum computing designed to protect quantum information from noise and errors that arise due to imperfections in quantum systems. Unlike classical error correction, where bits are used to represent information, quantum error correction must account for both bit-flip and phase-flip errors, as well as more complex quantum errors that affect quantum states, such as coherence.

TABLE I. Errors in the final output generated by Bob and Charlie, under amplitude damping noise with damping strength γ , for different operations applied by Alice, Bob and Charlie. Each of these cases may appear with probability $1/24$.

Bob's State	Charlie's Operation	Alice's Secret	Error Probability
$ 0\rangle\langle 0 $	I	0	0
		1	γ
	σ_y	0	$2\gamma - \gamma^2$
		1	$\gamma - \gamma^2$
	H	0	$\gamma/2$
		1	$\gamma/2$
$ 1\rangle\langle 1 $	I	0	$3\gamma - 3\gamma^2 + \gamma^3$
		1	$2\gamma - 3\gamma^2 + \gamma^3$
	σ_y	0	$\gamma - 2\gamma^2 + \gamma^3$
		1	$2\gamma - 2\gamma^2 + \gamma^3$
	H	0	$(3\gamma - 2\gamma^2)/2$
		1	$(3\gamma - 2\gamma^2)/2$
$ +\rangle\langle + $	I	0	$(1 - (1 - \gamma)^{3/2})/2$
		1	$(1 - (1 - \gamma)^{3/2})/2$
	σ_y	0	$(1 - (1 - \gamma)^{3/2})/2$
		1	$(1 - (1 - \gamma)^{3/2})/2$
	H	0	$(1 - 2\gamma + \gamma^2 - (1 - \gamma)^{5/2})/2$
		1	$(1 + \gamma^2 - (1 - \gamma)^{5/2})/2$
$ -\rangle\langle - $	I	0	$(1 - (1 - \gamma)^{3/2})/2$
		1	$(1 - (1 - \gamma)^{3/2})/2$
	σ_y	0	$(1 - (1 - \gamma)^{3/2})/2$
		1	$(1 - (1 - \gamma)^{3/2})/2$
	H	0	$(1 + 2\gamma - \gamma^2 - (1 - \gamma)^{5/2})/2$
		1	$(1 - \gamma^2 - (1 - \gamma)^{5/2})/2$
Average Error			$(3 + 8\gamma - 7\gamma^2 + 2\gamma^3 - 2(1 - \gamma)^{3/2} - (1 - \gamma)^{5/2})/12$

A. Shor's Code as Repetition Code

Shor's code is not only very easy to implement but it is also efficient for the QSSCM code we are considering here. As we already discussed in Section IV A, we do not require to combine the bit-flip and phase-flip correction together, rather we apply bit-flip correction for the states $|0\rangle$ and $|1\rangle$ and phase-flip correction for the states $|+\rangle$ and $|-\rangle$. Therefore, we only require to repeat each state three times, reducing the resource requirement for Shor's code from 9 to 3. This also makes the code resource efficient compared to other QEC codes, where we cannot separate bit-flip and phase-flip correction, requiring at least 5 physical qubits due to the quantum singleton bound [70]. As our modified Shor's code is only repeating the states, we would call it *repetition code*. Under this QEC scenario, Alice, Bob and Charlie randomly choose one operation as described in the QSSCM protocol and

apply this operation on three consecutive qubits. During decoding, the secret is decided based on majority voting among three consecutive states. Thus the components of the repetition code is as follow.

Encoding: Prepare three copies of each state during state preparation.

State Recovery: Measure each state in proper basis, as prepared. Apply majority voting to decide the measurement outcome.

Logical Operation: Apply each operation on three consecutive states.

This repetition code can also be used for other single-qubit-based quantum protocols [13, 39–53], where the outcome of the protocol is a sequence of classical bits, to improve the result.

TABLE II. Errors in the final output generated by Bob and Charlie, under amplitude damping noise with damping strengths γ_A, γ_B and γ_C corresponding to the channels from Alice to Charlie, from Bob to Charlie and from Charlie to Alice, respectively, for different operations applied by Alice, Bob and Charlie. Each of these cases may appear with probability $1/24$.

