Secure multiparty quantum computation protocol for quantum circuits: The exploitation of triply even quantum error-correcting codes

Petr A. Mishchenko [*] and Keita Xagawa [†]
NTT Social Informatics Laboratories, Tokyo 180-8585, Japan

(Received 15 June 2022; revised 15 March 2024; accepted 19 March 2024; published 28 August 2024)

Secure multiparty quantum computation (MPQC) protocol is a cryptographic primitive allowing error-free distributed quantum computation to a group of n mutually distrustful quantum nodes even when some quantum nodes disobey the instructions of the protocol. Here we suggest a modified MPQC protocol that adopts unconventional quantum error-correcting codes and as a consequence reduces the number of qubits required for the protocol execution. In particular, the replacement of the self-dual Calderbank-Shor-Steane quantum error-correcting codes with triply even ones permits us to avoid the previously indispensable but resource-intensive procedure of the "magic-state" verification. Besides, since every extra qubit reduces the credibility of physical devices, our suggestion makes the MPQC protocol more accessible for the near-future technology by reducing the number of necessary qubits per quantum node from $n^2 + \Theta(r)n$, where r is the security parameter, to $n^2 + 3n$.

DOI: 10.1103/PhysRevA.110.022444

I. INTRODUCTION

As a well-established and widely used tool secure multiparty classical computation (MPCC) protocol allows n classical nodes to jointly compute some publicly known function $y = f(x^1, \ldots, x^n)$ on their private inputs $x^1, \ldots, x^n$ in a distributed manner [1]. During the execution of the MPCC protocol cheating classical nodes, dishonestly following the instructions of the protocol cannot affect the output of the computation y beyond choosing their inputs and cannot obtain any information on the inputs of the honest classical nodes beyond what they can infer from the output of the computation y. Since the MPCC protocol allows for distributed computation of any function f it becomes a powerful cryptographic primitive with many practical applications, e.g., secure electronic auction, secure electronic voting, and secure machine learning [2].

A later-developed more powerful quantum approach, secure multiparty quantum computation (MPQC) protocol allows n quantum nodes to jointly compute some publicly known quantum circuit $\mathcal{U}(\rho^1, \ldots, \rho^n)$ on their private inputs $\rho^1, \ldots, \rho^n$ [3]. In more detail, MPQC protocol can be described as a cryptographic primitive where each quantum node i inputs some quantum state ρ^i and then n quantum nodes jointly perform arbitrary quantum circuit $\mathcal{U}$ with n inputs and n outputs. Finally, each quantum node i obtains some output quantum state ω^i. See the schematic representation of the MPQC protocol in Fig. 1. Akin to its classical counterpart, the MPQC protocol satisfies the following informal requirements even in the presence of cheating quantum nodes:

(1) *Correctness and soundness.* Cheating quantum nodes cannot affect the outcome of the MPQC protocol beyond choosing their inputs.

(2) *Privacy.* Cheating quantum nodes can learn nothing about the private inputs and outputs of the honest quantum nodes beyond what they can infer from the output of the computation.

Currently existing MPQC protocols developed for the quantum circuit model of computation can be divided into two types: information-theoretically secure ones [3–7], meaning that there are no assumptions on the computational power of the cheating quantum nodes, and computationally secure ones [8–13]. The former type of the MPQC protocols is based on a technique of quantum error correction, which limits the maximum number of cheating quantum nodes to $t < n/4$, i.e., a constraint inherent to the Knill-Laflamme bound or the so-called quantum Singleton bound [14], while the latter type of the MPQC protocols is based on a technique of quantum authentication codes and can tolerate $t < n$ cheating quantum nodes.

In this paper, we consider the information-theoretically secure MPQC protocol which is based on a technique of quantum error correction. As a matter of fact, the technique of quantum error correction is tightly related to the concept of quantum secret sharing [15], the verifiable version of which was first suggested in Ref. [3], and became a prevalent tool for constructing the information-theoretically secure MPQC protocols. In particular, following the approach taken in Refs. [6,16] we utilize the verifiable hybrid secret sharing (VHSS) protocol suggested in Ref. [17], i.e., a modified version of the original verifiable quantum secret sharing protocol presented in Ref. [3]. The VHSS protocol is rather versatile and works for any type of the Calderbank-Shor-Steane (CSS) quantum error-correcting codes (QECCs) [18,19]. Therefore, at the beginning of the MPQC protocol, all the quantum nodes should agree on some CSS QECC with which they will remain until the end of the MPQC protocol.

At the highest level of abstraction, the MPQC protocol built upon a technique of quantum error correction and associated with it verifiable quantum secret sharing is executed in the

[*]Contact author: petr.mishchenko.us@hco.ntt.co.jp
[†]Contact author: keita.xagawa@tii.ae

following way: First of all, each quantum node i encodes and shares his single-qubit input quantum state ρ^i. In such a way, quantum nodes create a global logical quantum state shared among all the n quantum nodes, and as a consequence, each quantum node i holds a part of the global logical quantum state which we call a *share*. Next, quantum nodes jointly verify the encoding of each single-qubit input quantum state ρ^i using the VHSS protocol [17]. Then, quantum nodes locally perform quantum operations on their *shares* of the global logical quantum state to evaluate the logical version of the quantum circuit $\mathcal{U}$. Finally, each quantum node i collects all the *shares* corresponding to his output from the other quantum nodes and by decoding these *shares* reconstructs his single-qubit output quantum state ω^i. Note that at this level of abstraction, our MPQC protocol follows the procedure of the previously suggested MPQC protocol in Refs. [6,16].

To implement the universal quantum computation (UQC) in the above MPQC protocol, a particular universal set of quantum gates need to be chosen. In addition, these quantum gates need to be transversal for a CSS QECC that is chosen at the beginning of the MPQC protocol. Specifically, this means that the application of local quantum operations to each *share* should yield a meaningful logical operation on the global logical quantum state. However, it is known to be impossible to implement an entire universal set of quantum gates transversally not only for the CSS QECCs but for any QECC [20]. Actually, the solution to this problem lies in the extension of the transversal set of quantum gates with a nontransversal quantum gate, which can be implemented for example by the gate teleportation technique, i.e., with the help of transversal quantum gates, local measurements, classical communication, and ancillary quantum state [21].

In particular, the MPQC protocol suggested in Refs. [6,16] is based on a subclass of CSS QECCs, i.e., self-dual CSS QECCs [18,19] where the universal set of quantum gates is chosen to be the Clifford gates (H, P, and C-X gates) in combination with the T gate [22], see Appendix D for definitions of the quantum gates. Self-dual CSS QECCs allow trivial implementation of the transversal Clifford gates but require additional techniques for implementation of the nontransversal T gate. In case of the MPQC protocol originally suggested in Ref. [6] and later significantly reconsidered in Ref. [16] one requires two additional techniques: the gate teleportation technique and the verification of the "magic-state" technique, the latter of which is implemented by a statistical testing of the randomly selected magic states with their subsequent distillation.[1] Indeed, these additional techniques require an extra workspace for the implementation.

In this paper, we suggest an MPQC protocol constructed on the basis of triply even CSS QECCs [23,24], which constitute another subclass of general CSS QECCs [18,19]. In case of triply even CSS QECCs, we decide on another universal set of quantum gates, i.e., X, Z, T, C-X, and H gates [25], among which, triply even CSS QECCs allow transversal implementation of X, Z, T, and C-X gates but do not allow transversal implementation of the H gate [24]. Therefore, in our MPQC protocol, a nontransversal H gate is implemented by the gate teleportation technique, which has a lot of similarities with the implementation of the T gate in Refs. [6,16]. Nonetheless, the implementation of the nontransversal H gate by the gate teleportation technique does not require verification of the ancillary logical magic state, i.e., whether it is certainly the logical magic state, see Ref. [16] and Appendix C, since as an ancillary quantum state we need the logical "plus" state, i.e., a logical version of the single-qubit quantum state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Unlike the case of the logical magic-state verification, the logical plus state can be easily verified by using the VHSS protocol only. Therefore, by avoiding the verification of the ancillary logical magic state we can reduce the workspace required for the implementation of the MPQC protocol from $n^2 + \Theta(r)n$ qubits in case of the previous suggestion, see Ref. [16], to $n^2 + 3n$ qubits in our case, where n is the number of quantum nodes participating in the MPQC protocol and r is the security parameter.

This paper is organized as follows: In Sec. II, we briefly overview our MPQC protocol. Then, in Sec. III, we declare our assumptions and definitions necessary for the construction of the MPQC protocol. We describe our assumptions on communication channels in Sec. III A, and our assumptions on the properties of the adversary in Sec. III B. In Sec. III C, we define properties common to any type of CSS QECCs, and in Sec. III D, we discuss a subclass of general CSS QECCs called triply even CSS QECCs. Subsequently, in Sec. IV, we outline all the subroutines involved in the MPQC protocol: the VHSS protocol in Sec IV A and the gate teleportation protocol in Sec. IV B. After that, in Sec. V, we present a detailed outline of our MPQC protocol. Next, in Sec. VI, we prove the security of our MPQC protocol. In particular, we begin with stating the security framework as well as the security definition of our MPQC protocol in Sec. VI A, and then we find that the security proof of our MPQC protocol should be identical to the previously suggested MPQC protocol in Sec. VI B. Moreover, to be self-contained, we briefly present the security proof of our MPQC protocol in Secs. VI B 1 and VI B 2. Finally, Sec. VII is devoted to the summary.

II. SUMMARY OF THE MULTIPARTY QUANTUM COMPUTATION PROTOCOL

Here we briefly describe our MPQC protocol (see Table I). In a similar manner to Refs. [3,4,6,16], our MPQC protocol is based on a technique of quantum error correction, or to be more specific, on the concept of quantum secret sharing [15], and in particular utilizes the VHSS protocol suggested in Ref. [17] as its building block. The VHSS protocol works for any type of CSS QECCs encoding single-qubit quantum states into n-qubit logical quantum states, see Sec. IV A. Therefore, in our MPQC protocol the input quantum states $\rho^1, \ldots, \rho^n$ and the output quantum states $\omega^1, \ldots, \omega^n$ will indeed be single-qubit quantum states. In particular, our construction of the MPQC protocol relies on a subclass of general CSS QECCs [18,19], see Sec. III C, i.e., triply even CSS

[1] In the original version of the MPQC protocol the verification of the magic-state technique was implemented by the protocol called "verification of the Clifford stabilized states" (VCSS) which contained potential problems coming from the engagement of a nontransversal C-$XP^\dagger$ gate, see Appendixes A and B.

TABLE I. Summary of the MPQC protocol.

Input. Single-qubit quantum state ρ^i from each quantum node i, agreement on a particular $\mathcal{C}_{\rm TE}$, and a particular $\mathcal{U}$.
Output. In case of success, single-qubit quantum state ω^i in the possession of each quantum node i. In case of failure, i.e., excess in the number of cheating quantum nodes, the MPQC protocol is aborted at the end of the computation.

1. *Sharing.* By encoding and sharing each of the inputs $\rho^1, \ldots, \rho^n$ *twice*, quantum nodes create a global logical quantum state $\bar{\bar{\mathcal{P}}}$ where each quantum node i holds a share $\bar{\bar{\mathcal{P}}}_i$. For the details see Sec. IV A.
2. *Verification.* All the quantum nodes jointly verify the encoding of each input ρ^i with the help of the VHSS protocol to check whether each quantum node i is honest. For the details see Sec. IV A.
3. *Computation.* Depending on whether the quantum gate appearing in $\mathcal{U}$ can be implemented transversally or not, or whether the implementation of the $\mathcal{U}$ requires an ancillary quantum state, quantum nodes behave in the following three ways:
   (a) In case of the transversal quantum gates, i.e., X, Z, T, or C-X gates, each quantum node i locally applies corresponding quantum operations to his share $\bar{\bar{\mathcal{P}}}_i$.
   (b) In case of the non-transversal H^i gate applied to the quantum wire i of the $\mathcal{U}$, quantum nodes jointly prepare verified by the VHSS protocol ancillary logical quantum state $|\bar{\bar{+}}\rangle^i$ created from the single-qubit quantum state $|+\rangle^i$, and then perform the gate teleportation technique. For the details see Sec. IV B.
   (c) In case the implementation of the $\mathcal{U}$ requires an ancillary quantum state, quantum nodes jointly prepare verified by the VHSS protocol ancillary logical quantum state $|\bar{\bar{0}}\rangle^i$ created from the single-qubit quantum state $|0\rangle^i$.
4. *Reconstruction.* Each quantum node i collects all the single-qubit quantum states corresponding to his output and by decoding in such a way obtained output logical quantum state $\bar{\bar{\Omega}}^i$ *twice*, reconstructs his output ω^i. For the details see Sec. IV A.

QECCs $\mathcal{C}_{\rm TE}$ [23,24], see Sec. III D. In fact, triply even CSS QECCs $\mathcal{C}_{\rm TE}$ allow transversal implementation of X, Z, T, and C-X gates but not allow transversal implementation of the H gate. To implement the nontransversal H gate we utilize the gate teleportation technique as will be explained below, see Sec. IVB.

At the beginning of the MPQC protocol, quantum nodes should agree on a particular triply even CSS QECC $\mathcal{C}_{\rm TE}$ described above and then create global logical quantum state $\bar{\bar{\mathcal{P}}}$ by encoding and sharing each of the inputs $\rho^1, \ldots, \rho^n$ *twice*, see Fig. 2. Hereafter, the double bar always means that the quantum state is encoded *twice*. As a result, each quantum node i holds a part of the global logical quantum state $\bar{\bar{\mathcal{P}}}$, i.e., a share denoted $\bar{\bar{\mathcal{P}}}_i$. Next, to check whether each quantum node i is honest, quantum nodes jointly verify the encoding of each input ρ^i by using the VHSS protocol [17], see Sec. IV A. After that, quantum nodes jointly evaluate logical quantum circuit $\bar{\bar{\mathcal{U}}}$, i.e., a *twice* encoded version of the quantum circuit $\mathcal{U}$, see Sec. V. Here, in the case of the transversal quantum gates, each quantum node i locally performs necessary quantum operations on his share $\bar{\bar{\mathcal{P}}}_i$. On the other hand, in the case of nontransversal quantum gates, quantum nodes jointly perform the gate teleportation technique, see Sec. IV B. In addition, if the implementation of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$ requires an ancillary quantum state, quantum nodes jointly create the ancillary logical quantum state $|\bar{\bar{0}}\rangle^i$ by encoding and sharing a single-qubit quantum state $|0\rangle^i$ *twice*. Finally, each quantum node i collects all the single-qubit quantum states corresponding to his output from the other quantum nodes and by decoding in such a way obtained output logical quantum state $\bar{\bar{\Omega}}^i$ *twice*, eventually reconstructs his output ω^i, see Sec. IV A. Also, during the execution of the MPQC protocol quantum nodes publicly record the positions of the cheating quantum nodes to decide whether to abort the MPQC protocol. In particular, information on the positions of the cheating quantum nodes is updated each time the VHSS protocol or the gate teleportation protocol is invoked.

