

Quantum steganography using catalytic and entanglement-assisted quantum codes

Sanjoy Dutta,^{1,2,*} Nihar Ranjan Dash,^{3,†} Subhashish Banerjee,^{3,‡} and R. Srikanth^{1,§}

¹*Poornaprajna Institute of Scientific Research (PPISR), Bidalur post, Devanahalli, Bengaluru 562164, India*

²*Graduate Studies, Manipal Academy of Higher Education, Madhava Nagar, Manipal 576104, India*

³*Indian Institute of Technology Jodhpur, Rajasthan 342030, India*

Steganography is the technique for transmitting a secret message by employing subterfuge to conceal it in innocent-looking data, rather than by overt security measures as in cryptography. Typically, non-degenerate quantum error-correcting codes (QECCs) are used as the cover medium, with the stego message disguised as noise. As in cryptography, a large number of bits or ebits are pre-shared, in this case mainly in order to ensure the innocence effect. In this work we develop three steganographic protocols: first, a scheme based on catalytic quantum codes to minimize initial pre-shared resources; second, a scheme incorporating prior entanglement into QECCs in the form of possibly degenerate entanglement-assisted QECCs; third, a scheme that uses the phase bit of a pre-shared ebit, combined with QECCs.

I. INTRODUCTION

Steganography is a technique to hide data within innocent-looking cover media [1]. For example, the secret information may be embedded in the cover provided by an audio signal [2], with the view to exploiting the large size, high data transmission rate and redundancy provided by this type of signal. In the traditional setting, steganography can be motivated by considering Alice and Bob, who have been imprisoned in two geographically separated cells of a penitentiary. The prison warden (Eve) allows them to communicate by swapping messages through a courier loyal to the warden. Under the circumstance, they exchange secret messages steganographically without rousing the warden's suspicion. Quantum steganography is a technique that enhances classical steganography by leveraging quantum information theoretic principles such as superposition, no-cloning and entanglement [3, 4]. Three basic requirements for steganography are imperceptibility, security and capacity [5]. This contrasts steganography from cryptography, which lacks the imperceptibility requirement [6]. Nevertheless, Sanguinetti et al. [7] point out that both steganographic and cryptographic protocols have a basic, identical requirement: a random key as long as the message. Moreover, a quantum cryptographic cover can be employed for steganography [8].

The first quantum protocol for steganography was proposed by Gea-Banacloche, who used a code word of a quantum error correcting code (QECC) as cover message, and an error syndrome as the secret message [9]. However the protocol lacked the innocence effect, as the error statistics would reflect the secret message rather than a natural noisy channel. For ensuring the innocence, Shaw and Brun use pre-shared bits to hide the secret information as (deliberately applied) typical errors of a depolarizing channel [10]. Building on this idea, a stego-protocol that exploits Eve's partial knowledge of the channel was proposed in Ref. [11]. Refs. [12] and [13] propose quantum stego-protocols using pre-shared entanglement

instead of pre-shared bits, with the encoding process exploiting QECC or Brown states, respectively, to combat against quantum noise.

More recently, quantum image steganography protocols have been proposed that extend steganography to quantum data hiding protocols based on image steganographic methods [14–16]. A proposal due to Abd El Latif et al. [17] exploits quantum walk for steganographic image transfer. Joshi et al. [18] present a scheme for steganographic communication based on encoding the secret bit in the position and momentum quadratures of coherent-states. In [19], the authors propose a quantum stego-protocol based on a Mach-Zehnder setup, where the secret is encoded using a particle's entanglement, while the cover data is encoded into its polarization. Quantum steganography can be applied over quantum networks [20], and furthermore machine-learning can be used to optimize data embedding strategies in quantum steganography [21].

In this manuscript, we study various directions for improving or simplifying the resource consumption in quantum steganography. In current stego-protocols that employ pre-shared entanglement, there is a requirement for a large number of ebits at the start of the protocol. First, after presenting preliminaries briefly (Section II), we propose a protocol that employs catalytic QECC to minimize the initial requirement for ebits (Section III). Moreover, in protocols that use pre-shared entanglement, the encoding (via QECC, Brown state etc.) required for noise resilience is independent of the pre-shared state. Here we study how these two processes can be combined by the use of entanglement assisted QECC (EAQECC), where we additionally consider the role of quantum degeneracy of errors (Section IV). Finally, we elucidate the mathematical structure of the Mihara protocol [12], in specific by presenting a stego-protocol that exploits the phase bit of the pre-shared ebit, rather than the parity bit, as done there (Section V). We present our conclusions and discussions in the final section (Section VI).

II. PRELIMINARIES

* sanjoy@ppisr.res.in

† dash.1@iitj.ac.in

‡ subhashish@iitj.ac.in

§ srik@ppisr.res.in

a. EAQECC An EAQECC uses pre-shared entanglement to improve the noise resistance of a QECC. Given ebits ($|\phi^+\rangle_{AB}^{\otimes e}$) between the two communicating parties, an EAQECC can be constructed from any linear classical code by relaxing the constraint of dual containing classical code, which is necessary for the construction of a stabilizer QECC [22, 23], defined by a set of commuting stabilizer generators. More generally, quadratic constraints are imposed on the classical code to obtain a quantum code of qubits or qudits. These constraints take the form of dual containment (in the case of stabilizer or CSS codes) or symplectic self-orthogonality (in the case of general qudit stabilizer codes), and ensure that the resulting error correcting code enforces commuting relationships among the stabilizers.