Bob's State	Charlie's Operation	Alice's Secret	Error Probability
$ 0\rangle\langle 0 $	I	0	0
		1	γ_A
	σ_y	0	$\gamma_A + \gamma_C - \gamma_A\gamma_C$
		1	$\gamma_C - \gamma_A\gamma_C$
	H	0	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_C)}\right) / 2$
		1	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_C)}\right) / 2$
$ 1\rangle\langle 1 $	I	0	$\gamma_A + \gamma_B + \gamma_C - \gamma_A\gamma_B - \gamma_B\gamma_C - \gamma_C\gamma_A + \gamma_A\gamma_B\gamma_C$
		1	$\gamma_B + \gamma_C - \gamma_A\gamma_B - \gamma_B\gamma_C - \gamma_C\gamma_A + \gamma_A\gamma_B\gamma_C$
	σ_y	0	$\gamma_B - \gamma_A\gamma_B - \gamma_B\gamma_C + \gamma_A\gamma_B\gamma_C$
		1	$\gamma_A + \gamma_B - \gamma_A\gamma_B - \gamma_B\gamma_C + \gamma_A\gamma_B\gamma_C$
	H	0	$\left(1 + (2\gamma_B - 1)\sqrt{(1-\gamma_A)(1-\gamma_C)}\right) / 2$
		1	$\left(1 + (2\gamma_B - 1)\sqrt{(1-\gamma_A)(1-\gamma_C)}\right) / 2$
$ +\rangle\langle + $	I	0	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
		1	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
	σ_y	0	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
		1	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
	H	0	$\left(1 - \gamma_A - \gamma_C + \gamma_A\gamma_C - (1-\gamma_A)(1-\gamma_C)\sqrt{1-\gamma_B}\right) / 2$
		1	$\left(1 + \gamma_A - \gamma_C + \gamma_A\gamma_C - (1-\gamma_A)(1-\gamma_C)\sqrt{1-\gamma_B}\right) / 2$
$ -\rangle\langle - $	I	0	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
		1	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
	σ_y	0	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
		1	$\left(1 - \sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 2$
	H	0	$\left(1 + \gamma_A + \gamma_C - \gamma_A\gamma_C - (1-\gamma_A)(1-\gamma_C)\sqrt{1-\gamma_B}\right) / 2$
		1	$\left(1 - \gamma_A + \gamma_C - \gamma_A\gamma_C - (1-\gamma_A)(1-\gamma_C)\sqrt{1-\gamma_B}\right) / 2$
Average Error			$\left(4 + 2(\gamma_A + \gamma_B + \gamma_C) - 2(\gamma_A\gamma_B + \gamma_B\gamma_C + \gamma_C\gamma_A) + 2\gamma_A\gamma_B\gamma_C - (1-\gamma_A)(1-\gamma_C)\sqrt{1-\gamma_B} - (1-\gamma_B)\sqrt{(1-\gamma_A)(1-\gamma_C)} - 2\sqrt{(1-\gamma_A)(1-\gamma_B)(1-\gamma_C)}\right) / 12$

B. Repetition Code on QSSCM Protocol

If at most one from the measurements of three consecutive states gives erroneous output, the majority voting decoder would provide the correct secret. However, if more than one output is erroneous, this decoder would provide the wrong secret bit. If e is the error for a single qubit, the error after QEC would be given by

$$e_{QEC} = 3e^2(1-e) + e^3. \quad (16)$$

The error correction would be effective, if $e > 0$ and $e_{QEC} < e$, that is,

$$\begin{aligned} 3e^2(1-e) + e^3 < e &\implies 3e(1-e) + e^2 < 1 \\ &\implies 2e^2 - 3e + 1 > 0 \\ &\implies \left(e - \frac{1}{2}\right)(e-1) > 0 \\ &\implies e < \frac{1}{2}, \text{ as } e \leq 1. \end{aligned} \quad (17)$$

This is the condition for effective error correction using the repetition code.

a. Bit-flip and Phase-flip Noise As we have discussed above, if more than one state from three consecutive states gets flipped, the state cannot be restored