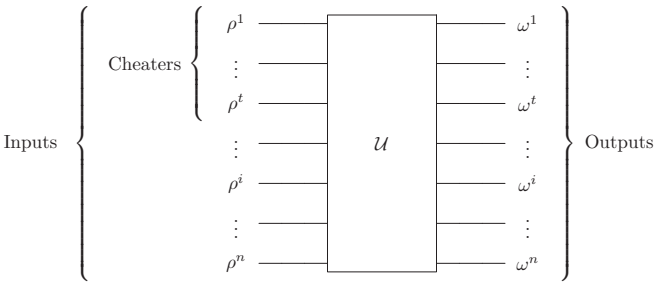

FIG. 1. Schematic picture of the MPQC protocol for the quantum circuit model of computation. At the beginning of the MPQC protocol, each quantum node i provides an input quantum state ρ^i. Then, n quantum nodes jointly perform quantum circuit $\mathcal{U}$ with n inputs and n outputs. At the end of the MPQC protocol, each quantum node i receives an output quantum state ω^i. The purpose of the MPQC protocol is to implement quantum circuit $\mathcal{U}$ in such a way that requirements of *correctness*, *soundness*, and *privacy* are satisfied even in the presence of $t < n/4$ cheating quantum nodes.

In short, the gate teleportation technique implementing a nontransversal H^i gate, where superscript i means that the quantum gate is applied to the quantum wire i of the quantum circuit $\mathcal{U}$, is performed as follows: Suppose quantum nodes want to apply a nontransversal $\bar{\bar{H}}^i$ gate, i.e., a logical version of the nontransversal H^i gate, applied to the part of the global logical quantum state $\bar{\bar{\mathcal{P}}}$ initially created from the single-qubit input quantum state ρ^i and denoted $\bar{\bar{\mathcal{P}}}^i$. Quantum nodes jointly prepare verified by the VHSS protocol ancillary logical quantum state $|\bar{\bar{+}}\rangle^i$ created from a single-qubit quantum state $|+\rangle^i$. Then, with the help of transversal quantum gates, local measurements, and classical communication, quantum nodes apply the nontransversal $\bar{\bar{H}}^i$ gate to the logical quantum state

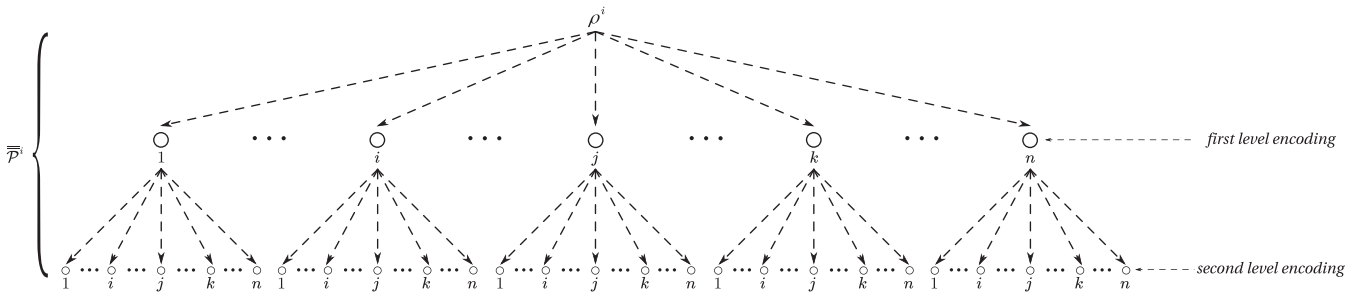

FIG. 2. Schematic picture of the sharing phase of the VHSS protocol during which a single-qubit input quantum state ρ^i from the dealer D^i undergoes the *first level encoding* and the *second level encoding* and eventually the global logical quantum state $\bar{\bar{\mathcal{P}}}^i$ is created. Each circle represents a single-qubit quantum state.

$\bar{\bar{\mathcal{P}}}^i$, or in other words, achieve the realization of the logical quantum state $\bar{\bar{H}}^i\bar{\bar{\mathcal{P}}}^i\bar{\bar{H}}^i$. During the gate teleportation protocol information on the positions of the cheating quantum nodes is updated, see Sec. IV B for the details.

We note that our MPQC protocol is information-theoretically secure, i.e., we make no assumptions on the computational power of the nonadaptive active adversary, see Sec. III B, but has an exponentially small probability of error inherited from the VHSS protocol, i.e., $\kappa 2^{-\Omega(r)}$, where r is the security parameter and $\kappa = n + \mathrm{No}_{\mathrm{ancillas}} + \mathrm{No}_H$, with $\mathrm{No}_{\mathrm{ancillas}}$ standing for the number of ancillary quantum states required for the implementation of the quantum circuit $\mathcal{U}$ and No_H standing for the number of the H gates.[2] Also, the aforementioned adversary in our MPQC protocol is limited only by the number of quantum nodes $t < n/4$ it can corrupt, see Sec. III B, which is a limitation derived from the Knill-Laflamme bound or the quantum Singleton bound [14], see Ref. [4] for the details. To be more specific, the number of corrupted quantum nodes is constrained by the distance d of the triply even CSS QECC $\mathcal{C}_{\mathrm{TE}}$ as $t \leqslant \lfloor \frac{d-1}{2} \rfloor$, see Sec. III C. This constraint allows honest quantum nodes to correct all the arbitrary quantum errors introduced by the $t < n/4$ cheating quantum nodes. Consequently, our MPQC protocol satisfies the security requirements, i.e., *correctness*, *soundness*, and *privacy*, which indeed hold with the probability exponentially close to 1 in the security parameter r, see Sec. VI. Important to note that we allow our MPQC protocol to abort at the end of computation if honest quantum nodes detect too many cheating quantum nodes during the execution of the protocol, in a similar manner to Refs. [6,16].

During the execution of the MPQC protocol, in addition to the n^2 single-qubit quantum states required for holding a share $\bar{\bar{\mathcal{P}}}_i$, each quantum node i uses $2n$ single-qubit ancillary quantum states to verify the encodings of the inputs $\rho^1, \ldots, \rho^n$ by the VHSS protocol, see Sec. IV A, and $3n$ single-qubit ancillary quantum states to apply a nontransversal H gate with the gate teleportation technique involving verification of the ancillary logical quantum state $|\bar{\bar{+}}\rangle^i$, see Sec. IV B, or to verify the ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ which may be required for the implementation of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$. Thus, in total each quantum node requires $n^2 + 3n$ qubits for the implementation of the MPQC protocol. Finally, since the communication complexity of the VHSS protocol per quantum node is $O(nr^2)$ qubits, see Sec. IV A, the communication complexity of our MPQC protocol per quantum node will be $O((n + \mathrm{No}_{\mathrm{ancillas}} + \mathrm{No}_H)nr^2)$ qubits, see Sec. V, which is proportional to the total number of the VHSS protocol executions during the MPQC protocol.

III. ASSUMPTIONS AND DEFINITIONS

In this section, we overview our assumptions and definitions necessary for the construction of the MPQC protocol. In Sec. III A, we describe our assumptions on the classical and quantum communication channels as well as on the broadcast channel, and in Sec. III B, we describe our assumptions on the adversary. Next, in Sec. III C, we define properties common to any type of CSS QECCs, and finally, in Sec. III D, we discuss a subclass of CSS QECCs, i.e., triply even CSS QECCs.

A. Communication channels

In our MPQC protocol, we assume that all the quantum nodes have an access to the classical authenticated broadcast channel [26] (which is feasible if and only if $t < n/3$ [27,28]) and to the public source of randomness, the latter of which can be created with the help of the secure multiparty classical computation [29,30] (which is also feasible if and only if $t < n/3$).[3] Also, each pair of quantum nodes is connected via the authenticated and private classical [31] and quantum [32] channels. Finally, we assume that each quantum node can perfectly process and store classical and quantum information.

[2]Namely, κ is equal to the number of times the VHSS protocol is invoked during the execution of the MPQC protocol.

[3]We note that aforementioned constraints on the feasibility of the classical authenticated broadcast channel and the public source of randomness do not cause any additional problems since we assume that only $t < n/4$ ($< n/3$) quantum nodes are corrupted by the adversary, see Sec. III B.

B. Adversary

In our MPQC protocol, we make no assumptions about the computational power of the adversary. Our nonadaptive,[4] but active[5] adversary is limited only by the number of quantum nodes $t < n/4$ it can corrupt. The quantum nodes which are corrupted by the adversary and therefore disobey the instructions of the MPQC protocol are called cheating quantum nodes. On the contrary, the quantum nodes which are not corrupted by the adversary and obey the instructions of the MPQC protocol are called honest quantum nodes.

C. Calderbank-Shor-Steane quantum error-correcting codes

Since in our MPQC protocol we consider a subclass of general CSS QECCs [18,19], i.e., triply even CSS QECCs $\mathcal{C}_{\text{TE}}$ [23,24], we first define properties common to any type of CSS QECCs. Hereinafter, $[n, k, d]$ stands for the distance d binary classical linear code that encodes k bits into n bits. General CSS QECC is defined through the two binary classical linear codes denoted as V and W, and these binary classical linear codes satisfy the following three conditions:

(1) V is an $[n, k_V, d_V]$ binary classical linear code that can correct $t_V \leqslant \lfloor \frac{d_V-1}{2} \rfloor$ bit errors.

(2) W is an $[n, k_W, d_W]$ binary classical linear code that can correct $t_W \leqslant \lfloor \frac{d_W-1}{2} \rfloor$ bit errors.

(3) $V^\perp$ and W satisfy $V^\perp \subseteq W$, where $V^\perp$ means the dual of the binary classical linear code V. Here, $V^\perp$ is an $[n, k_{V^\perp}, d_{V^\perp}]$ classical linear code that satisfies $k_{V^\perp} = n - k_V$.

These two binary classical linear codes generate an $[[n, k, d]]$ CSS QECC encoding k-qubit quantum state into n-qubit logical quantum state, and where the constraint $k = k_V + k_W - n$ is satisfied. Such a CSS QECC can correct t_V bit flip X errors and t_W phase flip Z errors, which leads to a CSS QECC with distance $d \geqslant \min(d_V, d_W)$ tolerating $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary quantum errors and $p \leqslant d - 1$ erasure quantum errors.

Since the VHSS protocol we employ in this paper works for any type of CSS QECCs encoding single-qubit quantum state into an n-qubit logical quantum state, see Sec. IV A, k will always be equal to 1, and therefore the encodings of the standard basis "zero" state and the Fourier basis plus state can be written as $|\bar{0}\rangle = \frac{1}{\sqrt{W^\perp}} \sum_{w \in W^\perp} |w\rangle$ and $|\bar{+}\rangle = \frac{1}{\sqrt{V}} \sum_{v \in V} |v\rangle$, correspondingly. Here individual codewords of the binary classical linear codes V and W are denoted as v and w, respectively.

Important to note that a CSS QECC generated by the two binary classical linear codes V and W may be denoted as a set $V \cap \mathcal{F}W$ (where $\mathcal{F}$ stands for the Fourier transform), which means that a CSS QECC is a set of n-qubit logical quantum states, which yield a codeword v in V when measured in the standard basis (also called Z basis in the literature) and a codeword w in W when measured in the Fourier basis (also called X basis in the literature) [33].

Also, we emphasize that any type of CSS QECC allows transversal implementation of the C-X gate, while not any type of CSS QECC allows transversal implementation of the other well-known quantum gates such as an H, P, or T gates. For example, a subclass of general CSS QECCs constructed from the two binary classical linear codes satisfying $V = W$ and called self-dual CSS QECCs [34], allows transversal implementation of H, P, and C-X gates but does not allow transversal implementation of the T gate. Besides, we should note that, in the case of CSS QECCs, logical measurement can be implemented transversally by local measurements of all the single-qubit quantum states comprising the n-qubit logical quantum state and the classical communication.

Finally, let us mention the important property of CSS QECCs. The set of stabilizer generators S of any CSS QECC can be divided into the set of stabilizer generators consisting of only X and I (in this case, each stabilizer generator is denoted as S_g^X and the entire set is denoted as S^X) or only Z and I (in this case, each stabilizer generator is denoted as S_g^Z and the entire set is denoted as S^Z) operators in the tensor product representation, which permits independent correction of the bit flip X and the phase flip Z errors. As it happens, the Steane-type quantum error-correction method [35] on the basis of which the VHSS protocol is built, takes advantage of this fact [17], see Sec. IV A for the details. Furthermore, the encoding of the standard basis zero state and the Fourier basis plus state in terms of the stabilizer generators can be written as $|\bar{0}\rangle = \frac{1}{\sqrt{2^{|S^X|}}} \prod_{g \in S^X} (I + S_g^X) |0\rangle^{\otimes n}$ and $|\bar{+}\rangle = \frac{1}{\sqrt{2^{|S^Z|}}} \prod_{g \in S^Z} (I + S_g^Z) |+\rangle^{\otimes n}$, correspondingly.

D. Triply even Calderbank-Shor-Steane quantum error-correcting codes

To be comprehensive, we briefly describe a method of constructing the triply even CSS QECCs $\mathcal{C}_{\text{TE}}$ [23,24], which constitute a subclass of general CSS QECCs [18,19] and allow transversal implementation of the T gate without any Clifford corrections [36]. This is in contrast with the so-called triorthogonal CSS QECCs, which constitute an another subclass of general CSS QECCs and a superclass for the triply even CSS QECCs $\mathcal{C}_{\text{TE}}$, and for which the transversal implementation of the T gate requires additional Clifford corrections [37]. We begin with the definition of the triply even binary matrices [23] from which the triply even CSS QECCs $\mathcal{C}_{\text{TE}}$ can be constructed [38]. Suppose the existence of two binary vectors $f, g \in \{0, 1\}^n$ with the Hamming weights $|f|$ and $|g|$, respectively, and for which the entry-wise product $f \cdot g \in \{0, 1\}^n$ is defined. In this case, we call an $m \times n$ binary matrix G triorthogonal if for its rows $f_1, \ldots f_m \in \{0, 1\}^n$ the following two conditions are satisfied:

$$|f_i \cdot f_j \cdot f_k| = 0 \pmod 2 \tag{1}$$

for all triples of rows $1 \leqslant i < j < k \leqslant m$,

$$|f_i \cdot f_j| = 0 \pmod 2 \tag{2}$$

[4]"Nonadaptive" is the adversary that chooses quantum nodes to corrupt before the MPQC protocol begins and remains with that choice.

[5]"Active" is the adversary that is able to perform arbitrary quantum operations on the shares in the possession of the corrupted quantum nodes.

for all pairs of rows $1 \leqslant i < j \leqslant m$. If in addition to the above two conditions the more restrictive constraint

$$|f_i \cdot f_j| = 0 \pmod 4 \tag{3}$$

is satisfied for all pairs of even weight rows $1 \leqslant i < j \leqslant l$, we call the binary matrix G triply even. The latter constraint implies that $|f_i| = 0 \pmod 8$ is satisfied for all the even-weight rows of the binary matrix G [38]. It is important to note that we assume the $m \times n$ binary matrix G consisting of two submatrices: the one comprised of l even weight rows and denoted as G_e (an $l \times n$ matrix) and the one comprised of $m - l$ odd weight rows and denoted as G_o (an $m - l \times n$ matrix).