In the case of an $[[n, k, d; e]]$ EAQECC, the stabilizer group over the n qubits can be non-abelian, thus allowing us to relax the above quadratic constraints on the classical linear codes. Here Alice encrypts the k -qubit state $|\psi\rangle$ in n -qubits, and appending the e extra Pauli operators, the stabilizers are rendered commuting. During encoding, Alice appends $a \equiv n - k - e$ ancillas before an encryption operation ($U_A \otimes I_B$) on her n particles to produce the encoded state $(U_A \otimes I_B)|\psi\rangle \otimes |0\rangle^a \otimes |\phi^+\rangle_{AB}^{\otimes e}$ [24].

b. Catalytic QECC In the context of quantum communication using EAQECC, Alice consumes pre-shared ebits prepared in the state $|\Phi^+\rangle$. Assume that they have small number of pre-shared ebits but she has the resource of locally available ebits. To compensate for the loss of ebits during communication, Alice includes e halves of the local ebits into the state $|\psi\rangle$ to be encoded, thus $k \geq e$. After her transmission of the encoded register to Bob, and his decoding, the entangled state $|\Phi^+\rangle^{\otimes e}$ will be established as the pre-shared entanglement for the next cycle. This technique of constructing catalytic QECC can also be applied to standard QECCs encoding entangled states. [25, 26].

c. Degenerate QECC Degeneracy of errors is the phenomenon whereby distinct error operators from the correctable set \mathcal{E} of errors act on a quantum code to send it to the same erroneous state [27]. By way of example, consider the 3 qubit code:

$$\begin{aligned} |w = 0_L\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ |w = 1_L\rangle &= \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle). \end{aligned} \quad (1)$$

The code space spanned by $|0_L\rangle$ and $|1_L\rangle$ is driven to the same erroneous subspace by the operators Z_1 and Z_3 .

III. PROTOCOL USING CATALYTIC QECC

A pre-shared resource is required in quantum steganography for producing the innocence effect, in the form of bits [10] or ebits [12]. This entails the consumption of this resource during each usage of the stego protocol. In the case of ebits, the resource being costly, a catalytic QECC can be useful in

recycling the consumed ebits. Our following protocol employs a dense-coding like scheme, in which entanglement is replenished after each round by using a QECC of sufficiently large rate and an initial stock of local entanglement.

1. Alice and Bob pre-share an ebit $|\Phi^+\rangle_{AB}$, and agree on a $[[n, k, d; 0]]$ QECC, with $k \geq 2$. (More generally, if secret rate is k_s , then $k = 2k_s$.) Further, Alice prepares a local ebit $|\Phi^+\rangle_{l_1, l_2}$.
2. Alice decides on two bits— the cover message w , and the secret bit b , and employs dense coding to prepare the Bell state $|\eta(w, b)\rangle_{AB} \equiv (|0, w\rangle + (-1)^b |1, \bar{w}\rangle)_{AB}$.
3. Alice then encodes one half of her local ebit and her entangled qubits, i.e., the first two particles in the state

$$\begin{aligned} |\Phi^+\rangle_{l_1, l_2} |\eta(w, b)\rangle_{AB} &= |0, 0\rangle_{l_1, A} |0, w\rangle_{l_2, B} + \\ &(-1)^b |0, 1\rangle_{l_1, A} |0, \bar{w}\rangle_{l_2, B} + |1, 0\rangle_{l_1, A} |1, w\rangle_{l_2, B} + \\ &(-1)^b |1, 1\rangle_{l_1, A} |1, \bar{w}\rangle_{l_2, B} \end{aligned}$$

obtaining

$$\begin{aligned} &|(0, 0)_L\rangle_{l_1, A} |0, w\rangle_{l_2, B} + (-1)^b |(0, 1)_L\rangle_{l_1, A} |0, \bar{w}\rangle_{l_2, B} + \\ &|(1, 0)_L\rangle_{l_1, A} |1, w\rangle_{l_2, B} + (-1)^b |(1, 1)_L\rangle_{l_1, A} |1, \bar{w}\rangle_{l_2, B} \end{aligned} \quad (2)$$

4. She transmits her particles to Bob over a noisy channel. After performing the necessary quantum error correction using her and his particles jointly, and decoding the resultant state, he obtains $|\Phi^+\rangle_{l_1, l_2} |\eta(w, b)\rangle_{A, B}$, where particles A, B, l_1 are now with Bob.
5. On the particles A, B Bob applies a CNOT with the control on B followed by a Hadamard on B . This results in the transformation

$$|\eta(w, b)\rangle \longrightarrow |w\rangle |b\rangle.$$

6. The state $|\Phi^+\rangle_{l_1, l_2}$ will serve as shared ebit of the next round.

The catalytic aspect, which is the replenishment of the entanglement consumed, ensures that the initial pre-shared ebit suffices to transmit any number of secret qubits, over subsequent rounds.

Note that because we employ a dense-coding protocol, Alice is restricted to transmitting a classical cover message and classical secret message. This rules out that the protocol as it is can be used for transmitting a quantum secret with a quantum cover message. Quite generally, this follows from the idea that even with pre-shared entanglement, Alice cannot transmit two qubits by sending one physical qubit. Even so, this doesn't rule out a probabilistic protocol for transmitting a qubit secret embedded in a qubit cover medium. We describe one below.