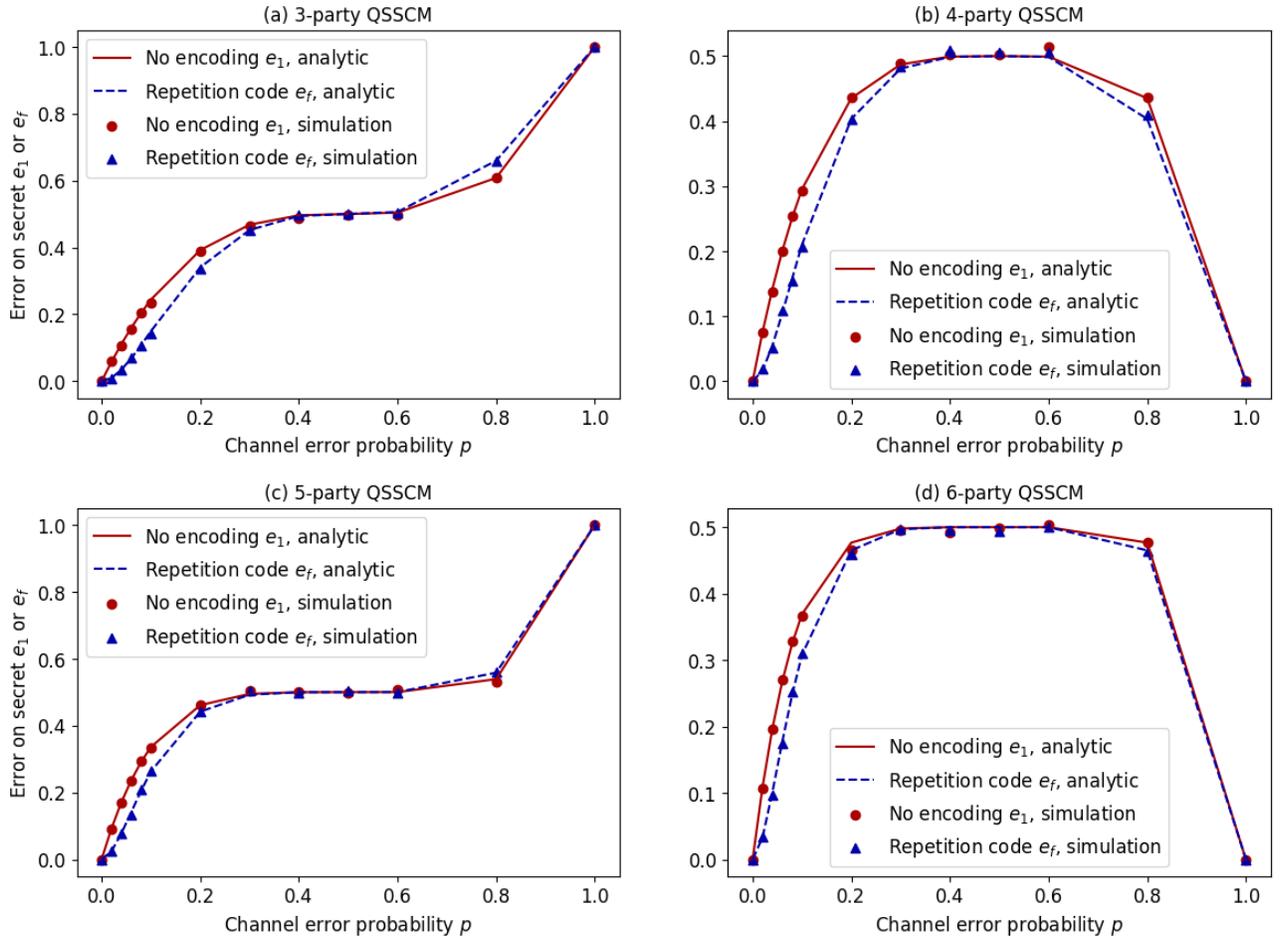


FIG. 3. Error on reconstructed secret is plotted against channel error probability p with and without repetition code. The plot is generated from analytic equations (15) and (20) and the simulated results. It shows that if $p < 0.5$, the repetition code can reduce the error in the reconstructed secret.

perfectly, leading to an error. Now, for 3-party QSSCM, using (11), we can write the probability that at least two out of three consecutive states get flipped as

$$e_f = 3e_1^2(1 - e_1) + e_1^3 = 27p^2 + \mathcal{O}(p^3), \quad (18)$$

which is the final error probability using the repetition code.

From (17), the condition for an effective error correction under bit-flip and phase-flip noise is given by

$$\begin{aligned} e_1 < \frac{1}{2} &\implies 3p(1-p)^2 + p^3 < \frac{1}{2} \\ &\implies \frac{1}{2} (1 - (1-2p)^3) < \frac{1}{2} \\ &\implies p < \frac{1}{2}. \end{aligned} \quad (19)$$

Therefore, if all three channels have an error probability less than $\frac{1}{2}$, the repetition code can effectively reduce the error, which is shown in Fig. 3(a). The result after simulating QSSCM under bit-flip and phase-flip noise is also shown in the same figure. The simulation plot also

shows that if $p < 0.5$, the repetition code can reduce the error.

For n -party QSSCM protocol, using (15), we can write the error on secret as

$$\begin{aligned} e_f^g &= 3(e_1^g)^2(1 - e_1^g) + (e_1^g)^3 \\ &= \frac{1}{4} (1 - (1-2p)^n)^2 (2 + (1-2p)^n). \end{aligned} \quad (20)$$

Also, the condition for effective error correction becomes

$$\begin{aligned} e_1^g < \frac{1}{2} &\implies \frac{1}{2} (1 - (1-2p)^n) < \frac{1}{2} \\ &\implies (1-2p)^n > 0 \\ &\implies \begin{cases} p \in (0, 1) \setminus \frac{1}{2}, & \text{if } n \text{ is even,} \\ p \in (0, \frac{1}{2}) & \text{if } n \text{ is odd.} \end{cases} \end{aligned} \quad (21)$$

This result along with the simulations for $n = 3, 4, 5$ and 6 has been shown in Fig. 3.

b. Amplitude Damping Noise For amplitude damping noise, if only one from three consecutive outputs is