With the above triply even binary matrix G at hand, one can construct the corresponding triply even CSS QECC $\mathcal{C}_{\rm TE}$ as follows [37,38]: For each row of the binary matrix G_e, one defines an X stabilizer generator by mapping nonzero entries of the row to the X operators (and zero entries of the row to the I operators). Next, for each row of the orthogonal complement of the triply even binary matrix G, i.e., $G^{\perp}$, one defines a Z stabilizer generator by mapping nonzero entries of the row to the Z operators (and zero entries of the row to the I operators). Finally, each row of the binary matrix G_o corresponds to both the $\bar{X}$ and $\bar{Z}$ operators, if nonzero entries of the rows are mapped to the X and Z operators respectively (and zero entries of the rows to the I operators in both cases).

Let us also mention the minimum distance of the triply even CSS QECCs $\mathcal{C}_{\rm TE}$ constructed above. If we denote the linear span of all the rows of the binary matrices G_e ($G_e^{\perp}$) and $G^{\perp}$ as $\mathcal{G}_e$ ($\mathcal{G}_e^{\perp}$) and $\mathcal{G}^{\perp}$, respectively, in the case of the triorthogonal CSS QECCs, and consequently the triply even CSS QECCs $\mathcal{C}_{\rm TE}$, the condition $\mathcal{G}_e \subseteq \mathcal{G}^{\perp}$ is satisfied and this fact will automatically imply the relation $d_Z \leqslant d_X$, where d_Z and d_X mean the distances against the phase flip Z and bit flip X errors, respectively [37,38]. Therefore, the minimum distance of the triply even CSS QECC $\mathcal{C}_{\rm TE}$ can be defined as the minimum weight of any nontrivial $\bar{Z}$ operator: $d = \min_{f \in \mathcal{G}_e^{\perp} \setminus \mathcal{G}^{\perp}} |f|$ [37,39].

Eventually, to introduce an essential property of the triply even CSS QECCs $\mathcal{C}_{\rm TE}$, i.e., a transversal implementation of the T gate without any Clifford corrections, we define the weight $|S|$ of a stabilizer generator S as the number of terms not equal to I in the tensor product representation. Actually, according to the Ref. [36], a CSS QECC allows transversal implementation of the T gate without any Clifford corrections if and only if the binary matrix G is triorthogonal, i.e., Eqs. (1) and (2) are satisfied, and the weight of all the stabilizer generators S^X is a multiple of eight: $|S^X| = 0 \pmod 8$.[6] An example of such a CSS QECC is [[15, 1, 3]] CSS QECC [24], as well as [[49, 1, 5]] CSS QECC [37].

As we can see from the above discussions, triply even CSS QECCs $\mathcal{C}_{\rm TE}$ allow transversal implementation of X, Z, and C-X gates (since any type of CSS QECC allows transversal implementation of these quantum gates), and T gate. Therefore, only the H gate in the chosen universal set of quantum gates (X, Z, C-X, T, and H gates) is not transversal and needs to be implemented by the gate teleportation technique, see Sec. IV B, since in case of the triply even CSS QECCs $\mathcal{C}_{\rm TE}$ binary classical linear codes V and W do not satisfy $V = W$.

[6]This statement is indeed consistent with the claim that the condition $|f_i| = 0 \pmod 8$ is satisfied for all the even-weight rows $1 \leqslant i \leqslant l$ of the triply even binary matrix G.

IV. SUBROUTINES OF THE MULTIPARTY QUANTUM COMPUTATION PROTOCOL

In this section, we describe subroutines used as building blocks in the construction of the MPQC protocol. In Sec. IV A, we review the VHSS protocol used during the *sharing*, *verification*, and *reconstruction* phases of the MPQC protocol, and in Sec. IV B, we outline the gate teleportation technique necessary for the implementation of the H gate, which is nontransversal in the case of triply even CSS QECCs used in our construction of the MPQC protocol.

A. Outline of the verifiable hybrid secret sharing protocol

An important ingredient required for the construction of our MPQC protocol based on a technique of quantum error correction is the VHSS protocol, which was recently introduced in Ref. [17]. First of all, quantum nodes participating in the MPQC protocol use the VHSS protocol to encode and share a single-qubit input quantum state ρ^i among all the n quantum nodes in a verifiable way. We note that the VHSS protocol in Ref. [17] is applicable to any type of CSS QECC and that if the minimum distance of the underlying CSS QECC is d, the VHSS protocol tolerates $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ cheating quantum nodes corrupted by the adversary described in Sec. III B. As already mentioned in Sec. II, this constraint indeed allows honest quantum nodes to correct all the arbitrary quantum errors introduced by the $t < n/4$ cheating quantum nodes. To be more specific, the VHSS protocol is information-theoretically secure and satisfies the security requirements, i.e., *soundness*, *completeness*, and *secrecy*, which hold with the probability exponentially close to 1 in the security parameter r. Namely, the verification performed by using the VHSS protocol has the probability of error $2^{-\Omega(r)}$. The detailed security proof can be found in Ref. [17].

First, let us describe the VHSS protocol itself (see Table II). In the sharing phase of the VHSS protocol, some quantum node i acting as a dealer D^i encodes his input ρ^i into the n-qubit logical quantum state by using some CSS QECC (some triply even CSS QECC $\mathcal{C}_{\rm TE}$ in our case) on which all the quantum nodes have an agreement and shares it among all the quantum nodes (including himself). We call this procedure the *first level encoding*. Then, each quantum node i one more time encodes a single-qubit quantum state obtained from the dealer D^i into the n-qubit logical quantum state by using the same CSS QECC (the same triply even CSS QECC $\mathcal{C}_{\rm TE}$ in our case) and one more time shares it among all the quantum nodes (including himself). We call this procedure the *second level encoding*. In such a way, quantum nodes create n branches of the *second level encoding*. Eventually, quantum nodes jointly possess logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (or global logical quantum state $\bar{\bar{\mathcal{P}}}$ if all the n quantum nodes participating in the MPQC protocol have finished the sharing phase of the VHSS protocol), see Fig. 2.

In the verification phase of the VHSS protocol, quantum nodes jointly verify that the quantum state $\bar{\bar{\mathcal{P}}}^i$ in their possession is for sure a valid logical quantum state encoded by

TABLE II. Outline of VHSS protocol.

Input. Private single-qubit quantum state ρ^i (or $|0\rangle^i$, $|+\rangle^i$) from the dealer D^i and an agreement on a particular $\mathcal{C}_{\text{TE}}$.
Output. At the end of the verification phase, each quantum node $j = 1, \ldots, n$ holds a share $\bar{\bar{\mathcal{P}}}_j^i$ (or ${}_v|\bar{\bar{0}}\rangle_j^i$, ${}_v|\bar{\bar{+}}\rangle_j^i$) of the jointly verified logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (or ${}_v|\bar{\bar{0}}\rangle^i$, ${}_v|\bar{\bar{+}}\rangle^i$) (and if required, quantum nodes are also able to confirm that what they hold is definitely a logical quantum state ${}_v|\bar{\bar{0}}\rangle^i$, ${}_v|\bar{\bar{+}}\rangle^i$) and a public set B.

1. *Sharing.* Quantum nodes jointly create logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (or ${}_v|\bar{\bar{0}}\rangle^i$, ${}_v|\bar{\bar{+}}\rangle^i$) by encoding and sharing input ρ^i (or $|0\rangle^i$, $|+\rangle^i$) among all the n quantum nodes. At the end of the sharing phase, each quantum node holds n single-qubit quantum states coming from every other quantum node.
   (a) Dealer D^i encodes his input ρ^i (or $|0\rangle^i$, $|+\rangle^i$) into the n-qubit logical quantum state by using $\mathcal{C}_{\text{TE}}$ and shares it among all the quantum nodes (including himself). We call this procedure the *first level encoding*.
   (b) Then, each quantum node $j = 1, \ldots, n$ one more time encodes a single-qubit quantum state obtained from the dealer D^i into the n-qubit logical quantum state by using $\mathcal{C}_{\text{TE}}$ and shares it among all the quantum nodes (including himself). We call this procedure the *second level encoding*.
2. *Verification.* Quantum nodes jointly verify that the input ρ^i (or $|0\rangle^i$, $|+\rangle^i$) from the dealer D^i is properly encoded and shared, and the valid logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (or ${}_v|\bar{\bar{0}}\rangle^i$, ${}_v|\bar{\bar{+}}\rangle^i$) is created. Let us call this procedure the *verification of* ρ^i. Also, if required, quantum nodes jointly confirm that the input from the dealer D^i is exactly $|0\rangle^i$ ($|+\rangle^i$). Let us call this procedure the *confirmation of* $|0\rangle^i$ ($|+\rangle^i$).
   (a) *Verification of* ρ^i. Quantum nodes create ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ and $|\bar{\bar{+}}\rangle^i$ with the same method as they created logical quantum state $\bar{\bar{\mathcal{P}}}^i$ in the sharing phase, propagate arbitrary quantum errors (if any) in the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ to these ancillary logical quantum states, logically measure them in the appropriate basis, and decode the results of these logical measurements to find arbitrary quantum errors in the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (if any).
   (b) *Confirmation of* $|0\rangle^i$ ($|+\rangle^i$). Quantum nodes create ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ ($|\bar{\bar{+}}\rangle^i$) with the same method as they created logical quantum state $\bar{\bar{\mathcal{P}}}^i$ in the sharing phase, propagate arbitrary quantum errors (if any) in the logical quantum state ${}_v|\bar{\bar{0}}\rangle^i$ (${}_v|\bar{\bar{+}}\rangle^i$) to these ancillary logical quantum states, and logically measure them in the standard (Fourier) basis. Finally, quantum nodes decode the results of the logical measurements and publicly check whether they correspond to the $|0\rangle^i$ ($|+\rangle^i$).
   (c) During the verification phase, quantum nodes jointly construct a public set B, which records all the arbitrary quantum errors introduced by the dealer D^i and by the cheating quantum nodes.
   (d) If at the end of the verification phase $|B| \leqslant t$ is satisfied, the dealer D^i passes the verification phase, and the VHSS protocol continues to the reconstruction phase. On the other hand, if $|B| > t$ is satisfied the VHSS protocol aborts.
3. *Reconstruction.* Reconstructor R^j performs the following quantum operations on the single-qubit quantum states collected from the other quantum nodes and at the end of the reconstruction phase obtains output $\omega^j = \rho^i$.
   (a) Reconstructor R^j identifies all the arbitrary quantum errors in each n-qubit logical quantum state originally encoded and shared by the quantum node $k \notin B$, by using $\mathcal{C}_{\text{TE}}$. After that, the reconstructor R^j decodes all the n-qubit logical quantum states with $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary quantum errors. This is the *second level decoding*. Otherwise, the reconstructor R^j adds quantum node k to the public set B.
   (b) From the single-qubit quantum states obtained during the *second level decoding*, the reconstructor R^j randomly chooses $n - 2t$ single-qubit quantum states, each originally encoded and shared by the quantum node $k \notin B$, performs erasure recovery by using $\mathcal{C}_{\text{TE}}$ and by decoding obtains output $\omega^j = \rho^i$. This is the *first level decoding*.

the aforementioned triply even CSS QECC $\mathcal{C}_{\text{TE}}$. To be more specific, quantum nodes publicly check that there are $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary quantum errors at the stage of the *first level encoding*, which will also mean that the dealer D^i is honest. For that purpose, first, quantum nodes jointly prepare ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ (to detect the phase flip Z errors) or $|\bar{\bar{+}}\rangle^i$ (to detect the bit flip X errors), which are generated in the same way as the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ but from the single-qubit input quantum states $|0\rangle^i$ or $|+\rangle^i$, respectively. Then, quantum nodes propagate arbitrary quantum errors in the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (if any) to these ancillary logical quantum states by means of the transversal application of the $\overline{\overline{\text{C-}X}}^i$ gate (superscript i means that the logical quantum gate is applied between the logical quantum states initially created from the single-qubit input quantum states ρ^i, $|0\rangle^i$, or $|+\rangle^i$) to their shares. Next, quantum nodes logically measure the ancillary logical quantum states in the appropriate basis, and, finally, by decoding the results of these logical measurements find arbitrary quantum errors in the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ (if any). The detailed procedure of the bit flip X errors detection is shown in Fig. 3.

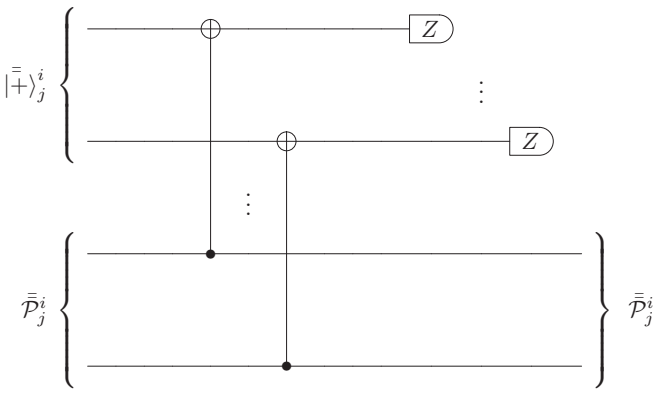

FIG. 3. Fragment of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$ in which quantum node j propagates arbitrary quantum errors in the share $\bar{\bar{\mathcal{P}}}_j^i$ (if any) to the ancillary share $|\bar{\bar{+}}\rangle_j^i$ to detect the bit flip X errors. Note that the logical quantum gates and the logical measurement presented in the fragment of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$ can be implemented transversally in the case of CSS QECCs.

Actually, the above procedure is an extension of the Steane-type quantum error-correction method introduced in Ref. [35] and stands for a single iteration in the verification phase of the VHSS protocol which contains $r^2 + 2r$ such iterations. To be more specific, there are r iterations to check the bit flip X errors (where each iteration spends single ancillary logical quantum state $|\bar{\bar{+}}\rangle^i$), r iterations to check the phase flip Z errors (where each iteration spends single ancillary logical quantum state $|\bar{\bar{0}}\rangle^i$), and r additional iterations for each ancillary logical quantum state $|\bar{\bar{0}}\rangle^i$ to check it for the bit flip X errors (where each iteration indeed spends single ancillary logical quantum state $|\bar{\bar{+}}\rangle^i$). Obviously, this procedure requires a workspace of $3n$ qubits per quantum node, i.e., a workspace of n qubits per quantum node for each of the logical quantum states $\bar{\bar{\mathcal{P}}}^i$, $|\bar{\bar{0}}\rangle^i$, and $|\bar{\bar{+}}\rangle^i$, which need to be stored simultaneously during the verification phase of the VHSS protocol, see Ref. [17] for the details.