Consider an arbitrary single qubit state $\cos(\alpha)|b=0\rangle + \sin(\alpha)e^{i\beta}|b=1\rangle$ as a secret, as well as an arbitrary cover message $\cos(\mu)|w=0\rangle + \sin(\mu)e^{i\gamma}|w=1\rangle$. Alice by means of her

local operations must prepare the state

$$|\eta(\mathbf{b}, \mathbf{w})\rangle = \cos(\mu) \left(\cos(\alpha) |\Phi^+\rangle + \sin(\alpha) e^{i\beta} |\Phi^-\rangle \right) + \sin(\mu) e^{i\nu} \left(\cos(\alpha) |\Psi^+\rangle + \sin(\alpha) e^{i\beta} |\Psi^-\rangle \right). \quad (3)$$

To do so, Alice prepares the secret state and cover message in qubit ancillas, and applies a C-phase and C-not gate with the former and the latter as the respective control qubits, while the target qubit is her half of the entanglement shared with Bob. This yields:

$$\begin{aligned} & \left(\cos(\mu) |0\rangle + \sin(\mu) e^{i\nu} |1\rangle \right) \left(\cos(\alpha) |0\rangle + \sin(\alpha) e^{i\beta} |1\rangle \right) |\Phi^+\rangle \\ & \rightarrow |\eta(\mathbf{b}, \mathbf{w})\rangle. \end{aligned}$$

Measuring the first two registers in the diagonal (XX) basis, she produces the required state $|\eta(\mathbf{b}, \mathbf{w})\rangle$ with probability $\frac{1}{4}$, conditioned on obtaining $|+, +\rangle$. It is assumed that Alice can publicly communicate to Bob the instance of successful encoding, without arousing Eve's suspicion.

For large n , we can use the asymptotic quantum Gilbert-Varshamov bound to estimate the allowed stego code rate. This bound asserts that given n and code distance $\delta \equiv d/n$, then there exist good codes, i.e., a code with rate $R = \frac{k}{n} \geq 1 - 2H_2(\delta) - 2\delta \log_2 3$. Noting that $k = 2k_s$, the asymptotic secrecy rate for our catalytic stego protocol is

$$R_s \geq \frac{1}{2} - H_2(\delta) - \delta \log_2 3, \quad (4)$$

where $R_s \equiv \frac{k_s}{n}$.

IV. USING DEGENERATE EAQECC

We now propose a stego protocol which, like that in Refs. [9, 10], employs channel noise in order to encode the message. We assume that Alice and Bob in fact use a noiseless channel, and simulate noise for the purpose of steganographic communication. In [10], the messages are camouflaged using twirling and pre-shared bits. In the present protocol (which we shall call scheme \mathcal{Q}), we will instead employ pre-shared entanglement of an EAQECC for this purpose, together with code degeneracy.

Suppose the set of errors that Alice (resp., Bob) can apply to her (resp., his) qubits is denoted $E_A \equiv \{e_A\}$ (resp., $E_B \equiv \{e_B\}$). Importantly, Alice's errors must be correctable and characteristic of the channel noise that Eve expects. The combination of the two legitimate parties' errors need not be correctable but must satisfy:

$$e_B e_A \in \mathcal{S} \cup (E_A - I) \circ \mathcal{N}(\mathcal{S}), \quad (5)$$

where $\mathcal{N}(\mathcal{S})$ denotes the normalizer of the stabilizer \mathcal{S} . The basic idea here is that Alice encodes her messages via errors, which Bob decodes by syndrome measurement. In the event of being challenged by Eve, Bob applies an element randomly drawn from set E_B . The effectiveness of the method is clarified by the following theorem.

Theorem 1. *In protocol \mathcal{Q} , Bob can eliminate Alice's messaging by his local application of errors, provided Eq. (5) is satisfied. To achieve innocence (asymptotically), the entropy in Alice's alphabet must be sufficiently low.*

Proof. To begin with, Alice encodes her cover message $|\psi\rangle_A$ into an EA code logical state $|\psi_L\rangle_{AB}$. Suppose her secret bit corresponds to error $e_A \in E_A$. She prepares the state $e_A |\psi_L\rangle_{AB}$ and transmits her qubits to Bob. As e_A is correctable, Bob obtains the secret message (normal mode). However, if Eve challenges the duo (challenge mode), Bob surrenders his qubit after applying to his qubits a random error e_B sampled over set E_B by a probability distribution \mathcal{P} . Two possibilities arise:

$e_B e_A \in \mathcal{S}$: The two errors neutralize by virtue of degeneracy of e_A and e_B . Eve interprets this as a possible action of the expected channel noise.

$e_B e_A \in (E_A - I) \circ \mathcal{N}(\mathcal{S})$: The logical state is rotated within the code space up to an allowed error. Eve interprets this as a possible action of the expected channel noise on a rotated state¹.