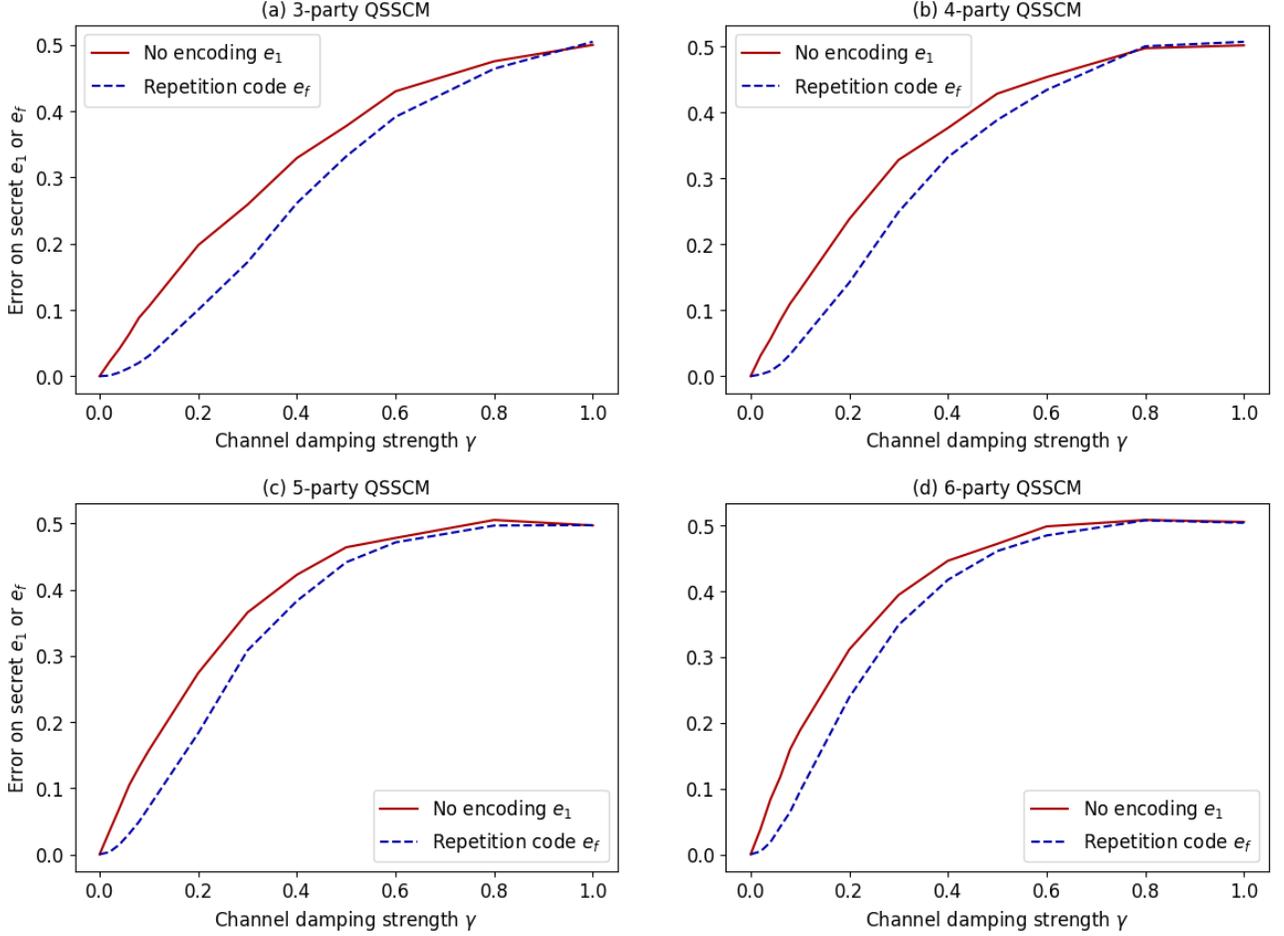


FIG. 4. Error on reconstructed secret is plotted against damping probability γ with and without repetition code. The plot is generated from analytic equations (13) and (22) and the simulated results. It shows that the repetition code can reduce the error in the reconstructed secret for all values of the damping strength.

erroneous, the majority voting decoder would provide the correct secret bit. However, if two or three outputs are erroneous, then the majority voting would fail. Using (13), the probability of at least two out of three consecutive outputs being erroneous can be written as

$$e_f^a = 3(e_1^a)^2(1 - e_1^a) + (e_1^a)^3 = \frac{3}{32}\gamma^2 + \mathcal{O}(\gamma^3). \quad (22)$$

From (13) one can see that, e_1^a satisfies the condition for effective error correction (17) for $\gamma \in (0, 1)$, that is,

$$e_1^a < \frac{1}{2} \text{ for } \gamma \in (0, 1). \quad (23)$$

Also, $e_{1,g}^a$ in (14) satisfies the effective error correcting condition for all $\gamma_A, \gamma_B, \gamma_C \in (0, 1)$. We have simulated the 3-party QSSCM protocol with amplitude damping noise. We see that the repetition code reduces the error in the reconstructed secret for all values of damping strength except 0 and 1, where it is the same as the error for the no-encoding scenario.

We have also simulated the n -party QSSCM protocol for $n = 3, 4, 5$ and 6 under the amplitude damping noise. The plots are shown in Fig. 4.

C. Five and Four-qubit QECs on QSSCM Protocol

In the previous section, we have applied encoding at the beginning of the protocol, and the decoding including recovery operation at the end of the complete protocol. As there is a single cycle of encoding, decoding and state recovery operations, we call this as *single-cycle QEC*. However, we can apply this QEC in multiple cycles, which performs better than a single-cycle QEC [71–76]. One straightforward towards multiple cycles is to apply a single cycle to each channel individually, first from Bob to Charlie, then from Charlie to Dave, and so on. In this scenario, each party can apply their physical operations directly on the main qubits after the recovery operations. Note that we cannot apply multiple cycles for the repetition code we discussed in Section V A as that requires

the knowledge about the basis on which Bob prepares the state. However, the five-qubit perfect code [54] and the four-qubit approximate code [56] being basis independent, this problem does not arise, and we can perform the multiple cycles. Fig. 5 and 6 show the performances of the five-qubit perfect code and the four-qubit approximate code in multi-cycle scenario for 3-party QSSCM under Pauli (bit-flip and phase-flip) noise and amplitude damping noise, respectively. Even the four-qubit and the five-qubit code performs worse than the no-encoding scenario. This is because, in the five-qubit code, all five qubits are subjected to errors, resulting in a higher overall error rate compared to the single-qubit error in the no-encoding case. In contrast, while the repetition code also exposes three qubits to errors, QEC keeps the total error rate below the threshold of the no-encoding scenario.

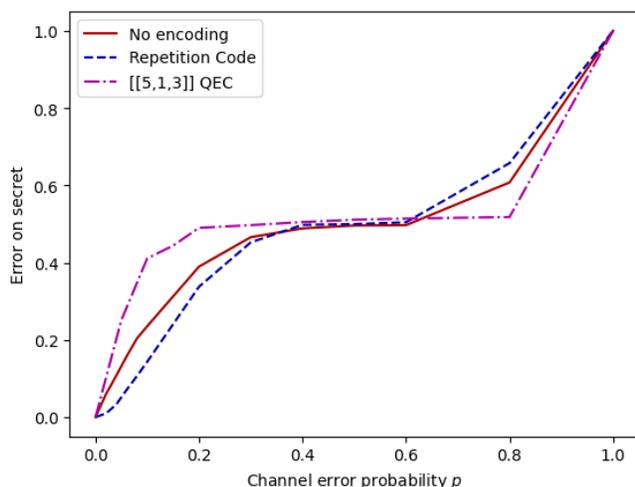


FIG. 5. Plots show the simulated errors on reconstructed secret against Pauli (bit-flip or phase-flip) error p . Observe that repetition code performs better than existing $[[5, 1, 3]]$ perfect QEC [54]. Even the five-qubit codes perform worse than the no encoding scenario. The reason is for five-qubit code, all the five qubits are going through the error, making the error very high compared to one-qubit error in no encoding scenario, and the QEC fails to recover it. Although for the repetition code, three qubits are going through the error, the QEC restricts it below the no encoding threshold.