Throughout the verification phase of the VHSS protocol, quantum nodes jointly construct a public set of apparent cheaters B, which records all the arbitrary quantum errors introduced by the dealer D^i during the procedure of the *first level encoding* and by the cheating quantum nodes during the procedure of the *second level encoding*. This allows identification of the cheating quantum nodes with probability exponentially close to 1 in the security parameter r, i.e., the probability of error is $2^{-\Omega(r)}$. Note that it is impossible to distinguish arbitrary quantum errors introduced by the dealer D^i from those introduced by the cheating quantum nodes. Anyway, if at the end of the verification phase $|B| \leqslant t$ is satisfied, i.e., there are $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary quantum errors at the stage of the *first level encoding*, then the dealer D^i passes the verification phase of the VHSS protocol. In this case, a logical quantum state $\bar{\bar{\mathcal{P}}}^i$ in the possession of the quantum nodes can always be reconstructed into the original input ρ^i because arbitrary quantum errors introduced during the *first level encoding* and the *second level encoding* can always be corrected by the triply even CSS QECC $\mathcal{C}_{\mathrm{TE}}$, since we assume that there are $t < n/4$ cheating quantum nodes and therefore $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary quantum errors can be introduced to each branch of the *second level encoding*. On the other hand, if $|B| > t$ is satisfied the VHSS protocol aborts.

In the reconstruction phase of the VHSS protocol, some quantum node j acting as a reconstructor R^j collects all the single-qubit quantum states from all the quantum nodes. Then, to correct arbitrary quantum errors introduced to the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ by the cheating quantum nodes after the verification phase and before the reconstruction phase, i.e., at the *second level encoding*, the reconstructor R^j identifies arbitrary quantum errors in the n-qubit logical quantum states (or in other words, in the branches of the *second level encoding*) coming from the quantum nodes not in the public set of apparent cheaters B by using the triply even CSS QECC $\mathcal{C}_{\mathrm{TE}}$ and subsequently updates a public set of apparent cheaters B. Next, the reconstructor R^j decodes all the n-qubit logical quantum states in his possession that may contain $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary quantum errors. We call this procedure the *second level decoding*. After that, from the single-qubit quantum states obtained during the *second level decoding*, the reconstructor R^j randomly chooses $n - 2t$ single-qubit quantum states[7] originally encoded and shared by the quantum nodes which are not in the public set of apparent cheaters B, performs erasure recovery by using the triply even CSS QECC $\mathcal{C}_{\mathrm{TE}}$, and finally obtains single-qubit output quantum state $\omega^j = \rho^i$. We note that the communication complexity of the VHSS protocol per quantum node becomes $O(nr^2)$ qubits, which is obvious considering that the quantum nodes send $n^2 - 1$ single qubit quantum states $(r + 1)^2$ times in the process of the VHSS protocol execution [17].

Actually, the VHSS protocol in Ref. [17] is also able to confirm that the single-qubit input quantum state from the dealer D^i is exactly $|0\rangle^i$ (or $|+\rangle^i$), i.e., that the quantum state ${}_v|\bar{\bar{0}}\rangle^i$ (${}_v|\bar{\bar{+}}\rangle^i$) (left subscript v denotes the logical quantum state which the quantum nodes want to verify and confirm, and is used to distinguish it from the ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ or $|\bar{\bar{+}}\rangle^i$ which are spent in the verification phase of the VHSS protocol) in the possession of the quantum nodes is for sure a valid logical quantum state created from the input $|0\rangle^i$ (or $|+\rangle^i$) and encoded by the triply even CSS QECC $\mathcal{C}_{\mathrm{TE}}$, see Refs. [3,4,17] for the details. To achieve that, all the $r^2 + 2r$ iterations in the verification phase of the VHSS protocol are performed with the ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ (or $|\bar{\bar{+}}\rangle^i$), which are indeed generated from the single-qubit input quantum states $|0\rangle^i$ (or $|+\rangle^i$).[8] Also, after the logical measurements of these ancillary logical quantum states in the standard (or Fourier) basis, quantum nodes publicly check that the twice decoded outcomes of the logical measurements correspond to $|0\rangle^i$ (or $|+\rangle^i$).

B. Outline of the gate teleportation protocol

Here we describe the gate teleportation technique which was first suggested in Ref. [21] (see Table III). The key idea of the technique is to use a specially created ancillary quantum state as a *control* quantum state, measure it with respect to the appropriate basis, and apply necessary quantum correction to the *target* quantum state depending on the measurement outcome. The gate teleportation technique is frequently used for the fault-tolerant realization of the quantum gate that cannot be implemented transversally once a particular QECC is chosen [40]. Since our MPQC protocol is constructed on the basis of the triply even CSS QECCs $\mathcal{C}_{\mathrm{TE}}$ [23,24], the only quantum gate which cannot be implemented transversally in the chosen universal set of quantum gates (X, Z, T, C-X, and H gates) will be the H gate [24]. Therefore, in our MPQC protocol, a nontransversal H gate needs to be implemented by the gate teleportation technique [24].

The gate teleportation protocol implementing the nontransversal H^i gate takes logical quantum state $\bar{\bar{\mathcal{P}}}^i$ and

[7]The number of arbitrary quantum errors at this point cannot exceed $2t$: The dealer D^i and the cheating quantum nodes can introduce only t arbitrary quantum errors during the sharing phase (otherwise the VHSS protocol aborts). Subsequently, the cheating quantum nodes can introduce only t additional quantum errors after the verification phase and before the reconstruction phase.

[8]This is different from the VHSS protocol employed to check whether the quantum node i is honest by simply verifying the encoding of the input ρ^i.

TABLE III. Outline of gate teleportation protocol.

Input. Logical quantum state $\bar{\bar{\mathcal{P}}}^i$ verified by the VHSS protocol, ancillary logical quantum state ${}_v|\bar{\bar{+}}\rangle^i$ verified and confirmed by the VHSS protocol, and a public set B, see Sec. IV A.

Output. Nontransversal $\bar{\bar{H}}^i$ gate applied to the logical quantum state $\bar{\bar{\mathcal{P}}}^i$, i.e., a logical quantum state $\bar{\bar{H}}^i\bar{\bar{\mathcal{P}}}^i\bar{\bar{H}}^i$, and an updated public set B.

1. *Quantum computation.* Each quantum node $j = 1, \ldots, n$ performs the following quantum operations on the $2n$ single-qubit quantum states among which there are n single-qubit quantum states comprising a share $\bar{\bar{\mathcal{P}}}^i_j$ at the beginning of the gate teleportation protocol (called *target* share hereafter), and n single-qubit quantum states comprising a share ${}_v|\bar{\bar{+}}\rangle^i_j$ also at the beginning of the gate teleportation protocol (called *control* share hereafter).
   (a) Quantum node j applies transversal $\bar{\bar{P}}^i_j$ gate to both *target* and *control* shares.
   (b) Quantum node j applies transversal $\overline{\overline{\text{C-}X}}^i_j$ gate with *control* share as the control and *target* share as the target.
   (c) Quantum node j applies transversal $\bar{\bar{P}}^i_j$ gate to the *target* share.
   (d) Quantum node j measures each single-qubit quantum state of the *control* share in the Fourier basis and announces its measurement outcome using a classical authenticated broadcast channel, see Sec. III A.
2. *Classical computation.* The measurement outcomes announced by all the quantum nodes yield codewords in W when rearranged into the groups in such a way that each group corresponds to the logical measurement outcome of the n-qubit logical quantum state (there are n of them) originally encoded and shared by some quantum node k. Here, quantum nodes publicly check the positions of the arbitrary quantum errors by decoding the results of the logical measurements and consequently update the set B. Also, by decoding the codewords in W twice, quantum nodes jointly identify whether the logical measurement results of the *control* shares reconstruct to the single-qubit quantum states $|+\rangle^i$ or $|-\rangle^i$.
3. *Correction.* According to the twice decoded outcomes of the logical measurements, each quantum node $j = 1, \ldots, n$ performs the following quantum operations on his *target* share.
   (a) If the twice decoded outcomes correspond to the $|-\rangle^i$, then the quantum node j does nothing to his *target* share.
   (b) If the twice decoded outcomes correspond to the $|+\rangle^i$, then the quantum node j transversally applies the $-i\bar{\bar{Y}}^i_j$ gate to his *target* share.

ancillary logical quantum state ${}_v|\bar{\bar{+}}\rangle^i$ as an input, see Fig. 4. At this point, both of these logical quantum states are already verified by using the VHSS protocol. In addition, quantum nodes has already jointly confirmed that the ancillary logical quantum state ${}_v|\bar{\bar{+}}\rangle^i$ in their possession is definitely a logical version of the single-qubit quantum state $|+\rangle^i$. It is important to note that this can be achieved by using the VHSS protocol only, see Sec. IV A. Here lies the main difference from the previous suggestion in Ref. [6] as well as its reconsidered version in Ref. [16], where the logical version of the ancillary magic state $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$, which is required for the implementation of the nontransversal T gate with the gate teleportation technique, cannot be verified by using the VHSS protocol only, and therefore an additional verification of the ancillary logical magic state becomes vital [6,16], see Appendix C for the details.[9]

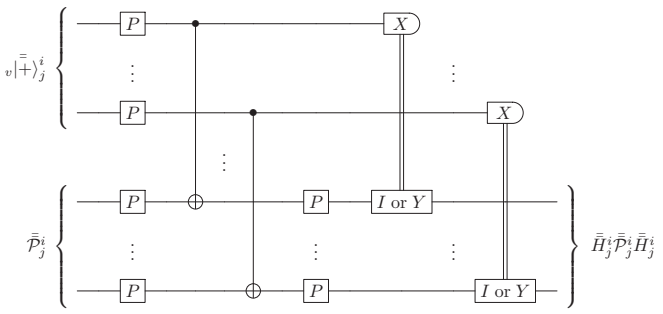

FIG. 4. Fragment of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$ in which quantum node j applies a nontransversal $\bar{\bar{H}}^i_j$ gate to the *target* share $\bar{\bar{\mathcal{P}}}^i_j$ with the gate teleportation technique by taking advantage of the *control* share ${}_v|\bar{\bar{+}}\rangle^i_j$. Note that the quantum gates and the logical measurement presented in the fragment of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$ can be implemented transversally in case of the triply even CSS QECCs $\mathcal{C}_{\text{TE}}$.

To perform the gate teleportation technique and apply a nontransversal $\bar{\bar{H}}^i$ gate to the logical quantum state $\bar{\bar{\mathcal{P}}}^i$, in addition to the n^2 qubits required for holding a share $\bar{\bar{\mathcal{P}}}_i$, each quantum node requires $3n$ qubits to verify and confirm the input ancillary logical quantum state ${}_v|\bar{\bar{+}}\rangle^i$ by using the VHSS protocol, see Sec. IV A, and afterwards n qubits to actually perform the gate teleportation technique. Therefore, the communication complexity of the gate teleportation protocol is the same as of the VHSS protocol, i.e., $O(nr^2)$ qubits per quantum node.

The detailed procedure of the gate teleportation technique is shown in Fig. 4. To apply a nontransversal $\bar{\bar{H}}^i$ gate to the logical quantum state $\bar{\bar{\mathcal{P}}}^i$, quantum nodes transversally apply $\bar{\bar{P}}^i = \bar{\bar{T}}^i \circ \bar{\bar{T}}^i$ gate to their shares of both input logical quantum states $\bar{\bar{\mathcal{P}}}^i$ and ${}_v|\bar{\bar{+}}\rangle^i$, then transversally apply $\overline{\overline{\text{C-}X}}^i$ gate to their shares, taking shares of the ancillary logical quantum state ${}_v|\bar{\bar{+}}\rangle^i$ as the *control* shares and shares of the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ as the *target* shares. Then, quantum nodes transversally apply $\bar{\bar{P}}^i$ gate to the *target* shares and logically measure the *control* shares in the Fourier basis. Next, quantum nodes decode the result of the logical measurements twice and

[9]For the details of the protocol called "verification of the Clifford stabilized states" (VCSS), which was employed in the original version of the MPQC protocol for the verification of the ancillary logical magic state, see Appendixes A and B.

publicly check whether this twice-decoded result corresponds to the $|+\rangle^i$ or $|-\rangle^i$. Finally, if the result corresponds to the $|-\rangle^i$, then quantum nodes do nothing to their *target* shares, but if the result corresponds to the $|+\rangle^i$, then quantum nodes transversally apply the $-i\bar{\bar{Y}}^i = -i\bar{\bar{P}}^i \circ \bar{\bar{X}}^i \circ \overline{\overline{P^\dagger}}^i$ gate to their *target* shares, see Appendix E for the detailed calculations. At the same time, quantum nodes update the public set of apparent cheaters B, and if $|B| > t$ is satisfied, quantum nodes assume that the twice-decoded result of the logical measurement corresponds to the $|-\rangle^i$, and do nothing to their *target* shares. For the detailed procedure of the gate teleportation protocol, see Table III.

V. OUTLINE OF THE MULTIPARTY QUANTUM COMPUTATION PROTOCOL

Here we describe our MPQC protocol in more detail. First of all, the entire MPQC protocol consists of *sharing*, *verification*, *computation*, and *reconstruction* phases and has two subprotocols as its building blocks, i.e., the VHSS protocol and the gate teleportation protocol. Let us see the entire flow of the MPQC protocol by closing up each phase and in parallel explaining how the two subprotocols are involved in the process.

Sharing. At this stage of the MPQC protocol, quantum nodes create global logical quantum state $\bar{\bar{\mathcal{P}}}$ by executing the sharing phase of the VHSS protocol n times. Each time quantum nodes execute the sharing phase of the VHSS protocol with the quantum node i acting as a dealer D^i and the single-qubit quantum state ρ^i as an input, they jointly prepare logical quantum state $\bar{\bar{\mathcal{P}}}^i$, see Table II. Here, each quantum node j requires a workspace of n^2 qubits for holding his share of the global logical quantum state $\bar{\bar{\mathcal{P}}}$, i.e., a share $\bar{\bar{\mathcal{P}}}_j$. We also note that this phase of the MPQC protocol has a communication complexity of $O(n^2)$ qubits per quantum node, which is obvious considering that at this stage of the MPQC protocol quantum nodes simply execute the sharing phase of the VHSS protocol n times. For the details, see Table IV.

Verification. At this stage of the MPQC protocol, quantum nodes jointly verify that the quantum state $\bar{\bar{\mathcal{P}}}$ in their possession is for sure a valid logical quantum state encoded by the triply even CSS QECC $\mathcal{C}_{\mathrm{TE}}$ which is achieved by executing the verification phase of the VHSS protocol n times. Each time quantum nodes execute the verification phase of the VHSS protocol with the quantum node i acting as a dealer D^i, they jointly verify the logical quantum state $\bar{\bar{\mathcal{P}}}^i$ by recording the positions of arbitrary quantum errors introduced by the dealer D^i at the first level encoding and by the cheating quantum nodes at the second level encoding in a public set of apparent cheaters B^i, see Table II. After executing the verification phase of the VHSS protocol n times, quantum nodes jointly construct a global public set of apparent cheaters $B = \bigcup_i B^i$. If at the end of the verification phase $|B| \leqslant t$ is satisfied, then quantum nodes proceed to the computation phase with their shares of the input global logical quantum state $\bar{\bar{\mathcal{P}}}$, i.e., each quantum node i holds a share $\bar{\bar{\mathcal{P}}}_i$. On the other hand, if $|B| > t$ is satisfied, quantum nodes also proceed to the computation phase but the honest quantum nodes replace all the single-qubit quantum states in their possession with $|0\rangle$ and the MPQC protocol is aborted at the end of the computation, see Ref. [6] for the details. We call this procedure the *abortion sequence*. This phase of the MPQC protocol requires a workspace of $n^2 + 2n$ qubits per quantum node for the implementation, among which $2n$ qubits are required for holding ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ and $|\bar{\bar{+}}\rangle^i$ during the verification phase of the VHSS protocol. Also, we note that this phase of the MPQC protocol has a communication complexity of $O(n^2r^2)$ qubits per quantum node, since at this stage of the MPQC protocol quantum nodes simply execute the verification phase of the VHSS protocol n times. For details, see Table IV.