Bob's action corresponds to a trace-preserving completely positive (TPCP) map and thus doesn't decrease the entropy of Alice's secret message. Let p_j be the probability with which Alice applies error $e_A^{(j)}$. Alice's encoding action represents the quantum map $|\Psi_L\rangle \rightarrow \rho_A \equiv \sum_j p_j e_A^{(j)} |\Psi_L\rangle \langle \Psi_L| e_A^{(j)\dagger}$. Since the applied errors are correctable, each of them takes the encoded state to an orthogonal state. Thus the von Neumann entropy $S(\rho_A) = H(\{p_j\})$, where $H(\cdot)$ denotes the Shannon binary entropy. Bob's action is a similar TPCP map, given by $\rho_A \rightarrow \rho_B \equiv \sum_j q_j e_B^{(j)} \rho_A e_B^{(j)\dagger}$. We then have

$$\begin{aligned} S(\rho_B) &= S\left(\sum_j q_j e_B^{(j)} \rho_A e_B^{(j)\dagger}\right) \geq \sum_j q_j S(e_B^{(j)} \rho_A e_B^{(j)\dagger}) \\ &= \sum_j q_j S(\rho_A) = S(\rho_A) \\ &= H(\{p_j\}), \end{aligned} \quad (6)$$

where the inequality in the first line follows from the concavity of the entropy function S , and the subsequent equality follows from the unitary invariance of Shannon entropy. (The derivation essentially expresses the positivity of the Holevo quantity.) The non-increase of entropy under Bob's action implies that only if the entropy of Alice's message is sufficiently low, then Bob can tune the probability distribution of his choices such that he simulates the statistics of the noisy channel expected by Eve. \square

We give below a simple example to illustrate the basic idea behind Theorem 1. Suppose Eve expects Alice's communication to be subject to a dephasing channel $\mathcal{E} \equiv (1-r)\mathcal{I} + r\mathcal{Z}$ ($0 \leq r \leq 1$), and Alice and Bob know this.

¹ In the second possibility above, the reason that we exclude the case $I \circ \mathcal{N}(\mathcal{S})$ is that the weight of an arbitrary error e satisfies $|e| \leq \lfloor \frac{d-1}{2} \rfloor$. Thus $|e_A e_B| \leq d-1$, whereas any logical operator O_L is such that $|O_L| \geq d$.

The duo replace the channel with a noiseless one, and use $[[6, 1, 3; 3]]$ EAQECC constructed from $[[9, 1, 3]]$ Shor code, represented by the stabilizer generator set

$$\mathcal{S} = \{s_1 = Z_1 Z_2, s_2 = Z_2 Z_3, s_3 = Z_4 Z_5, s_4 = Z_5 Z_6, s_5 = Z_7 Z_8, s_6 = Z_8 Z_9, s_7 = X_1 X_2 X_3 X_4 X_5 X_6, s_8 = X_4 X_5 X_6 X_7 X_8 X_9\}. \quad (7)$$

A cover message $w = 0, 1$ corresponds to the codewords, respectively:

$$\begin{aligned} |0_L\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ |1_L\rangle &= \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle), \end{aligned} \quad (8)$$

where the qubits 3, 6 and 9 (represented by the bold letter) are with Bob, while the other six with Alice. The stego channel allows a 2-bit communication. To encode secret messages, Alice applies her errors according to the following convention

Bit value	Error applied	Degenerate counterpart
00	I	I
01	Z_1, Z_2	Z_3
10	Z_4, Z_5	Z_6
11	Z_7, Z_8	Z_9

Thus $E_A = \{I, Z_1, Z_2, Z_4, Z_5, Z_6, Z_7\}$. In the event of Eve's challenge, Bob randomly applies error from the set $E_B = \{I, Z_3, Z_6, Z_9\}$.

To encode the secret message $b = 10$ into the cover message $w = 0$, the stego message used can be $Z_4|0_L\rangle$. In the challenge mode, to erase or randomize the secret message, Bob randomly applies one of I, Z_3, Z_6, Z_9 on his qubits before surrendering his three qubits to Eve. If Bob applies Z_6 , which acts on the block as Z_4 , then the errors cancel by virtue of degeneracy, noting that $Z_6 Z_4$ lies in the stabilizer \mathcal{S} . On the other hand, he could also apply Z_3 or Z_9 , which lie in a different block than Z_4 . Suppose without loss of generality, it is the latter:

$$Z_9 Z_4 |0_L\rangle = (Z_1)^2 Z_9 Z_4 |0_L\rangle = Z_1 X_L |0_L\rangle = Z_1 |1_L\rangle \quad (9)$$

Thus, Eve interprets the state as a Z_1 error on the code word $|1_L\rangle$.

Let Alice encode the bits 00, 01, 10 and 11 with probability p_{00}, p_{01}, p_{10} and p_{11} respectively. Suppose during this transmission Eve suspects and challenges them to surrender their qubits. To randomize the secret encoded message, Bob before surrendering randomly applies I, Z_3, Z_6 or Z_9 operators on his entangled qubits with probability q_{00}, q_{01}, q_{10} and q_{11} respectively. Suppose that the resulting probabilities are denoted r_{00}, r_{01}, r_{10} and r_{11} . It is readily shown that

$$\begin{pmatrix} r_{00} \\ r_{01} \\ r_{10} \\ r_{11} \end{pmatrix} = \begin{pmatrix} q_{00} & q_{01} & q_{10} & q_{11} \\ q_{01} & q_{00} & q_{11} & q_{10} \\ q_{10} & q_{11} & q_{00} & q_{01} \\ q_{11} & q_{10} & q_{01} & q_{00} \end{pmatrix} \begin{pmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{pmatrix}. \quad (10)$$

By Eq. (6), we have

$$H(\{r_j\}) = - \sum_{j=0}^{11} r_j \log_2(r_j) \geq H(\{p_j\}) = - \sum_{j=0}^{11} p_j \log_2(p_j). \quad (11)$$

In other words, Bob cannot lower the randomness in the errors in Alice's message. Thus Alice's message should start with sufficiently low entropy such that after Bob's randomization, the $\{r_k\}$ matches Eve's expected error behavior of the channel.