VI. SSQI PROTOCOL UNDER NOISE

Zhang et al. also proposed a SSQI protocol in the same article [11] combining the above QSSCM protocol with the standard teleportation protocol [77]. To perform the secret sharing of a quantum state among $n - 1$ receivers, Alice sends the state to Bob using the standard teleportation protocol. However, instead of announcing the Bell-measurement outcomes, she shares these among the other $n - 2$ receivers except Bob using the QSSCM proto-

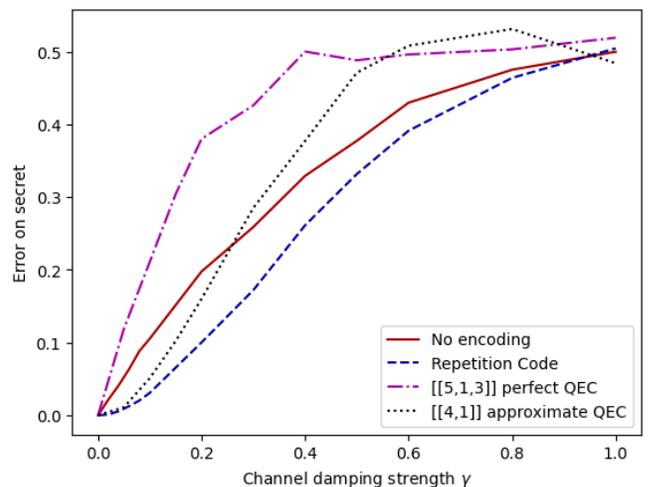


FIG. 6. Plots show the simulated error of the secret as a function of the amplitude damping strength, γ . Notably, the repetition code outperforms both the $[[5, 1, 3]]$ perfect QEC code [54] and the $[[4, 1]]$ approximate QEC code [56]. Both the four-qubit and five-qubit codes perform worse than the no-encoding scenario. This is because, during quantum error correction, all qubits in these codes are exposed to noise, resulting in a higher cumulative error than the single-qubit error encountered without encoding. In contrast, although the repetition code also subjects three qubits to noise, the QEC process effectively suppresses the total error below that of the no-encoding case.

col. Therefore, this SSQI protocol requires QEC for the QSSCM part as well as for the standard teleportation. Several fault-tolerant teleportation schemes [78–83] have been proposed to deal with the noise during quantum teleportation. However, if e_t is the error in the teleportation process, and e_{noise} and e_{QEC} are the errors for the QSSCM protocol, without and with QEC, respectively, for effective error correction we require

$$\begin{aligned}
 & \text{fidelity with correction} > \text{fidelity without correction} \\
 \implies & (1 - e_{QEC})(1 - e_t) > (1 - e_{noise})(1 - e_t) \\
 \implies & e_{QEC} < e_{noise},
 \end{aligned} \tag{24}$$

which is the effective error correcting condition for the QSSCM protocol. Therefore, all the results we have discussed in Section V are also valid for the SSQI protocol.

VII. CONCLUSION AND FUTURE WORKS

In this article, we investigate the effects of quantum noise on the multiparty QSSCM and SSQI protocols proposed by Zhang et al. [11]. The QSSCM protocol utilizes single-qubit transmissions without the need for entanglement, offering a relatively simple and practical implementation. The SSQI protocol builds upon QSSCM to enable the sharing of quantum information. Despite their

simplicity, these protocols are highly vulnerable to quantum noise, which can corrupt the transmitted qubits and significantly hinder the accurate reconstruction of the secret.

To address the vulnerability of the QSSCM protocol to quantum noise, we analyze the impact of various noise models—including bit-flip, phase-flip, and amplitude damping—on its performance. Our analysis demonstrates how these noise sources introduce errors that degrade the fidelity of the reconstructed secret. To mitigate these effects, we apply an optimized version of Shor’s 9-qubit quantum error correction (QEC) code. By separating the bit-flip and phase-flip correction processes, we reduce the required resources from 9 qubits to just 3. This simplified, repetition-based QEC approach significantly lowers the error probability compared to conventional QEC schemes, thereby enhancing the robustness of the QSSCM protocol against quantum noise. In general,

such a 3-qubit abridged version of Shor’s code is not capable of correcting amplitude damping noise. However, in this context, it proves effective due to the specific structure of the QSS protocol. Our findings and methodology are equally applicable to the SSQI protocol, and we argue that the proposed QEC technique can be extended to other single-qubit-based quantum protocols.

Future research could investigate more efficient quantum error correction techniques—such as surface codes or optimized encoding strategies—to further improve the security and practicality of multiparty quantum secret sharing in realistic, noisy environments. Additionally, the application of repetition-based error correction could be extended to other single-qubit-based quantum protocols, including QSS, QKD, QSDC, and QA schemes, to evaluate its effectiveness in enhancing their resilience to noise.