Computation. At this stage of the MPQC protocol, quantum nodes jointly perform logical quantum circuit $\bar{\bar{\mathcal{U}}}$ on the jointly verified global logical quantum state $\bar{\bar{\mathcal{P}}}$, and at the end of this stage quantum nodes will jointly possess some output global logical quantum state $\bar{\bar{\Omega}}$, from which each quantum node i can calculate his output logical quantum state $\bar{\bar{\Omega}}^i = \mathrm{Tr}_{[n]\setminus i}(\bar{\bar{\Omega}})$. We note that the global public set of apparent cheaters B is cumulative throughout the entire MPQC protocol, namely, during the computation phase the global public set of apparent cheaters B is updated whenever the VHSS protocol or the gate teleportation protocol is invoked, see Table IV. If at any stage of the MPQC protocol execution $|B| > t$ is satisfied, the honest quantum nodes replace all the single-qubit quantum states in their possession with $|0\rangle$, and the MPQC protocol is aborted at the end of the computation. Otherwise, quantum nodes proceed to the reconstruction phase with their shares of the output global logical quantum state $\bar{\bar{\Omega}}$. Application of the transversal quantum gates, i.e., $\bar{\bar{X}}^i$, $\bar{\bar{Z}}^i$, $\bar{\bar{T}}^i$, and $\overline{\overline{\text{C-}X}}^{i,j}$ gates (superscripts i, j means that the nonlogical version of the quantum gate is applied between the quantum wires i and j of the quantum circuit $\mathcal{U}$, where the quantum wire i acts as a control and the quantum wire j acts as a target) does not require any additional workspace. On the other hand, whenever the implementation of the logical quantum circuit $\bar{\bar{\mathcal{U}}}$ requires an ancillary logical quantum state or whenever the nontransversal $\bar{\bar{H}}^i$ gate is applied, each quantum node will require an additional workspace of $3n$ qubits to verify and confirm the ancillary logical quantum states $|\bar{\bar{0}}\rangle^i$ or $|\bar{\bar{+}}\rangle^i$, respectively, by using the VHSS protocol, see Table III. Therefore, this phase of the MPQC protocol requires a workspace of $n^2 + 3n$ qubits per quantum node for the implementation and has a communication complexity of $O((\mathrm{No}_{\mathrm{ancillas}} + \mathrm{No}_H)nr^2)$ qubits per quantum node, which is easily evaluated from the number of times the VHSS protocol is invoked during the computation phase. For the details, see Table IV.

Reconstruction. At this stage of the MPQC protocol, each quantum node i acting as a reconstructor R^i collects all the single-qubit quantum states corresponding to his output logical quantum state $\bar{\bar{\Omega}}^i$ from the other quantum nodes and by executing the reconstruction phase of the VHSS protocol eventually obtains his single-qubit output quantum state ω^i, see Table II. During the reconstruction phase of the VHSS protocol, the reconstructor R^i creates another public set of apparent cheaters $\tilde{B}^i$ which records all the arbitrary quantum errors introduced by the cheating quantum nodes at the

TABLE IV. Outline of MPQC protocol.

Input. Private single-qubit quantum state ρ^i from each quantum node i, agreement on a particular $\mathcal{C}_{\text{TE}}$ and on a particular $\mathcal{U}$.
Output. In case of success, each quantum node i possesses a private single-qubit quantum state ω^i. In case of failure, the honest quantum nodes replace all the single-qubit quantum states in their possession with $|0\rangle$ and the MPQC protocol is aborted at the end of the computation.

1. *Sharing.* For $i = 1, \ldots, n$, quantum nodes execute the sharing phase of the VHSS protocol with the quantum node i acting as a dealer D^i and the ρ^i as an input, and jointly prepare logical quantum state $\bar{\bar{\mathcal{P}}}^i$, see Table II. When all the n quantum nodes participating in the MPQC protocol have finished the sharing phase of the VHSS protocol, quantum nodes jointly possess a global logical quantum state $\bar{\bar{\mathcal{P}}}$.
2. *Verification.* For $i = 1, \ldots, n$, quantum nodes execute the verification phase of the VHSS protocol with the quantum node i acting as a dealer D^i and jointly verify the logical quantum state $\bar{\bar{\mathcal{P}}}^i$, see Table II.
   (a) Quantum nodes jointly construct a public set $B^{i,j}$ which records all the arbitrary quantum errors introduced by the dealer D^i and by the cheating quantum nodes during all the n executions of the VHSS protocol. For $j = 1, \ldots, n$, if $|B^{i,j}| > t$ is satisfied, then quantum nodes add quantum node j to the public set B^i.
   (b) After all the n executions of the VHSS protocol, quantum nodes jointly construct a global public set $B = \bigcup_i B^i$. If $|B| > t$ is satisfied, the *abortion sequence* is invoked.
3. *Computation.* Quantum nodes apply logical quantum gates ($\bar{\bar{X}}^i$, $\bar{\bar{Z}}^i$, $\bar{\bar{T}}^i$, $\overline{\overline{\text{C-}X}}^{i,j}$, and $\bar{\bar{H}}^i$ gates) to the global logical quantum state $\bar{\bar{\mathcal{P}}}$ in a particular order specified by the logical quantum circuit $\bar{\bar{\mathcal{U}}}$.
   (a) For every transversal $\bar{\bar{X}}^i$, $\bar{\bar{Z}}^i$, or $\bar{\bar{T}}^i$ gate applied to the logical quantum state $\bar{\bar{\mathcal{P}}}^i$, each quantum node $j = 1, \ldots, n$ applies X, Z, or T gates to the n single-qubit quantum states comprising his share $\bar{\bar{\mathcal{P}}}^i_j$.
   (b) For every transversal $\overline{\overline{\text{C-}X}}^{i,j}$ gate applied between the logical quantum states $\bar{\bar{\mathcal{P}}}^i$ and $\bar{\bar{\mathcal{P}}}^j$, each quantum node $k = 1, \ldots, n$ applies C-$X^{i,j}$ gates between the n single-qubit quantum states comprising a share $\bar{\bar{\mathcal{P}}}^i_k$ and the n single-qubit quantum states comprising a share $\bar{\bar{\mathcal{P}}}^j_k$.
   (c) For every non-transversal $\bar{\bar{H}}^i$ gate applied to the logical quantum state $\bar{\bar{\mathcal{P}}}^i$, quantum nodes take the following two actions:
      i. Quantum nodes jointly create, then verify and confirm ancillary logical quantum state ${}_v|\bar{\bar{+}}\rangle^i$ by using the VHSS protocol, see Table II.
      ii. Then, quantum nodes jointly perform the gate teleportation protocol with two input logical quantum states: $\bar{\bar{\mathcal{P}}}^i$ and ${}_v|\bar{\bar{+}}\rangle^i$, see Table III, and if at the end of the gate teleportation protocol execution $|B| > t$ is satisfied, the *abortion sequence* is invoked.
   (d) If the ancillary single-qubit quantum state $|0\rangle^i$ is required for the implementation of the quantum circuit $\mathcal{U}$, quantum nodes jointly create, then verify and confirm ancillary logical quantum state ${}_v|\bar{\bar{0}}\rangle^i$ by using the VHSS protocol with the randomly chosen quantum node $i \notin B$ acting as a dealer D^i.
   (e) If at any stage of the MPQC protocol execution $|B| > t$ is satisfied, the *abortion sequence* is invoked.
4. *Reconstruction.* Each quantum node $i = 1, \ldots, n$ executes the reconstruction phase of the VHSS protocol as a reconstructor R^i after collecting all the single-qubit quantum states corresponding to his output logical quantum state $\bar{\bar{\Omega}}^i$ from the other quantum nodes.
   (a) Reconstructor R^i identifies arbitrary quantum errors in each n-qubit logical quantum state originally encoded and shared by the quantum node $j \notin B$ during the second level encoding, by using $\mathcal{C}_{\text{TE}}$. In parallel, the reconstructor R^i creates another public set $\tilde{B}^{i,j}$ which records all the arbitrary quantum errors introduced by the cheating quantum nodes at the second level encoding and satisfies $B^{i,j} \subseteq \tilde{B}^{i,j}$. After that, the reconstructor R^i decodes each n-qubit logical quantum state satisfying $|\tilde{B}^{i,j}| \leqslant t$. On the other hand, if some n-qubit logical quantum state originally encoded and shared by the quantum node $j \notin B$ during the second level encoding satisfies $|\tilde{B}^{i,j}| > t$, the reconstructor R^i adds quantum node j to the public set B.
   (b) Reconstructor R^i randomly chooses $n - 2t$ single-qubit quantum states, each originally encoded and shared by the quantum node $j \notin B$, performs erasure recovery by using $\mathcal{C}_{\text{TE}}$, and by decoding obtains output ω^i.

second level encoding, and in such a way checks whether each quantum node j is honest, i.e., if $|\tilde{B}^i| > t$ is satisfied, the reconstructor R^i adds quantum node j to the global public set of apparent cheaters B. This phase of the MPQC protocol does not require any additional workspace for the implementation and has a communication complexity of $O(n^2)$ qubits per quantum node, which indeed should be identical to the sharing phase since, in terms of the communication complexity, they are identical. For the details, see Table IV.

VI. SECURITY PROOF OF THE MULTIPARTY QUANTUM COMPUTATION PROTOCOL

In this section, we prove that our MPQC protocol is secure. First, we state the security framework as well as the security definition in Sec. VI A, and second, in Sec. VI B, we show that the security proof of our MPQC protocol is identical to the security proof of the previously suggested MPQC protocol. In addition, to be self-contained, we briefly present the security proof of our MPQC protocol in Secs. VI B 1 and VI B 2.

A. Security statements

Here we state the security framework and the security definition following Refs. [6,41–44]. To prove that our MPQC protocol is secure we employ the simulator-based security definition, which automatically satisfies requirements of *correctness*, *soundness*, and *privacy* mentioned in Sec. I. The simulator-based security definition uses two models: the "real" model corresponding to the execution of the actual MPQC protocol and the "ideal" model where quantum nodes interact with an oracle that performs the MPQC protocol perfectly and cannot be corrupted by the adversary. In this security framework, the MPQC protocol is said to be secure if

one cannot distinguish a real execution from an ideal execution of the MPQC protocol.

In the ideal model the honest quantum nodes solely send their input quantum states to the oracle and merely output whatever they receive from the oracle as their results. On the other hand, cheating quantum nodes are allowed to perform any joint quantum operation on their input quantum states before sending them to the oracle and also to perform any joint quantum operation on whatever they receive from the oracle before they output their results. We assume that the cheating quantum nodes are nonadaptively corrupted by an active adversary $\mathcal{A}$, which can corrupt $t < n/4$ quantum nodes but otherwise has unlimited computational power, see Sec. III B. Hereafter, an adversary in the real model will be denoted $\mathcal{A}_{\text{real}}$ and an adversary in the ideal model will be denoted $\mathcal{A}_{\text{ideal}}$.

Definition of ϵ-security The MPQC protocol Π is ϵ-secure, if for any input quantum state ρ, and for any adversary in the real model $\mathcal{A}_{\text{real}}$, there exists an adversary in the ideal model $\mathcal{A}_{\text{ideal}}$ such that the output quantum state $\omega_{\text{real}} \coloneqq \Pi_{\text{real}}(\rho)$ of the real model is ϵ-close to the output quantum state $\omega_{\text{ideal}} \coloneqq \Pi_{\text{ideal}}(\rho)$ of the ideal model, i.e.,

$$\tfrac{1}{2}\|\omega_{\text{real}} - \omega_{\text{ideal}}\|_1 \leqslant \epsilon. \tag{4}$$

By using the definition of the ϵ-security we can state the security of our MPQC protocol as follows, see Refs. [6,16] for the details.

Theorem 1. The MPQC protocol is $\kappa 2^{-\Omega(r)}$-secure, where $\kappa = n + \text{No}_{\text{ancillas}} + \text{No}_H$.

Proof of the security of our MPQC protocol will be almost the same as the security proof of the previously suggested MPQC protocol in Refs. [6,16],[10] and the only essential difference lies in the type of the nontransversal quantum gate, namely, the T gate is substituted for the H gate, and in the basis of the logical measurement, namely, the normal basis is substituted for the Fourier basis. In particular, in the security proof of the previously suggested MPQC protocol the ideal protocol is constructed by using a simulation technique, i.e., for any real adversary $\mathcal{A}_{\text{real}}$ an ideal adversary $\mathcal{A}_{\text{ideal}}$ is constructed by saying that an ideal adversary $\mathcal{A}_{\text{ideal}}$ internally simulates the execution of the real protocol with real adversary $\mathcal{A}_{\text{real}}$. Specifically, one writes the execution of the real protocol and the ideal protocol and shows that the outputs of both protocols are equivalent in the case of success of the VHSS protocol. Finally, we note that the security definition employed in this paper follows the paradigm of sequential composability, see Refs. [6,16] for the details.

B. Security proof

Here we show that the security proof of our MPQC protocol can be reduced to the security proof of the previously suggested MPQC protocol presented in Refs. [6,16]. To achieve that, we borrow statements from the previous suggestion and restate the lemma with the corresponding proof, as will be given below, and in such a way show that there is no difference between our MPQC protocol and the MPQC protocol in Refs. [6,16] when the security proof is the concern. The lemma shows that preparing, sharing, and verifying the input quantum state, then performing logical quantum circuit $\bar{\bar{\mathcal{U}}}$, and finally reconstructing and measuring the output quantum state is equivalent to preparing the input quantum state, performing quantum circuit $\mathcal{U}$, and measuring the output quantum state without any encoding. After restating the lemma, we also restate the property that extends the applicability of the lemma from individual quantum operations to the entire quantum circuit.