V. STEGANOGRAPHY USING PHASE BIT OF EBIT

In the stego protocol of Ref. [12], the parity bit of a pre-shared EPR pair is used for transmitting the secret bit, reminiscent of partial dense coding. The encoding employs parts of a quantum code rather than the full code. Yet parity errors can be corrected by applying the parity check matrix of the underlying classical code, to each ket in the superposition. The receiver corrects the phase flip error later, after making the parity-error corrected state separable. In our method we use the phase bit instead of the parity bit for the purpose. In this case, directly adapting Mihara's idea isn't possible, because the underlying classical code cannot correct phase errors, and converting the phase errors to bit-flip errors by applying Hadamards to all qubits won't work because the state with Bob is not separable. Thus, we need to make suitable modifications, as described below.

A linear $[[n, k, d]]$ QECC can be defined by $m = n - k$ stabilizer generators. Let $|w_L\rangle$ ($0 \leq w \leq 2^k - 1$) denote a codeword of this QECC, and $q \equiv \lfloor \frac{d-1}{2} \rfloor + 1$. Let \mathbb{G} be the group consisting of all computational basis states in the support of $|0_L\rangle$ and $L_0 (\subseteq \mathbb{G})$ be the subgroup defined as follows

$$L_0 = \{v \in \mathbb{G} \mid \vec{q} \cdot v = 0\}, \quad (12)$$

where \vec{q} is a n -bit vector of Hamming weight $|\vec{q}| = q$. Applying Lagrange theorem, we find that the integer $l \equiv \frac{|\mathbb{G}|}{|L_0|} \in \{1, 2\}$. We choose \vec{q} such that $l = 2$. Further define coset $L_1 \equiv \mathbb{G} - L_0$. Note that $\forall_{v \in L_1} \vec{q} \cdot v = 1$.

We express $|0_L\rangle$ as the superposition:

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|L_0\rangle + |L_1\rangle), \quad (13)$$

where

$$\begin{aligned} |L_0\rangle &= \sqrt{2} \left(\sum_{v \in L_0} |v\rangle \langle v|0_L\rangle \right), \\ |L_1\rangle &= \sqrt{2} \left(\sum_{v \in L_1} |v\rangle \langle v|0_L\rangle \right). \end{aligned} \quad (14)$$

Analogous to Eq. (13), we can define such superpositions for all codewords:

$$|w_L\rangle = \frac{1}{2}(|L_0^{(w)}\rangle + |L_1^{(w)}\rangle), \quad (15)$$

since in each case, $L_0^{(w)} \cup L_1^{(w)}$ is a coset of \mathbb{G} . Note that in our notation $L_j^{(0)} = L_j$ for $j \in \{0, 1\}$.

Alice and Bob share an entangled state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{AB}. \quad (16)$$

For encoding secret bit $b \in \{0, 1\}$, she applies the local unitary Z_1^b to her qubit to produce the state:

$$Z_1^b |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + (-1)^b |1,1\rangle)_{AB}. \quad (17)$$

She encodes her entangled qubit to create the following state :

$$|\Upsilon(w, b)\rangle \equiv \frac{1}{\sqrt{2}}(|L_0^{(w)}, 0\rangle + (-1)^b |L_1^{(w)}, 1\rangle)_{AB}. \quad (18)$$

She dispatches her qubits to Bob. During transit, her n qubits may pick up an arbitrary error E of weight up to $\lfloor \frac{d-1}{2} \rfloor$. Bob receives the erroneous state:

$$E |\Upsilon(w, b)\rangle = E \frac{1}{\sqrt{2}}(|L_0^{(w)}, 0\rangle + (-1)^b |L_1^{(w)}, 1\rangle)_{AB}. \quad (19)$$

In general, Bob won't be able to measure the error syndrome, because the code fragments $|L_j^{(w)}\rangle$ ($j \in \{0, 1\}$) are entangled with Bob's qubit. Error correction will thus require an indirect method.

We define the Hamming support $h_q(\mathcal{P})$ of an n -qubit Pauli operator \mathcal{P} as the set of Pauli operators that appear in \mathcal{P} at the coordinates where \hat{q} has 1. For example, given $\hat{q} = (1, 0, 0, 1)$, we have $\hat{q}[IXYX] = \{I_1, X_4\}$ and $\hat{q}[ZXIZ] = \{Z_1, Z_4\}$. Now, the set of stabilizer generators are of two types:

Non-flipping: A stabilizer generator S_{NF} such that $h_q(S_{\text{NF}})$ contains an even number of operators X and Y . It is easy to show that they have the symmetry property:

$$S_{\text{NF}} |L_j^{(w)}\rangle = |L_j^{(w)}\rangle \quad (j \in \{0, 1\}). \quad (20)$$

In other words, the stabilizers S_{NF} are equivalent to an identity operation in the subspace $\mathfrak{S}^{(w)}$ spanned by the vectors $|L_0^{(w)}\rangle$ and $|L_1^{(w)}\rangle$.

Flipping: A stabilizer generator S_{F} is such that $h_q(S_{\text{F}})$ contains an odd number of operators X or Y . It is easy to show that they have the flipping property:

$$S_{\text{F}} |L_j^{(w)}\rangle = |\overline{L_j^{(w)}}\rangle \quad (j \in \{0, 1\}), \quad (21)$$

where the overline represents the complementation operation $\overline{0} = 1$ and $\overline{1} = 0$. In other words, the stabilizers S_{F} are equivalent to a NOT operation in the subspace $\mathfrak{S}^{(w)}$.