-
- [1] Adi Shamir, “How to share a secret,” *Commun. ACM* **22**, 612–613 (1979).
- [2] G. R. BLAKLEY, “Safeguarding cryptographic keys,” in *1979 International Workshop on Managing Requirements Knowledge (MARK)* (1979) pp. 313–318.
- [3] Arup Kumar Chattopadhyay, Sanchita Saha, Amitava Nag, and Sukumar Nandi, “Secret sharing: A comprehensive survey, taxonomy and applications,” *Computer Science Review* **51**, 100608 (2024).
- [4] Dimitrios Panagopoulos, “A secret sharing scheme using groups,” *arXiv preprint arXiv:1009.0026* (2010), <https://doi.org/10.48550/arXiv.1009.0026>.
- [5] Maggie Habeeb, Delaram Kahrobaei, and Vladimir Shpilrain, “A secret sharing scheme based on group presentations and the word problem,” in *Computational and Combinatorial Group Theory and Cryptography* (American Mathematical Society, 2012).
- [6] Samaneh Mashhadi, “How to fairly share multiple secrets stage by stage,” *Wireless Personal Communications* **90**, 93–107 (2016).
- [7] J. He and E. Dawson, “Multistage secret sharing based on one-way function,” *Electronics Letters* **30**, 1591–1592 (1994).
- [8] P.W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.
- [9] Lov K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC ’96 (Association for Computing Machinery, New York, NY, USA, 1996) p. 212–219.
- [10] Mark Hillery, Vladimír Bužek, and André Berthiaume, “Quantum secret sharing,” *Phys. Rev. A* **59**, 1829–1834 (1999).
- [11] Zhan-jun Zhang, Yong Li, and Zhong-xiao Man, “Multiparty quantum secret sharing,” *Phys. Rev. A* **71**, 044301 (2005).
- [12] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, “Efficient multiparty quantum-secret-sharing schemes,” *Phys. Rev. A* **69**, 052307 (2004).
- [13] Guo-Ping Guo and Guang-Can Guo, “Quantum secret sharing without entanglement,” *Physics Letters A* **310**, 247–251 (2003).
- [14] Daniel Gottesman, “Theory of quantum secret sharing,” *Phys. Rev. A* **61**, 042311 (2000).
- [15] Yaoyao Zhou, Juan Yu, Zhihui Yan, Xiaojun Jia, Jing Zhang, Changde Xie, and Kunchi Peng, “Quantum secret sharing among four players using multipartite bound entanglement of an optical field,” *Phys. Rev. Lett.* **121**, 150502 (2018).
- [16] Qin Liao, Haijie Liu, Lingjin Zhu, and Ying Guo, “Quantum secret sharing using discretely modulated coherent states,” *Phys. Rev. A* **103**, 032410 (2021).
- [17] W. Tittel, H. Zbinden, and N. Gisin, “Experimental demonstration of quantum secret sharing,” *Phys. Rev. A* **63**, 042301 (2001).
- [18] Werner Heisenberg, “Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik,” *Zeitschrift für Physik* **43**, 172–198 (1927).
- [19] William K Wootters and Wojciech H Zurek, “A single quantum cannot be cloned,” *Nature* **299**, 802–803 (1982).
- [20] Nirupam Basak, Nayana Das, Goutam Paul, Kaushik Nandi, and Nixon Patel, “Quantum secret sharing protocol using ghz state: implementation on ibm qiskit,” *Quantum Information Processing* **22**, 393 (2023).
- [21] John Preskill, “Quantum Computing in the NISQ era and beyond,” *Quantum* **2**, 79 (2018).
- [22] Michael A Nielsen and Isaac L Chuang, *Quantum computation and quantum information: 10th Anniversary Edition* (Cambridge University Press, 2010).
- [23] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven, “Characterizing quantum supremacy in near-term devices,” *Nature Physics* **14**, 595–600 (2018).
- [24] Daniel Gottesman, “An introduction to quantum error correction and fault-tolerant quantum computation,” *arXiv preprint arXiv:0904.2557* (2009), <https://doi.org/10.48550/arXiv.0904.2557>.