Lemma 1. Let us define a public set of apparent cheaters at the end of the computation phase as B_{C}, such that $|B_{\text{C}}| \leqslant t$, and let us define a set of real cheaters at the end of the computation phase as A_{C}. Let us also denote the decoding procedure for the triply even CSS QECC $\mathcal{C}_{\text{TE}}$ as $\mathcal{D}$ and the erasure recovery procedure for the triply even CSS QECC $\mathcal{C}_{\text{TE}}$ as $\hat{\mathcal{D}}$. If the global logical quantum state $\bar{\bar{\mathcal{P}}}$ encoded twice by using the triply even CSS QECC $\mathcal{C}_{\text{TE}}$ is decodable, i.e.,

$$\mathcal{P} = \bigotimes_{i\in[n]} \left(\hat{\mathcal{D}}_{\overline{B_{\text{C}}\cup A_{\text{C}}}} \circ \bigotimes_{j\in\overline{B_{\text{C}}\cup A_{\text{C}}}} \mathcal{D}_j \right) (\bar{\bar{\mathcal{P}}}), \tag{5}$$

then application of a logical quantum operation $\bar{\bar{\mathcal{Q}}}$ to the global logical quantum state $\bar{\bar{\mathcal{P}}}$ is also decodable, i.e.,

$$\mathcal{Q}(\mathcal{P}) = \bigotimes_{i\in[n]} \left(\hat{\mathcal{D}}_{\overline{B_{\text{C}}\cup A_{\text{C}}}} \circ \bigotimes_{j\in\overline{B_{\text{C}}\cup A_{\text{C}}}} \mathcal{D}_j \right) [\bar{\bar{\mathcal{Q}}}(\bar{\bar{\mathcal{P}}})], \tag{6}$$

where the logical quantum operation $\bar{\bar{\mathcal{Q}}}$ may denote:

(1) Logical versions of the transversal quantum gates, i.e., X, Z, T, or C-X gates, applied to the global logical quantum state $\bar{\bar{\mathcal{P}}}$.

(2) Logical version of the nontransversal H gate applied to the global logical quantum state $\bar{\bar{\mathcal{P}}}$ by using the gate teleportation protocol.

(3) Logical measurement in the standard or Fourier basis $\bar{\bar{\mathcal{M}}}$ which is implemented by local measurements of the single-qubit quantum states, each denoted as $\mathcal{M}$, and the classical communication.

Proof. Lemma 1 follows from the fact that, to realize a logical quantum operation $\bar{\bar{\mathcal{Q}}}$, it is sufficient to apply quantum operations $\mathcal{Q}$ honestly on the shares of the quantum nodes in the set $\overline{B_{\text{C}} \cup A_{\text{C}}}$. First, the application of transversal quantum gates (X, Z, T, and C-X gates) on the shares of the quantum nodes in the set $\overline{B_{\text{C}} \cup A_{\text{C}}}$ indeed realizes the logical versions of these quantum gates ($\bar{\bar{X}}$, $\bar{\bar{Z}}$, $\bar{\bar{T}}$, and $\overline{\overline{\text{C-}X}}$ gates) [45]. Second, in case of CSS QECCs, the logical measurement $\bar{\bar{\mathcal{M}}}$ in the standard or Fourier basis can be implemented transversally. Third, we implement a nontransversal H gate by combining the transversal quantum gates with the transversally implemented logical measurement. ■

Property 1. Let us define a quantum circuit as $\mathcal{R}$. Then, Lemma 1 holds even when we replace quantum operation $\mathcal{Q}$

[10] In Ref. [16] it was shown that the security proofs of the original version of the MPQC protocol in Ref. [6] and the reconsidered version of the MPQC protocol in Ref. [16] are identical.

by a quantum circuit $\mathcal{R}$, i.e.,

$$\mathcal{R}(\mathcal{P}) = \bigotimes_{i\in[n]} \left(\hat{\mathcal{D}}_{\overline{B_C \cup A_C}} \circ \bigotimes_{j\in\overline{B_C\cup A_C}} \mathcal{D}_j \right) [\bar{\bar{\mathcal{R}}}(\bar{\bar{\mathcal{P}}})]. \tag{7}$$

Proof. Property 1 immediately follows from the fact that any quantum circuit $\mathcal{R}$ can be decomposed as $\mathcal{R} = \mathcal{U} \circ \mathcal{M}$, where the quantum circuit $\mathcal{U}$ can be decomposed into the quantum gates chosen so as to implement the UQC (which are the X, Z, T, C-X, and H gates in our case). ■

With the Property 1 at hand, it becomes clear that the security proof of our MPQC protocol will be absolutely the same as the security proof of the previously suggested MPQC protocol presented in Refs. [6,16] since the difference between Property 1 in our current suggestion and the property in the previous suggestion is reduced to which quantum gate is implemented by the gate teleportation technique (H gate instead of T gate in our case) and in which basis logical measurement is performed during the gate teleportation technique (Fourier basis instead of normal basis in our case). Note that in our MPQC protocol the previously inevitable verification of the magic-state technique, see Appendix C, is not necessary at all,[11] and, therefore, is out of consideration.

However, solely to be self-contained, we briefly present the security proof of our MPQC protocol, i.e., the proof of Theorem 1. Specifically, we follow the security proof of the previously suggested MPQC protocol presented in Refs. [6,16], which was actually inspired by the approach taken in Refs. [3,4,46]. We construct the real protocol by expressing each quantum operation performed during the execution of the real protocol, and consequently the output quantum state of the real protocol ω_{real} in terms of the general maps, see Sec. VI B 1. Then, the same is done for the ideal protocol and the output quantum state of the ideal protocol ω_{ideal} is also obtained, see Sec. VI B 2. Indeed, if these outputs are compared it becomes clear that they are exponentially close to each other in the security parameter r, see Theorem 1.[12]

Finally, let us explain where the probability of error in the security statement of the MPQC protocol in Theorem 1 comes from. Every verification performed by using the VHSS protocol has the probability of error $2^{-\Omega(r)}$. During the MPQC protocol, the VHSS protocol is invoked in the following three situations:

(1) when the quantum nodes jointly verify the encoding of each single-qubit input quantum state ρ^i (there are n of them);

(2) when quantum nodes jointly verify and confirm the ancillary logical quantum state $|\bar{\bar{+}}\rangle^i$ necessary for the implementation of the nontransversal H^i gate via the gate teleportation technique;

(3) when quantum nodes jointly verify and confirm the ancillary logical quantum state $|\bar{\bar{0}}\rangle^i$ necessary for the implementation of the quantum circuit $\mathcal{U}$.

If we summarize the above three cases we obtain the total number of VHSS protocol executions during the MPQC protocol as $\kappa = n + \text{No}_{\text{ancillas}} + \text{No}_H$ and the total probability of error will be $\kappa 2^{-\Omega(r)}$. ■

1. Real protocol

Here we construct the real execution of the MPQC protocol. As explained in Sec. VI B 2, since in the ideal protocol the *oracle* receives an "abort" flag at the end of the computation, in the real protocol one should also abort at the end of the computation. However, computation with $|B| > t$ already satisfied may allow cheating quantum nodes to obtain some information on the inputs of the honest quantum nodes. Therefore, to avoid this situation, the honest quantum nodes replace single-qubit quantum states in their possession with $|0\rangle$ whenever $|B| > t$ is satisfied, see Ref. [6] for the details.

First of all, let us denote the registers of the honest and cheating quantum nodes in the real protocol as H_R and A_R, respectively. Then, if we denote the general map of the sharing and verification phases as $\mathcal{VS}_{H_R A_R}$, and the input quantum state of all the quantum nodes as $\rho_{H_R A_R}$, the quantum state after the sharing and the verification will be denoted

$$\sigma^{\mathcal{VS}} = \mathcal{VS}_{H_R A_R}(\rho_{H_R A_R}). \tag{8}$$

Then, real protocol continues to the computation phase. Here, if $|B| \leqslant t$ is satisfied, all the quantum nodes jointly perform the logical quantum circuit $\bar{\bar{\mathcal{R}}}_{H_R A_R}$. On the other hand, if $|B| > t$ is satisfied, the honest quantum nodes replace single-qubit quantum states in their possession with $|0\rangle$ and the cheating quantum nodes perform the arbitrary quantum operation $\mathcal{M}'_{A_R}$ on the shares in their possession. Therefore, the quantum state after the computation will be denoted

$$\sigma^{\mathcal{R}} = \begin{cases} \bar{\bar{\mathcal{R}}}_{H_R A_R}(\sigma^{\mathcal{VS}}) & |B| \leqslant t \\ \mathcal{M}'_{A_R} \circ \text{Tr}_{H_R}(\sigma^{\mathcal{VS}}) \otimes |0\rangle\langle 0|_{H_R} & |B| > t. \end{cases} \tag{9}$$

Next, if $|B| \leqslant t$ is satisfied after the computation phase, the real protocol continues to the reconstruction phase. The honest quantum nodes perform the decoding procedure and the erasure recovery procedure, together denoted as $\mathcal{D}_{H_R}$. At the same time, the cheating quantum nodes perform arbitrary quantum operation $\mathcal{W}_{A_R}$ on the shares in their possession. On the other hand, if $|B| > t$ is satisfied, the honest quantum nodes output the "abort" flag $|\perp\rangle\langle\perp|_{H_R}$. Simultaneously, the cheating quantum nodes perform arbitrary quantum operation $\mathcal{M}''_{A_R}$ on the shares in their possession. Consequently, the quantum state after the reconstruction will be denoted

$$\sigma^{\mathcal{D}} = \begin{cases} (\mathcal{D}_{H_R} \otimes \mathcal{W}_{A_R})(\sigma^{\mathcal{R}}) & |B| \leqslant t \\ |\perp\rangle\langle\perp|_{H_R} \otimes \mathcal{M}''_{A_R}[\text{Tr}_{H_R}(\sigma^{\mathcal{R}})] & |B| > t. \end{cases} \tag{10}$$

Hereinafter, we describe only the case when $|B| \leqslant t$ is satisfied, since it is enough for our purpose. The case when $|B| > t$ is satisfied can be found in Ref. [6]. To simplify Eq. (10), we introduce an identity map $\mathbb{I}_{H_R A_R} = \mathcal{D}_{H_R A_R} \circ \mathcal{E}_{H_R A_R}$, where $\mathcal{D}_{H_R A_R}$ and $\mathcal{E}_{H_R A_R}$ denote the decoding and the encoding procedures, respectively. By using this identity map, the

[11] The same can be said also for the protocol called "verification of the Clifford stabilized states" (VCSS), see Appendix A and Appendix B.

[12] If we suppose that the VHSS protocol involved in the construction of the MPQC protocol has no any probability of error, one will actually achieve $\omega_{\text{real}} = \omega_{\text{ideal}}$.

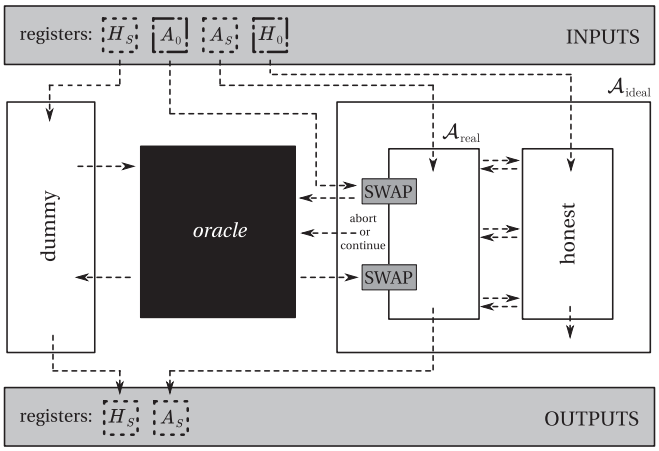

FIG. 5. Schematic picture of the simulator-based security proof of the MPQC protocol. The ideal execution of the MPQC protocol requires following four types of quantum registers: registers of the simulated honest quantum nodes H_0, registers of the simulated cheating quantum nodes A_0, "dummy" input registers of the honest quantum nodes in the simulation H_S, and input registers of the cheating quantum nodes in the simulation A_S. Also, ideal protocol requires a classical flag to decide whether to abort the MPQC or not, which is denoted "abort" or "continue."

output quantum state ω_{real} of the real protocol can be written as

$$\omega_{\text{real}} = (\mathcal{D}_{H_R} \otimes \mathcal{W}_{A_R}) \circ \mathcal{E}_{H_R A_R} \circ \mathcal{D}_{H_R A_R}(\sigma^{\mathcal{R}}). \tag{11}$$

To simplify Eq. (11), we employ the results of the Lemma 1 and the Property 1, i.e., that preparing, sharing, and verifying the input quantum state of all the quantum nodes $\rho_{H_R A_R}$, then performing logical quantum circuit $\bar{\bar{\mathcal{R}}}_{H_R A_R}$, and finally reconstructing and measuring the output quantum state is equivalent to preparing the input quantum state of all the quantum nodes $\rho_{H_R A_R}$, performing quantum circuit $\mathcal{R}_{H_R A_R}$, and measuring the output quantum state without any encoding, see Sec. VI B. Therefore, the output quantum state ω_{real} of the real protocol can be further simplified as

$$\omega_{\text{real}} = (\mathcal{D}_{H_R} \otimes \mathcal{W}_{A_R}) \circ \mathcal{E}_{H_R A_R} \circ \mathcal{R}_{H_R A_R}(\rho_{H_R A_R}). \tag{12}$$

2. *Ideal protocol*

Next we construct the ideal execution of the MPQC protocol. The adversary in the ideal protocol $\mathcal{A}_{\text{ideal}}$ will internally simulate the real protocol with the real adversary $\mathcal{A}_{\text{real}}$. Here, the simulated honest quantum nodes will interact with the simulated cheating quantum nodes controlled by the real adversary $\mathcal{A}_{\text{real}}$, see Fig. 5. In the ideal protocol, the ideal adversary $\mathcal{A}_{\text{ideal}}$ and the honest quantum nodes interact with an *oracle* that perfectly realizes the MPQC protocol and cannot be corrupted. As an input, the *oracle* requires "dummy" quantum registers of the honest quantum nodes in the simulation H_S, quantum registers of the cheating quantum nodes in the simulation A_S, and a classical flag which indicates whether the *oracle* should abort the ideal protocol.

If we denote the input quantum state of all the quantum nodes in the simulation as $\rho_{H_S A_S}$ the entire input into the ideal protocol will be $\rho_{H_S A_S} \otimes |0\rangle\langle 0|_{H_0 A_0}$. Furthermore, if we denote the general map of the sharing and verification phases as $\mathcal{VS}_{H_0 A_S}$,[13] the quantum state after the sharing and the verification will be denoted

$$\sigma^{\mathcal{VS}} = \mathcal{VS}_{H_0 A_S}\big(\rho_{H_S A_S} \otimes |0\rangle\langle 0|_{H_0 A_0}\big). \tag{13}$$

Before the ideal protocol continues to the computation phase, the ideal adversary $\mathcal{A}_{\text{ideal}}$ does the following:

(1) If $|B| \leqslant t$ is satisfied, the ideal adversary $\mathcal{A}_{\text{ideal}}$ performs an encoding procedure twice, which we denoted $\mathcal{E}_{A_0}$, and subsequently applies a SWAP gate between the registers A_0 and A_S. After that, the ideal adversary $\mathcal{A}_{\text{ideal}}$ performs an erasure recovery procedure twice, which we denoted $\mathcal{D}_{A_0}$, on the registers of the quantum nodes not in the public set of apparent cheaters B, and finally sends the registers of the simulated cheating quantum nodes A_0 to the *oracle*.

(2) On the other hand, if $|B| > t$ is satisfied, the simulated honest quantum nodes replace single-qubit quantum states in their possession with $|0\rangle$, while the ideal adversary $\mathcal{A}_{\text{ideal}}$ sends the registers of the simulated cheating quantum nodes A_0, as inputs of the cheating quantum nodes in the simulation, to the *oracle*. Also, simulated cheating quantum nodes perform arbitrary quantum operation $\mathcal{M}'_{A_S}$ on the shares in their possession.