The syndrome corresponding to a non-flipping stabilizer generators can be obtained in the standard way, by ignoring the entanglement. Given stabilizer S_{NF} with corresponding syndrome s_{NF} , we find

$$\begin{aligned} & (S_{\text{NF}} \otimes \mathbb{I})(E \otimes \mathbb{I}) |\Upsilon(w, b)\rangle \\ &= (S_{\text{NF}} E \otimes \mathbb{I}) \frac{1}{\sqrt{2}}(|L_0^{(w)}, 0\rangle + (-1)^b |L_1^{(w)}, 1\rangle)_{AB} \\ &= (-1)^{s_{\text{NF}}} (E \otimes \mathbb{I}) \frac{1}{\sqrt{2}}(|L_0^{(w)}, 0\rangle + (-1)^b |L_1^{(w)}, 1\rangle)_{AB}, \end{aligned} \quad (22)$$

where $s_{\text{NF}} \in \{0, 1\}$.

However, the state in Eq. (18) is not an eigenstate of any $(S_{\text{F}} \otimes \mathbb{I})$. Thus, error correction must proceed in another way. To this end, we observe that the stego-state is an eigenstate of the product of any two distinct flipping stabilizer generators, for

$$\begin{aligned} & (S'_{\text{F}} S_{\text{F}} E \otimes \mathbb{I}) |\Upsilon(w, b)\rangle_{AB} \\ &= (S'_{\text{F}} S_{\text{F}} E \otimes \mathbb{I}) \frac{1}{\sqrt{2}}(|L_0^{(w)}, 0\rangle + (-1)^b |L_1^{(w)}, 1\rangle)_{AB} \\ &= (-1)^{s'_{\text{F}} + s_{\text{F}}} (E \otimes \mathbb{I}) \frac{1}{\sqrt{2}}(|L_0^{(w)}, 0\rangle + (-1)^b |L_1^{(w)}, 1\rangle)_{AB} \end{aligned}$$

where $s_{\text{F}}, s'_{\text{F}} \in \{0, 1\}$. Bob extracts the syndrome value $s'_{\text{F}} + s_{\text{F}}$. Proceeding thus pairwise, he can obtain $\binom{\varphi}{2}$ sums, where φ is the number of flipping stabilizers. Provided this isn't smaller than φ , i.e.,

$$\binom{\varphi}{2} \geq \varphi,$$

we have enough sums to simultaneously solve for the φ eigenvalues of the flipping stabilizer generators.

From the error syndromes he can identify E and correct it to obtain the original state Eq. (18). To this end, we require to identify the *sublogical* operations, i.e., encoded operations for the subspace spanned by $\{|L_0\rangle, |L_1\rangle\}$. Denote by q_i ($1 \leq i \leq n$) the bits constituting vector \vec{q} . Then the encoded Z operator in the subspace spanned by $|L_0\rangle$ and $|L_1\rangle$, denoted \overline{Z} , is given by $\bigotimes_{i=1}^n Z^{q_i}$, with the identity $Z^0 = \mathbb{I}$. For example, given $\vec{q} = 010011$, we have $\overline{Z} = Z_2 Z_5 Z_6$. This ensures that $\overline{Z}|L_0\rangle = |L_0\rangle$, $\overline{Z}|L_1\rangle = -|L_1\rangle$. Recollecting that the flipping and non-flipping stabilizers behave, respectively, like the encoded identity \overline{I} and \overline{X} in the subspace $\mathfrak{S}^{(w)}$, we find that $[\overline{Z}, S_{\text{NF}}] = 0$ and $[\overline{Z}, S_{\text{F}}] = 0$.

Now Bob applies Controlled- S_{F} to the stego-state in Eq. (18), with the transmitted qubits as target and his entangled qubit as control:

$$|\Upsilon(w, b)\rangle_{AB} \xrightarrow{C-S_{\text{F}}} |L_0^{(w)}\rangle (|0\rangle + (-1)^b |1\rangle) \quad (23)$$

Measuring his qubit in the X basis, he extracts the secret message b . Finally, application of the *sublogical* Hadamard $\overline{H} \equiv \frac{1}{\sqrt{2}}(S_{\text{F}} + \overline{Z})$ to the transmitted qubits restores the cover message

$$|L_0^{(w)}\rangle \xrightarrow{\overline{H}} \frac{1}{\sqrt{2}}(|L_0^{(w)}\rangle + |L_1^{(w)}\rangle)$$

. We remark that by virtue of linearity, the secret can be a quantum state $\alpha|b=0\rangle + \beta|b=1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, in which case the initial entangled state will be $\alpha|\Phi^+\rangle + \beta|\Phi^-\rangle$ in Eq. (17). Similarly, the cover message can also be a superposition $\sum_w c_w |w\rangle$ ($\sum_w |c_w|^2 = 1$).