- [25] Rami Barends, Julian Kelly, Anthony Megrant, Andrzej Veitia, Daniel Sank, Evan Jeffrey, Ted C White, Josh Mutus, Austin G Fowler, Brooks Campbell, *et al.*, “Superconducting quantum circuits at the surface code threshold for fault tolerance,” *Nature* **508**, 500–503 (2014).
- [26] Dintomon Joy, M Sabir, Bikash K Behera, and Prasanta K Panigrahi, “Implementation of quantum secret sharing and quantum binary voting protocol in the ibm quantum computer,” *Quantum Information Processing* **19**, 1–20 (2020).
- [27] Joschka Roffe, “Quantum error correction: an introductory guide,” *Contemporary Physics* **60**, 226–245 (2019).
- [28] Zhenyu Cai, Ryan Babbush, Simon C. Benjamin, Suguru Endo, William J. Huggins, Ying Li, Jarrod R. McClean, and Thomas E. O’Brien, “Quantum error mitigation,” *Rev. Mod. Phys.* **95**, 045005 (2023).
- [29] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo, “Experimental quantum error correction,” *Phys. Rev. Lett.* **81**, 2152–2155 (1998).
- [30] Simon J Devitt, William J Munro, and Kae Nemoto, “Quantum error correction for beginners,” *Reports on Progress in Physics* **76**, 076001 (2013).
- [31] Peter W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Phys. Rev. A* **52**, 2493–2496 (1995).
- [32] P. Zanardi and M. Rasetti, “Noiseless quantum codes,” *Phys. Rev. Lett.* **79**, 3306–3309 (1997).
- [33] Paolo Zanardi and Mario Rasetti, “Error avoiding quantum codes,” *Modern Physics Letters B* **11**, 1085–1093 (1997).
- [34] Fumiko Yamaguchi, Kae Nemoto, and William J. Munro, “Quantum error correction via robust probe modes,” *Phys. Rev. A* **73**, 060302 (2006).
- [35] A. M. Steane, “Simple quantum error-correcting codes,” *Phys. Rev. A* **54**, 4741–4751 (1996).
- [36] A. M. Steane, “Error correcting codes in quantum theory,” *Phys. Rev. Lett.* **77**, 793–797 (1996).
- [37] Daniel Gottesman, “Class of quantum error-correcting codes saturating the quantum hamming bound,” *Phys. Rev. A* **54**, 1862–1868 (1996).
- [38] Daniel Gottesman, “Theory of fault-tolerant quantum computation,” *Phys. Rev. A* **57**, 127–137 (1998).
- [39] Kuo, Shu-Yu, Tseng, Kuo-Chun, Yang, Chia-Ching, and Chou, Yao-Hsin, “Efficient multiparty quantum secret sharing based on a novel structure and single qubits,” *EPJ Quantum Technol.* **10**, 29 (2023).
- [40] V. Karimipour and M. Asoudeh, “Quantum secret sharing and random hopping: Using single states instead of entanglement,” *Phys. Rev. A* **92**, 030301 (2015).
- [41] BENNET C. H., “Quantum cryptography : Public key distribution and coin tossing,” *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, Dec. 1984*, 175–179 (1984).
- [42] Charles H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Phys. Rev. Lett.* **68**, 3121–3124 (1992).
- [43] Ryutaroh Matsumoto, “Multiparty quantum-key-distribution protocol without use of entanglement,” *Phys. Rev. A* **76**, 062316 (2007).
- [44] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Phys. Rev. Lett.* **92**, 057901 (2004).
- [45] Fu-Guo Deng and Gui Lu Long, “Secure direct communication with a quantum one-time pad,” *Phys. Rev. A* **69**, 052319 (2004).
- [46] Jian Wang, Quan Zhang, and Chao jing Tang, “Quantum secure direct communication based on order rearrangement of single photons,” *Physics Letters A* **358**, 256–258 (2006).
- [47] Arpita Maitra, “Measurement device-independent quantum dialogue,” *Quantum Information Processing* **16**, 1–15 (2017).
- [48] Ji Xin and Zhang Shou, “Secure quantum dialogue based on single-photon,” *Chinese Physics B* **15**, 1418-1420 (2006).
- [49] D. J. Guan, Yuan-Jiun Wang, and E. S. Zhuang, “A practical protocol for three-party authenticated quantum key distribution,” *Quantum Information Processing* **13**, 2355–2374 (2014).
- [50] Tzonelih Hwang, Kuo-chang Lee, and Chuan-ming Li, “Provably secure three-party authenticated quantum key distribution protocols,” *IEEE Transactions on Dependable and Secure Computing* **4**, 71–80 (2007).
- [51] Song Lin, Hui Wang, Gong-De Guo, Guo-Hua Ye, Hong-Zhen Du, and Xiao-Fen Liu, “Authenticated multi-user quantum key distribution with single particles,” *International Journal of Quantum Information* **14**, 1650002 (2016).
- [52] Daniel Ljunggren, Mohamed Bourennane, and Anders Karlsson, “Authority-based user authentication in quantum key distribution,” *Phys. Rev. A* **62**, 022305 (2000).
- [53] Piotr Zawadzki, “Quantum identity authentication without entanglement,” *Quantum Information Processing* **18**, 1–12 (2019).
- [54] Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek, “Perfect quantum error correcting code,” *Physical Review Letters* **77**, 198 (1996).
- [55] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters, “Mixed-state entanglement and quantum error correction,” *Physical Review A* **54**, 3824 (1996).
- [56] Debbie W Leung, Michael A Nielsen, Isaac L Chuang, and Yoshihisa Yamamoto, “Approximate quantum error correction can lead to better codes,” *Physical Review A* **56**, 2567 (1997).
- [57] Sourav Dutta, Aditya Jain, and Prabha Mandayam, “Smallest quantum codes for amplitude damping noise,” *arXiv preprint arXiv:2410.00155* (2025), <https://doi.org/10.48550/arXiv.2410.00155>.
- [58] Andrew Steane, “Multiple-particle interference and quantum error correction,” *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **452**, 2551–2577 (1996).
- [59] Nirupam Basak, Andrew Tanggara, Ankith Mohan, Goutam Paul, and Kishor Bharti, “Approximate dynamical quantum error-correcting codes,” *arXiv preprint arXiv:2502.09177* (2025), <https://doi.org/10.48550/arXiv.2502.09177>.
- [60] Andrew S. Fletcher, Peter W. Shor, and Moe Z. Win, “Optimum quantum error recovery using semidefinite programming,” *Phys. Rev. A* **75**, 012338 (2007).
- [61] Claude Crepeau, Daniel Gottesman, and Adam Smith, “Approximate quantum error-correcting codes and secret sharing schemes,” *arXiv preprint arXiv:uant-ph/0503139* (2005), <https://doi.org/10.1007/11426639.17>.