Therefore, the quantum state after the first interaction with the *oracle* can be written as

$$\sigma^{or.1} = \begin{cases} \mathcal{D}_{A_0} \circ \text{SWAP}_{A_0 A_S} \circ \mathcal{E}_{A_0}(\sigma^{\mathcal{VS}}) & |B| \leqslant t \\ \mathcal{M}'_{A_S} \circ \text{Tr}_{H_0}(\sigma^{\mathcal{VS}}) \otimes |0\rangle\langle 0|_{H_0} & |B| > t. \end{cases} \tag{14}$$

Then, the ideal adversary $\mathcal{A}_{\text{ideal}}$ proceeds to the computation phase on the registers H_0 and A_S. Meanwhile, the *oracle* performs the ideal quantum circuit $\mathcal{R}^{\text{ideal}}_{H_S A_0}$. Therefore, the quantum state after these quantum operations can be written as

$$\sigma^{\mathcal{R}} = \begin{cases} \big(\mathcal{R}^{\text{ideal}}_{H_S A_0} \otimes \bar{\bar{\mathcal{R}}}_{H_0 A_S}\big)\big(\sigma^{or.1}\big) & |B| \leqslant t \\ \big(\mathcal{R}^{\text{ideal}}_{H_S A_0} \otimes \bar{\bar{\mathcal{R}}}_{H_0 A_S}\big)\big(\sigma^{or.1}\big) & |B| > t. \end{cases} \tag{15}$$

Next, depending on the number of apparent cheaters, the ideal adversary $\mathcal{A}_{\text{ideal}}$ and the *oracle* will behave in the following two ways:

(1) If $|B| \leqslant t$ is satisfied, the ideal adversary $\mathcal{A}_{\text{ideal}}$ sends the flag "continue" to the *oracle* and the *oracle* outputs the result of the ideal quantum circuit $\mathcal{R}^{\text{ideal}}_{H_S A_0}$ evaluation.

(2) On the other hand, if $|B| > t$ is satisfied, the ideal adversary $\mathcal{A}_{\text{ideal}}$ sends the flag "abort" to the *oracle* and the *oracle* outputs $|\perp\rangle\langle\perp|$.

After that, the honest quantum nodes in the simulation output whatever they receive from the *oracle* as their results. On the other hand, after receiving the output of the *oracle* the ideal adversary $\mathcal{A}_{\text{ideal}}$ does the following:

(1) If $|B| \leqslant t$ is satisfied, the ideal adversary $\mathcal{A}_{\text{ideal}}$ performs an encoding procedure twice, which we already denoted $\mathcal{E}_{A_0}$, and finally, the ideal adversary $\mathcal{A}_{\text{ideal}}$ applies a SWAP gate between the registers A_S and A_0.

(2) On the other hand, if $|B| > t$ is satisfied, the simulated real protocol aborts and the ideal adversary $\mathcal{A}_{\text{ideal}}$ outputs the result of the real adversary $\mathcal{A}_{\text{real}}$. Finally, simulated cheating

[13] Simultaneously, the identity map $\mathbb{I}_{H_S A_0}$ is applied to the quantum registers H_S and A_0.

quantum nodes perform an arbitrary quantum operation $\mathcal{M}''_{A_S}$ on the shares in their possession.

The quantum state after the second interaction with the *oracle* can be written as

$$\sigma^{or.^2} = \begin{cases} \mathrm{SWAP}_{A_0A_S} \circ \mathcal{E}_{A_0}(\sigma^{\mathcal{R}}) & |B| \leqslant t \\ |\perp\rangle\langle\perp|_{H_SA_0} \otimes \mathrm{Tr}_{H_SA_0}[\mathcal{M}''_{A_S}(\sigma^{\mathcal{R}})] & |B| > t. \end{cases} \tag{16}$$

Hereinafter, we describe only the case when $|B| \leqslant t$ is satisfied, since it is enough for our purpose. The case when $|B| > t$ is satisfied can be found in Ref. [6] as well. To simplify Eq. (16) we employ the identity which holds for any quantum operation $Q_{H_SA_0H_0A_S}$ and can be written as $\mathrm{SWAP}_{A_0A_S} \circ Q_{H_SA_0H_0A_S} \circ \mathrm{SWAP}_{A_0A_S} = Q_{H_SA_SH_0A_0}$. By using this identity, as well as Eq. (13), the simplified quantum state after the second interaction with the oracle and in the case when $|B| \leqslant t$ is satisfied can be written as

$$\begin{aligned} \sigma^{\mathrm{simp.}} &= \left(\mathcal{E}_{A_S} \circ \mathcal{R}^{\mathrm{ideal}}_{H_SA_S} \circ \mathcal{D}_{A_S}\right) \otimes (\bar{\bar{R}}_{H_0A_0} \circ \mathcal{E}_{A_0})(\sigma^{\mathcal{VS}}) \\ &= \left[\mathcal{E}_{A_S} \circ \mathcal{R}^{\mathrm{ideal}}_{H_SA_S} \circ \mathcal{D}_{A_S} \circ \mathcal{VS}_{A_S}(\rho_{H_SA_S})\right] \\ &\quad \otimes [\bar{\bar{R}}_{H_0A_0} \circ \mathcal{E}_{A_0} \circ \mathcal{VS}_{A_0}(|0\rangle\langle 0|_{H_0A_0})]. \end{aligned} \tag{17}$$

Note that the simplification in Eq. (17) means that the composition of two SWAP gates between the registers A_0 and A_S with the ideal quantum circuit $\mathcal{R}^{\mathrm{ideal}}_{H_SA_0}$ performed by the *oracle* is equivalent to the evaluation of the ideal quantum circuit $\mathcal{R}^{\mathrm{ideal}}_{H_SA_S}$ by the *oracle*.

Finally, the ideal adversary $\mathcal{A}_{\mathrm{ideal}}$ proceeds to the reconstruction phase, in which the simulated honest quantum nodes perform the decoding procedure and the erasure recovery procedure, together denoted $\mathcal{D}_{H_0}$. Simultaneously, the simulated cheating quantum nodes perform the arbitrary quantum operation $\mathcal{W}_{A_S}$ on the shares in their possession and the ideal adversary $\mathcal{A}_{\mathrm{ideal}}$ outputs the result of the real adversary $\mathcal{A}_{\mathrm{real}}$. Therefore, the output quantum state ω_{ideal} of the ideal protocol can be written as

$$\omega_{\mathrm{ideal}} = \mathrm{Tr}_{H_0A_0}[\mathcal{D}_{H_0} \otimes \mathcal{W}_{A_S}(\sigma^{\mathrm{simp.}})], \tag{18}$$

and, if we employ the identity maps $\mathbb{I}_{A_S} = \mathcal{D}_{A_S} \circ \mathcal{VS}_{A_S}$ and $\mathbb{I}_{H_S} = \mathcal{D}_{H_S} \circ \mathcal{E}_{H_S}$, Eq. (18) can be further simplified as

$$\omega_{\mathrm{ideal}} = (\mathcal{D}_{H_S} \otimes \mathcal{W}_{A_S}) \circ \mathcal{E}_{H_SA_S} \circ \mathcal{R}^{\mathrm{ideal}}_{H_SA_S}(\rho_{H_SA_S}). \tag{19}$$

VII. SUMMARY

To summarize, in this paper we suggested an MPQC protocol built upon a technique of quantum error correction and in particular constructed on the basis of the triply even CSS QECCs. With the triply even CSS QECCs at hand, once we decide on the X, Z, T, C-X, and H gates as our universal set of quantum gates, since all the transversal quantum gates can be implemented trivially, the task of the UQC realization in the MPQC protocol reduces to the implementation of the nontransversal H gate, which can be easily addressed by the gate teleportation technique. Importantly, this technique requires a logical plus state as an ancillary quantum state, whose preparation, verification, and confirmation can be accomplished by using the VHSS protocol only. In contrast, the previously suggested MPQC protocol was constructed on the basis of the self-dual CSS QECCs, in which case, the task of the UQC realization cannot be attained without the implementation of the nontransversal T gate and the gate teleportation technique comes to aid again. Crucially, the implementation of the nontransversal T gate with the gate teleportation technique requires a logical magic state as an ancillary quantum state, which preparation, verification, and confirmation can be accomplished only by using a combination of the two subprotocols: the VHSS protocol and the protocol verifying the magic state, the latter of which is implemented by a statistical testing of the randomly selected magic states with their subsequent distillation.[14] Therefore, our decision on the triply even CSS QECCs allows us to avoid execution of the resource-intensive protocol verifying the magic state and consequently reduce our demand for the workspace per quantum node from $n^2 + \Theta(r)n$ qubits in the previous suggestion to $n^2 + 3n$ qubits in our case, where n is the number of quantum nodes participating in the MPQC protocol and r is the security parameter. Besides, since every extra qubit reduces the credibility of physical devices, our suggestion makes the MPQC protocol more accessible for the near-future technology.

ACKNOWLEDGMENTS

The authors would like to thank Suguru Endo, Kaoru Yamamoto, Yuuki Tokunaga, and especially Yasunari Suzuki for fruitful discussions on the techniques of quantum error correction. The authors also acknowledge Akinori Hosoyamada for insightful comments on the techniques of classical cryptography.

APPENDIX A: SUMMARY OF THE VCSS PROTOCOL

Here we briefly describe the VCSS protocol which is necessary for the verification of the ancillary logical magic state $|\bar{\bar{m}}\rangle^i$, i.e., whether it is certainly a logical magic state, in case of the original version of the MPQC protocol based on self-dual CSS QECCs [6]. The idea of the VCSS protocol construction is inspired by the procedure of the stabilizer measurement in the technique of quantum error correction. To begin with, consider $XP^\dagger$ gate, and the magic state $|m\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$ which is a $+1$ eigenstate of the $XP^\dagger$ gate (see Sec. B for the criticism towards this claim). Then the equation C-$XP^\dagger(|+\rangle|m\rangle) = |+\rangle|m\rangle$ holds, where C-$XP^\dagger$ gate is applied between the single-qubit quantum state $|+\rangle$ acting as the control quantum state and the ancillary magic state $|m\rangle$ acting as the target quantum state. This insight suggests on how to implement the verification of the $|m\rangle$. If the target quantum state was $|m\rangle$, then after applying C-$XP^\dagger$ gate one will always measure the control quantum state in $|+\rangle$. On the other hand, if the target quantum state was not $|m\rangle$ and one measures the control quantum state in $|+\rangle$, then one has projected the target quantum state onto $|m\rangle$.

The above procedure can be adapted to confirm that the quantum state $|\bar{\bar{m}}\rangle^i$ in the possession of the quantum nodes is for sure an anticipated ancillary logical magic state. First,

[14] The original version of the protocol verifying the magic state employed a nontransversal C-$XP^\dagger$ gate potentially leading to a failure of the entire MPQC protocol.

by using the VHSS protocol, quantum nodes jointly verify and confirm the logical quantum state ${}_v|\bar{\bar{0}}\rangle^i$, see Sec. IV A. Second, by using the VHSS protocol one more time, quantum nodes jointly verify that the quantum state $|\bar{\bar{m}}\rangle^i$ in their possession is for sure a valid logical quantum state encoded by a self-dual CSS QECC, see Sec. IV A. Next, to obtain the logical quantum state $|\bar{\bar{+}}\rangle^i$ quantum nodes transversally apply $\bar{\bar{H}}^i$ gate [15] to the logical quantum state ${}_v|\bar{\bar{0}}\rangle^i$, and subsequently apply $\overline{\overline{\text{C-}XP^\dagger}}^i$ gate to their shares, taking shares of the logical quantum state $|\bar{\bar{+}}\rangle^i$ as the control shares and shares of the logical quantum state $|\bar{\bar{m}}\rangle^i$ as the target shares. Then, quantum nodes one more time transversally apply $\bar{\bar{H}}^i$ gate to the control shares and logically measure them in the standard basis. Finally, quantum nodes decode the result of the logical measurement twice and publicly check whether their twice decoded result corresponds to $|0\rangle^i$. In parallel, quantum nodes update a public set of apparent cheaters B. Note that the above procedure works if and only if the C-$XP^\dagger$ gate is transversal for a self-dual CSS QECC (see Sec. B for the criticism towards this claim).

Execution of the VCSS protocol requires a workspace of $4n$ qubits per quantum node. First, verification of the logical quantum state $|\bar{\bar{m}}\rangle^i$ requires a workspace of $3n$ qubits per quantum node. Second, after the verification of the logical quantum state $|\bar{\bar{m}}\rangle^i$, each quantum node requires a workspace of n qubits for holding this logical quantum state in addition to the extra workspace of $3n$ qubits for verification of the logical quantum state ${}_v|\bar{\bar{0}}\rangle^i$. Thus in total, each quantum node requires a workspace of $4n$ qubits for the execution of the VCSS protocol. The communication complexity of the VCSS protocol is the same as of the VHSS protocol, i.e., $O(nr^2)$ qubits per quantum node.

APPENDIX B: CRITICISM OF THE VCSS PROTOCOL

Here we describe two problems underlying the implementation of the VCSS protocol suggested in Ref. [6]. The authors of Ref. [6] claim that the magic state $|m\rangle$ is a $+1$ eigenstate of the $XP^\dagger$ gate while in reality, it is a $e^{i7\pi/4}$ eigenstate, see Ref. [47] for the calculations. This fact alone may cause some problems when applying a C-$XP^\dagger$ gate during the execution of the VCSS protocol, but the issue can be easily fixed by applying a C-$e^{i\pi/4}XP^\dagger$ gate instead, since $|m\rangle$ is indeed a $+1$ eigenstate of the $e^{i\pi/4}XP^\dagger$ gate. Furthermore, authors of the Ref. [6] claim that the VCSS protocol works as long as the C-$XP^\dagger$ gate can be implemented transversally. However, the C-$XP^\dagger$ gate is not transversal for the self-dual CSS QECCs. First of all, it is known to be impossible to implement an entire universal set of quantum gates transversally for any QECC [20]. Therefore, the C-$XP^\dagger$ gate needs to be a Clifford gate. Actually, C-$XP^\dagger$ gate can be easily decomposed as C-$XP^\dagger$ = C-$X \circ$ C-$P^\dagger$, which implies that the C-$P^\dagger$ gate is a Clifford gate. But the C-$P^\dagger$ gate is obviously not a Clifford gate and we attain a contradiction.

[15]For the self-dual CSS QECCs H gate is transversal.

APPENDIX C: OUTLINE OF THE MAGIC STATE VERIFICATION PROTOCOL

Here we briefly describe the protocol necessary for the verification of the ancillary logical magic state $|\bar{\bar{m}}\rangle^i$, i.e., whether it is certainly a logical magic state, in case of the reconsidered version of the MPQC protocol suggested in Ref. [16]. The protocol we describe here circumvents the questionable applicability of the VCSS protocol suggested in the original version of the MPQC protocol in Ref. [6]. The ambiguity in the VCSS protocol comes from the engagement of the C-$XP^\dagger$ gate, which is nontransversal in case of the self-dual CSS QECCs.