Below we present an example of this protocol using the 5-qubit code. Consider the $[[n=5, k=1, d=3]]$ QECC code

for steganographic communication defined by the stabilizer generators $S_1 = XZZXI, S_2 = XIXZZ, S_3 = IXZZX, S_4 = ZXIXZ$. For the cover message $w \in \{0, 1\}$, we use the encoded cover message state $|w_L\rangle = \prod_{i=1}^4 (I^{\otimes 5} + S_i) |w\rangle^{\otimes 5}$ [28]. For the cover message $w = 0$, the logical state is

$$\begin{aligned} |0_L\rangle = & \frac{1}{4} \left(|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \right. \\ & + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ & - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ & \left. - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle \right). \end{aligned} \quad (24)$$

We choose $\vec{q} = (0, 0, 0, 1, 1)$. In the manner of Eqs. (13) and (14), we have

$$|0_L\rangle = \frac{1}{\sqrt{2}} \left(|L_0\rangle + |L_1\rangle \right), \quad (25)$$

where

$$\begin{aligned} |L_0\rangle = & \frac{1}{2\sqrt{2}} \left(|00000\rangle + |10100\rangle - |11011\rangle - |11000\rangle \right. \\ & \left. - |00011\rangle - |01111\rangle - |01100\rangle - |10111\rangle \right), \\ |L_1\rangle = & \frac{1}{2\sqrt{2}} \left(|10010\rangle + |01001\rangle + |01010\rangle - |00110\rangle \right. \\ & \left. - |11101\rangle - |11110\rangle - |10001\rangle + |00101\rangle \right). \end{aligned} \quad (26)$$

Beforehand, sender Alice and receiver Bob pre-share the Bell state $|\Phi^+\rangle$. Alice encodes the secret message b as in Eq. (17). She then encodes her particle in the manner of Eq. (18), $|\Upsilon(0, b)\rangle_{AB} \equiv \frac{1}{\sqrt{2}} \left(|L_0\rangle |0\rangle + (-1)^b |L_1\rangle |1\rangle \right)_{AB}$. She transmits her 5 qubits to Bob through the noisy channel and Bob receives the erroneous state as given in Eq. (19) $E|\Upsilon(w, b)\rangle$, with E being an arbitrary single-qubit error. We assume that his entangled particle is error-free, an assumption justified because his qubit hasn't been transmitted across the channel.

Here S_1, S_3 and S_4 are the flipping stabilizers, while S_2 is the only non-flipping stabilizer. Upon receiving Alice's qubits, Bob implements the following protocol:

(1) For the non-flipping stabilizer, Bob can extract the syndrome by direct measurement of the stabilizer on the first 5 qubits.

$$\begin{aligned} S_2 E |\Upsilon(0, b)\rangle_{AB} &= S_2 E (|L_0\rangle |0\rangle + (-1)^b |L_1\rangle |1\rangle) \\ &= (-1)^{s_2} E S_2 (|L_0\rangle |0\rangle + (-1)^b |L_1\rangle |1\rangle) \\ &= (-1)^{s_2} E |\Upsilon(0, b)\rangle_{AB}. \end{aligned} \quad (27)$$

(2) For the flipping stabilizers, Bob extracts the pairwise sums of syndromes by joint measurement of pairs of stabilizers. For example

$$\begin{aligned} S_4 S_3 E |\Upsilon(0, b)\rangle_{AB} &= S_4 S_3 E (|L_0\rangle |0\rangle + (-1)^b |L_1\rangle |1\rangle)_{AB} \\ &= (-1)^{s_3} S_4 E S_3 (|L_0\rangle |0\rangle + (-1)^b |L_1\rangle |1\rangle)_{AB} \\ &= (-1)^{s_3} S_4 E (|L_1\rangle |0\rangle + (-1)^b |L_0\rangle |1\rangle)_{AB}, \\ &= (-1)^{s_3+s_4} E S_4 (|L_1\rangle |0\rangle + (-1)^b |L_0\rangle |1\rangle)_{AB} \\ &= (-1)^{s_3+s_4} E |\Upsilon(0, b)\rangle_{AB}. \end{aligned} \quad (28)$$

By measuring $S_3 S_4$, Bob obtains the sum of syndromes, or $s_3 + s_4$.

(3) By simultaneously solving the syndrome sums $s_3 + s_4, s_1 + s_3, s_1 + s_4$, Bob extracts the individual s_j 's, and thereby determines and corrects error E .

(4) He applies a controlled- S_F as in Eq. (23):

$$|\Upsilon(0, b)\rangle_{AB} \xrightarrow{\text{CNOT}} |L_0\rangle \frac{1}{\sqrt{2}} (|0\rangle + (-1)^b |1\rangle), \quad (29)$$

and determines b by measuring his qubit in the X basis.

(5) In order to make the cover message available, the *sublogical* Hadamard $\overline{H} = \frac{1}{\sqrt{2}} (S_1 + Z_4 Z_5)$ is applied to the code qubits, which effects the transformation

$$|L_0\rangle \xrightarrow{\overline{H}} \frac{1}{\sqrt{2}} (|L_0\rangle + |L_1\rangle) \equiv |0_L\rangle.$$

Note that $Z_4 Z_5$ is the sublogical Z operator, and any other flipping stabilizer could be used in place of S_1 .

VI. CONCLUSIONS AND DISCUSSIONS

Quantum steganography implements a quantum version of classical steganography, providing corresponding advantages in security, appearance of innocence, and capacity. To enforce innocence, quantum steganography typically uses pre-shared correlated bits or entanglement. In this article, we presented three steganographic protocols that apply this pre-shared resource in diverse ways: first, a scheme to optimize prior ebits by means of a catalytic QECC; second, a scheme that uses possibly degenerate EAQECCs in place of QECCs and pre-shared ebits; third, a scheme that uses the phase bit (instead of the parity bit à la Mihara [12]) of a pre-shared ebit, combined with QECCs.