- [62] Matthew B. Hastings and Jeongwan Haah, “Dynamically Generated Logical Qubits,” *Quantum* **5**, 564 (2021).
- [63] Margarita Davydova, Nathanael Tantivasadakarn, and Shankar Balasubramanian, “Floquet codes without parent subsystem codes,” *PRX Quantum* **4**, 020341 (2023).
- [64] Jeongwan Haah and Matthew B. Hastings, “Boundaries for the Honeycomb Code,” *Quantum* **6**, 693 (2022).
- [65] David K. Tuckett, Stephen D. Bartlett, and Steven T. Flammia, “Ultra-high error threshold for surface codes with biased noise,” *Phys. Rev. Lett.* **120**, 050505 (2018).
- [66] David K. Tuckett, Stephen D. Bartlett, Steven T. Flammia, and Benjamin J. Brown, “Fault-tolerant thresholds for the surface code in excess of 5% under biased noise,” *Phys. Rev. Lett.* **124**, 130501 (2020).
- [67] DM Tong, Jing-Ling Chen, JY Huang, LC Kwek, and CH Oh, “Kraus representation for the density operator of a qubit,” *Laser physics* **16**, 1512–1516 (2006).
- [68] Luca Chirolli and Guido Burkard, “Decoherence in solid-state qubits,” *Advances in Physics* **57**, 225–285 (2008).
- [69] Akshaya Jayashankar, My Duy Hoang Long, Hui Khoon Ng, and Prabha Mandayam, “Achieving fault tolerance against amplitude-damping noise,” *Phys. Rev. Res.* **4**, 023034 (2022).
- [70] Ivan Djordjevic, “Chapter 7 - quantum error correction,” in *Quantum Information Processing and Quantum Error Correction*, edited by Ivan Djordjevic (Academic Press, Oxford, 2012) pp. 227–276.
- [71] Aravind P. Babu, Tuure Orell, Vasilii Vadimov, Wallace Teixeira, Mikko Möttönen, and Matti Silveri, “Quantum error correction under numerically exact open-quantum-system dynamics,” *Phys. Rev. Res.* **5**, 043161 (2023).
- [72] Philipp Schindler, Julio T. Barreiro, Thomas Monz, Volckmar Nebendahl, Daniel Nigg, Michael Chwalla, Markus Hennrich, and Rainer Blatt, “Experimental repetitive quantum error correction,” *Science* **332**, 1059–1061 (2011).
- [73] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, “Repeated quantum error correction on a continuously encoded qubit by real-time feedback,” *Nature Communications* **7** (2016), 10.1038/ncomms11526.
- [74] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Yu Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P. J. J. O’Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A. N. Cleland, and John M. Martinis, “State preservation by repetitive error detection in a superconducting quantum circuit,” *Nature* **519**, 66–69 (2015).
- [75] Christian Kraglund Andersen, Ants Remm, Stefania Lazar, Sebastian Krinner, Nathan Lacroix, Graham J. Norris, Mihai Gabureac, Christopher Eichler, and Andreas Wallraff, “Repeated quantum error detection in a surface code,” *Nature Physics* **16**, 875–880 (2020).
- [76] Sebastian Krinner, Nathan Lacroix, Ants Remm, Agustin Di Paolo, Elie Genois, Catherine Leroux, Christoph Hellings, Stefania Lazar, Francois Swiadek, Johannes Herrmann, Graham J. Norris, Christian Kraglund Andersen, Markus Müller, Alexandre Blais, Christopher Eichler, and Andreas Wallraff, “Realizing repeated quantum error correction in a distance-three surface code,” *Nature* **605**, 669–674 (2022).
- [77] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
- [78] John Stack, Ming Wang, and Frank Mueller, “Assessing teleportation of logical qubits in a distributed quantum architecture under error correction,” *arXiv preprint arXiv:2504.05611* (2025), <https://doi.org/10.48550/arXiv.2504.05611>.
- [79] J. Pablo Bonilla Ataides, Hengyun Zhou, Qian Xu, Gefen Baranes, Bikun Li, Mikhail D. Lukin, and Liang Jiang, “Constant-overhead fault-tolerant bell-pair distillation using high-rate codes,” *arXiv preprint arXiv:2502.09542* (2025), <https://doi.org/10.48550/arXiv.2502.09542>.
- [80] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters, “Purification of noisy entanglement and faithful teleportation via noisy channels,” *Phys. Rev. Lett.* **76**, 722–725 (1996).
- [81] C. Ryan-Anderson, N. C. Brown, C. H. Baldwin, J. M. Dreiling, C. Foltz, J. P. Gaebler, T. M. Gatterman, N. Hewitt, C. Holliman, C. V. Horst, J. Johansen, D. Lucchetti, T. Mengle, M. Matheny, Y. Matsuoka, K. Mayer, M. Mills, S. A. Moses, B. Neyenhuis, J. Pino, P. Siegfried, R. P. Stutz, J. Walker, and D. Hayes, “High-fidelity teleportation of a logical qubit using transversal gates and lattice surgery,” *Science* **385**, 1327–1331 (2024).
- [82] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger, “Experimental quantum teleportation,” *Nature* **390**, 575–579 (1997).
- [83] Mohamed A. Shalby, Renyu Wang, Denis Sedov, and Leonid P. Pryadko, “Optimized noise-resilient surface code teleportation interfaces,” *arXiv preprint arXiv:2503.04968* (2025), <https://doi.org/10.48550/arXiv.2503.04968>.