The protocol verifying the ancillary logical magic state $|\bar{\bar{m}}\rangle^i$ relies on a statistical testing of the randomly selected magic states $|m\rangle^i$, with the subsequent distillation of the logical magic states $|\bar{\bar{m}}\rangle^i$ via the distributed version of the 15-to-1 magic-state distillation protocol [48]. This approach increases the workspace required for the implementation of the MPQC protocol from $n^2 + 4n$ qubits per quantum node in the original suggestion [6] to $n^2 + \Theta(r)n$ qubits per quantum node in the reconsidered suggestion [16], where n is the number of the quantum nodes and r is the security parameter. Fortunately, the security proof does not change between the two versions of the MPQC protocol.

In short, the verification of the magic-state technique is performed as follows [16]: First of all, quantum nodes jointly prepare M copies of the verified by the VHSS protocol logical magic state $|\bar{\bar{m}}\rangle^i$, see Sec. IV A. Next, by using the public source of randomness, quantum nodes jointly select k out of M copies, and to perform the statistical testing of the randomly selected magic states, randomly ascribe some quantum node j to each selected copy. After that, each quantum node j collects all the single-qubit quantum states corresponding to the copy ascribed to him and by decoding it twice reconstructs a magic state $|m\rangle^i$, see Sec. IV A. Then, each quantum node j measures the reconstructed magic state in the $\{|m\rangle, |m^\perp\rangle\}$ basis and, if all the measurement results correspond to the magic state $|m\rangle^i$, then the quantum nodes can be sure that the remaining $M - k$ copies of the logical quantum state $|\bar{\bar{m}}\rangle^i$ in their possession is for sure an anticipated logical magic states with high probability. In parallel, quantum nodes update a public set of apparent cheaters B. After that, the dephasing procedure is performed, where, by using the public source of randomness, quantum nodes randomly apply the $\overline{\overline{PX}}^i$ gate to each of the remaining $M - k$ copies of the logical quantum state $|\bar{\bar{m}}\rangle^i$ in such a way that it brings them into the diagonal form in the $\{|m\rangle, |m^\perp\rangle\}$ basis, and subsequently randomly permute these $M - k$ copies of the logical quantum state $|\bar{\bar{m}}\rangle^i$. Finally, quantum nodes jointly perform the distillation of the logical magic state $|\bar{\bar{m}}\rangle^i$ by using the distributed version of the 15-to-1 magic-state distillation protocol [48] which can be implemented by combining the transversal quantum gates with the transversally implemented logical measurements in case of the self-dual CSS QECCs.

Execution of the above protocol requires a workspace of $(M + 2)n = \Theta(r)n$ qubits per quantum node, since during the verification of the magic-state quantum nodes should jointly prepare M copies of the verified by the VHSS protocol logical

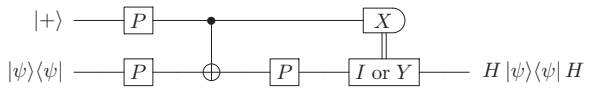

FIG. 6. The quantum circuit $\mathcal{T}$ in which the H gate is applied to the single-qubit quantum state $|\psi\rangle$ (alternatively $|\psi\rangle\langle\psi|$) with the gate teleportation technique by taking an advantage of the ancillary quantum state $|+\rangle$.

magic state $|\bar{\bar{m}}\rangle^i$. The communication complexity of the above protocol is $(Mr^2 + k)n = O(\Theta(r)nr^2)$ qubits per quantum node since in addition to the M executions of the VHSS protocol the verification of the magic-state technique requires a collection of the k randomly selected copies of the logical magic state $|\bar{\bar{m}}\rangle^i$.

APPENDIX D: DEFINITIONS OF THE QUANTUM GATES

We define single-qubit quantum gates used throughout the paper, i.e., X, Y, Z, H, P, and T gates, in a matrix form as follows:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{D1}$$

In addition, we define two-qubit quantum gates used throughout the paper, i.e., C-X and C-$P^\dagger$ gates, as follows:

$$\text{C-}X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \text{C-}P^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}. \tag{D2}$$

APPENDIX E: TELEPORTATION OF THE H GATE

Here we explicate the detailed calculations behind the teleportation of the H gate. For the sake of simplicity, let us consider the quantum circuit $\mathcal{T}$ which takes single-qubit quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (alternatively $|\psi\rangle\langle\psi|$) and ancillary quantum state $|+\rangle$ as an input, see Fig. 6. The calculations before the measurement in the Fourier basis are straightforward and the two-qubit result can be written in the matrix form as

$$|\phi\rangle = (\mathbb{I} \otimes P) \circ \text{C-}X \circ (P \otimes P) \circ (|+\rangle \otimes |\psi\rangle). \tag{E1}$$

Next, to implement the measurement in the Fourier basis, let us define the measurement operators as $|+\rangle\langle+| \otimes \mathbb{I}$ and $|-\rangle\langle-| \otimes \mathbb{I}$ for the two measurement outcomes which, by using the result in Eq. (E1), can be written as follows:

$$^{+}|\chi\rangle = \frac{(|+\rangle\langle+| \otimes \mathbb{I})}{\sqrt{\langle\phi|(|+\rangle\langle+| \otimes \mathbb{I})|\phi\rangle}}|\phi\rangle, \tag{E2}$$
$$^{-}|\chi\rangle = \frac{(|-\rangle\langle-| \otimes \mathbb{I})}{\sqrt{\langle\phi|(|-\rangle\langle-| \otimes \mathbb{I})|\phi\rangle}}|\phi\rangle, \tag{E3}$$

and if we write Eqs. (E2) and (E3) explicitly, the result will be

$$^{+}|\chi\rangle = |+\rangle(\alpha|-\rangle - \beta|+\rangle), \tag{E4}$$
$$^{-}|\chi\rangle = |-\rangle(\alpha|+\rangle + \beta|-\rangle). \tag{E5}$$

As one can observe, we obtain an anticipated result in the case of Eq. (E5), i.e., the H gate is definitely applied to the single-qubit input quantum state $|\psi\rangle$ (alternatively $|\psi\rangle\langle\psi|$). On the other hand, in the case of Eq. (E4) we do not obtain an anticipated result and an additional application of the $-iY$ gate is required. The result of the $-iY$ gate application can be explicitly written as

$$|+\rangle(\alpha|+\rangle + \beta|-\rangle) = (\mathbb{I} \otimes -iY) \circ (|+\rangle(\alpha|-\rangle - \beta|+\rangle)), \tag{E6}$$

and one can observe that we indeed obtain and anticipated result where the H gate is applied to the single-qubit input quantum state $|\psi\rangle$ (alternatively $|\psi\rangle\langle\psi|$).

[1] A. C. Yao, Protocols for secure computations (extended abstract), in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82 (IEEE Computer Society, New York, 1982), pp. 160–164.

[2] D. Evans, V. Kolesnikov, and M. Rosulek, A pragmatic introduction to secure multi-party computation, Found. Trends Priv. Secur. **2**, 70 (2018).

[3] C. Crépeau, D. Gottesman, and A. Smith, Secure multiparty quantum computation, in *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (ACM, New York, 2002), pp. 643–652.

[4] A. Smith, Multi-party quantum computation, arXiv:quant-ph/0111030.

[5] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith, Secure multiparty quantum computation with (only) a strict honest majority, in *47th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '06 (IEEE Computer Society, Berkeley, 2006), pp. 249–260.

[6] V. Lipinska, J. Ribeiro, and S. Wehner, Secure multiparty quantum computation with few qubits, Phys. Rev. A **102**, 022405 (2020).

[7] V. Goyal, C.-D. Liu-Zhang, J. Raizes, and J. Ribeiro, Asynchronous Multi-Party Quantum Computation, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023), Leibniz International Proceedings in Informatics (LIPIcs)* (Schloss Dagstuhl—Leibniz-Zentrum für Informatik, 2023), Vol. 251, pp. 62:1–62:22.

[8] F. Dupuis, J. B. Nielsen, and L. Salvail, Secure two-party quantum evaluation of unitaries against specious adversaries, in *Advances in Cryptology–CRYPTO 2010*, Lecture Notes in Computer Science, edited by T. Rabin (Springer, Berlin, Heidelberg, 2010), Vol. 6223, pp. 685–706.

[9] F. Dupuis, J. B. Nielsen, and L. Salvail, Actively secure two-party evaluation of any quantum operation, in *Advances in Cryptology–CRYPTO 2012*, Lecture Notes in Computer Science, edited by R. Safavi-Naini and R.

Canetti (Springer, Berlin, Heidelberg, 2012), Vol. 7417, pp. 794–811.

[10] Y. Dulek, A. B. Grilo, S. Jeffery, C. Majenz, and C. Schaffner, Secure multi-party quantum computation with a dishonest majority, in *Advances in Cryptology–EUROCRYPT 2020*, Lecture Notes in Computer Science, edited by A. Canteaut and Y. Ishai (Springer, Cham, 2020), Vol. 12107, pp. 729–758.

[11] B. Alon, H. Chung, K.-M. Chung, M.-Y. Huang, Y. Lee, and Y.-C. Shen, Round efficient secure multiparty quantum computation with identifiable abort, in *Advances in Cryptology–CRYPTO 2021*, Lecture Notes in Computer Science, edited by T. Malkin and C. Peikert (Springer, Cham, 2021), Vol. 12825, pp. 436–466.

[12] J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma, On the round complexity of secure quantum computation, in *Advances in Cryptology–CRYPTO 2021*, Lecture Notes in Computer Science, edited by T. Malkin and C. Peikert (Springer, Cham, 2021), Vol. 12825, pp. 406–435.

[13] K.-M. Chung, M.-Y. Huang, E.-C. Tang, and J. Zhang, Best-of-both-worlds multiparty quantum computation with publicly verifiable identifiable abort, Cryptology ePrint Archive, Paper 2022/1517 (2022), https://eprint.iacr.org/2022/1517.

[14] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A **55**, 900 (1997).

[15] R. Cleve, D. Gottesman, and H.-K. Lo, How to share a quantum secret, Phys. Rev. Lett. **83**, 648 (1999).

[16] V. Lipinska, J. Ribeiro, and S. Wehner, Erratum: Secure multiparty quantum computation with few qubits [Phys. Rev. A **102**, 022405 (2020)], Phys. Rev. A **110**, 019901(E) (2024).

[17] V. Lipinska, G. Murta, J. Ribeiro, and S. Wehner, Verifiable hybrid secret sharing with few qubits, Phys. Rev. A **101**, 032332 (2020).

[18] A. Steane, Multiple-particle interference and quantum error correction, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).

[19] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A **54**, 1098 (1996).

[20] B. Eastin and E. Knill, Restrictions on transversal encoded quantum gate sets, Phys. Rev. Lett. **102**, 110502 (2009).

[21] D. Gottesman and I. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature (London) **402**, 390 (1999).

[22] G. Nebe, E. M. Rains, and N. J. A. Sloane, The invariants of the Clifford groups, Des. Codes Cryptogr. **24**, 99 (2001).

[23] K. Betsumiya and A. Munemasa, On triply even binary codes, J. Lond. Math. Soc. **86**, 1 (2012).

[24] E. Knill, R. Laflamme, and W. Zurek, Threshold accuracy for quantum computation, arXiv:quant-ph/9610011.

[25] C. Chamberland and T. Jochym-O'Connor, Error suppression via complementary gauge choices in Reed-Muller codes, Quantum Sci. Technol. **2**, 035008 (2017).

[26] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, Multicast security: A taxonomy and some efficient constructions, in *IEEE INFOCOM '99 Conference on Computer Communications, Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, The Future is Now (Cat. No.99CH36320)* (IEEE, New York, 1999), Vol. 2, pp. 708–716.

[27] L. Lamport, R. Shostak, and M. Pease, The Byzantine generals problem, ACM Trans. Program. Lang. Syst. **4**, 382 (1982).

[28] M. Pease, R. Shostak, and L. Lamport, Reaching agreement in the presence of faults, J. Assoc. Comput. Mach. **27**, 228 (1980).

[29] M. Ben-Or, S. Goldwasser, and A. Wigderson, Completeness theorems for non-cryptographic fault-tolerant distributed computation, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, STOC '88 (Association for Computing Machinery, New York, 1988), pp. 1–10.

[30] D. Chaum, C. Crépeau, and I. Damgard, Multiparty unconditionally secure protocols, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, STOC '88 (Association for Computing Machinery, New York, 1988), pp. 11–19.

[31] R. Canetti, Universally composable signature, certification, and authentication, in *Proceedings of the 17th IEEE Computer Security Foundations Workshop, 2004* (IEEE, Pacific Grove, 2004), pp. 219–233.

[32] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, Authentication of quantum messages, in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002* (IEEE, Vancouver, BC, Canada, 2002), pp. 449–458.

[33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, 2011).

[34] J. Preskill, *Lecture Notes for Physics 219: Quantum Computation*, Lecture notes (California Institute of Technology, California, 1999).

[35] A. M. Steane, Active stabilization, quantum computation, and quantum state synthesis, Phys. Rev. Lett. **78**, 2252 (1997).

[36] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister, On optimality of CSS codes for transversal T, IEEE J. Sel. Areas Inf. Theory **1**, 499 (2020).

[37] S. Bravyi and J. Haah, Magic-state distillation with low overhead, Phys. Rev. A **86**, 052329 (2012).

[38] A. Paetznick, Resource optimization for fault-tolerant quantum computing, arXiv:1410.5124.

[39] S. Nezami and J. Haah, Classification of small triorthogonal codes, Phys. Rev. A **106**, 012437 (2022).

[40] D. Gottesman, An introduction to quantum error correction and fault-tolerant quantum computation, arXiv:0904.2557.

[41] D. Beaver, Foundations of secure interactive computing, in *Advances in Cryptology–CRYPTO '91*, edited by J. Feigenbaum (Springer, Berlin, Heidelberg, 1992), pp. 377–391.

[42] S. Micali and P. Rogaway, Secure computation, in *Advances in Cryptology–CRYPTO '91*, edited by J. Feigenbaum (Springer, Berlin, Heidelberg, 1992), pp. 392–404.

[43] R. Canetti, Universally composable security: A new paradigm for cryptographic protocols, in *Proceedings 42nd IEEE Symposium on Foundations of Computer Science* (IEEE, Newport Beach, 2001), pp. 136–145.

[44] D. Unruh, Universally composable quantum multi-party computation, in *Advances in Cryptology–EUROCRYPT 2010*, edited by H. Gilbert (Springer, Berlin, Heidelberg, 2010), pp. 486–505.

[45] D. Gottesman, Theory of fault-tolerant quantum computation, Phys. Rev. A **57**, 127 (1998).

[46] R. Cramer, I. B. Damgard, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*, 1st ed. (Cambridge University Press, New York, 2015).

[47] J. G. Hölting, On secret sharing-based classical and quantum multi-party computation, Master's thesis, Universiteit Utrecht, 2020, https://studenttheses.uu.nl/handle/20.500.12932/38635.

[48] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).