We indicate a few possible future directions here. Quantum cryptography is typically a two-step process, involving establishing shared correlation first before secure transmission. On the other hand, the cryptography variant of quantum secure direct communication uses a one-step process of direct message transmission [29, 30]. In line with this, we may consider the question of design of a protocol for "direct steganography", where the innocent appearance can be produced without pre-shared ebits or bits. Furthermore, quantum cryptography and steganography typically require equal resources [7], and moreover stego messages can be embedded within a cryptogram [8]. This prompts the question of whether any cryptographic protocol can, with minimal additional resources, be turned into a stego protocol. Finally, one direction worth considering in terms of practical implementation in quantum steganography is whether the use of QECCs can be replaced by that of decoherence free subspace (DFS) [31] and continuous-variable codes such as Gottesman-Kitaev-Preskill (GKP) code [32].

ACKNOWLEDGMENTS

SD acknowledges the financial assistance of UGC NET scholarship and also Udupi Sri Admar Mutt Education Foundation. N.R.D. acknowledges financial support from the

Department of Science and Technology, Ministry of Science and Technology, India, through the INSPIRE fellowship. RS acknowledges partial financial support of the Indian Science & Engineering Research Board (SERB) grant CRG/2022/008345.

-
- [1] G. J. Simmons, in *Advances in Cryptology: Proceedings of Crypto 83* (Springer, 1984) pp. 51–67.
- [2] H. Dutta, R. K. Das, S. Nandi, and S. M. Prasanna, *IETE Technical Review* **37**, 632 (2020).
- [3] T. A. Brun, *Physical Review A* **99**, 032343 (2019).
- [4] R.-h. Shi, L.-s. Huang, W. Yang, and H. Zhong, *IEEE Transactions on Computers* **69**, 1805 (2020).
- [5] Z.-G. Qu, X.-B. Chen, X.-J. Zhou, X.-X. Niu, and Y.-X. Yang, *Optics Communications* **283**, 4782 (2010).
- [6] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, in *IOP conference series: materials science and engineering*, Vol. 518 (IOP Publishing, 2019) p. 052003.
- [7] B. Sanguinetti, G. Traverso, J. Lavoie, A. Martin, and H. Zbinden, *Physical Review A* **93**, 012336 (2016).
- [8] Z. Qu and I. B. Djordjevic, *IEEE Photonics Journal* **14**, 1 (2022).
- [9] J. Gea-Banacloche, *Journal of Mathematical Physics* **43**, 4531 (2002).
- [10] B. A. Shaw and T. A. Brun, *Physical Review A* **83**, 022310 (2011).
- [11] C. Sutherland and T. A. Brun, *Physical Review A* **100**, 052312 (2019).
- [12] T. Mihara, *Physics Letters A* **379**, 952 (2015).
- [13] Z. Qu, T. Zhu, J. Wang, and X. Wang, *Computers, Materials & Continua* **56** (2018).
- [14] A.-G. Tudorache, V. Manta, and S. Caraiman, *Advances in Electrical & Computer Engineering* **21** (2021).
- [15] N. Min-Allah, N. Nagy, M. Aljabri, M. Alkharraa, M. Alqah-tani, D. Alghamdi, R. Sabri, and R. Alshaikh, *Applied Sciences* **12**, 10294 (2022).
- [16] G. Luo, R.-G. Zhou, and W. Hu, *Quantum Information Processing* **22**, 138 (2023).
- [17] A. A. Abd El-Latif, B. Abd-El-Atty, S. Elseuofi, H. S. Khalifa, A. S. Alghamdi, K. Polat, and M. Amin, *Physica A: Statistical Mechanics and its Applications* **541**, 123687 (2020).
- [18] R. Joshi, A. Gupta, K. Thapliyal, R. Srikanth, and A. Pathak, *Quantum Information Processing* **21**, 164 (2022).
- [19] M. Nagy and N. Nagy, *Ieee Access* **8**, 213671 (2020).
- [20] T. Mihara, *Quantum Information Processing* **20**, 1 (2021).
- [21] J. Wang and Q. Zhang, in *Proceedings of the IEEE International Conference on Quantum Computing and Engineering (IEEE, 2021)* pp. 1–6.
- [22] M.-H. Hsieh, I. Devetak, and T. Brun, *Physical Review A—Atomic, Molecular, and Optical Physics* **76**, 062313 (2007).
- [23] F. R. F. Pereira and S. Mancini, *Entropy* **25**, 37 (2022).
- [24] D. A. Lidar and T. A. Brun, *Quantum error correction* (Cambridge university press, 2013).
- [25] T. Brun, I. Devetak, and M.-H. Hsieh, *science* **314**, 436 (2006).
- [26] T. A. Brun, I. Devetak, and M.-H. Hsieh, *IEEE Transactions on Information Theory* **60**, 3073 (2014).
- [27] G. Smith and J. A. Smolin, *Physical review letters* **98**, 030501 (2007).
- [28] S. J. Devitt, W. J. Munro, and K. Nemoto, *Reports on Progress in Physics* **76**, 076001 (2013).
- [29] A. Banerjee and A. Pathak, *Physics Letters A* **376**, 2944 (2012).
- [30] Y.-B. Sheng, L. Zhou, and G.-L. Long, *Science Bulletin* **67**, 367 (2022).
- [31] N. R. Dash, S. Dutta, R. Srikanth, and S. Banerjee, *Physical Review A* **109**, 062411 (2024).
- [32] A. L. Grimsmo and S. Puri, *PRX Quantum* **2**, 020101 (2021).