Verifiable hybrid secret sharing with few qubits

Lipinska, Victoria; Murta, Gláucia; Ribeiro, Jérémy; Wehner, Stephanie

DOI
10.1103/PhysRevA.101.032332

Publication date
2020

Document Version
Final published version

Published in
Physical Review A

Verifiable hybrid secret sharing with few qubits

Victoria Lipinska,[1,2,*] Gláucia Murta,[1,3,†] Jérémy Ribeiro,[1,2] and Stephanie Wehner[1,2]
[1]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[2]*Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[3]*Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany*

(Received 27 November 2019; accepted 5 February 2020; published 20 March 2020)

We consider the task of sharing a secret quantum state in a quantum network in a verifiable way. We propose a protocol that achieves this task, while reducing the number of required qubits, as compared to the existing protocols. To achieve this, we combine classical encryption of the quantum secret with an existing verifiable quantum secret sharing scheme based on Calderbank-Shor-Steane quantum error correcting codes. In this way we obtain a verifiable hybrid secret sharing scheme for sharing qubits, which combines the benefits of quantum and classical schemes. Our scheme does not reveal any information to any group of less than half of the n nodes participating in the protocol. Moreover, for sharing a one-qubit state each node needs a quantum memory to store n single-qubit shares, and requires a workspace of at most $3n$ qubits in total to verify the quantum secret. Importantly, in our scheme an individual share is encoded in a single qubit, as opposed to previous schemes requiring $\Omega(\log n)$ qubits per share. Furthermore, we define a ramp verifiable hybrid scheme. We give explicit examples of various verifiable hybrid schemes based on existing quantum error correcting codes.

DOI: 10.1103/PhysRevA.101.032332

I. INTRODUCTION

Secret sharing is a task which allows us to securely split a secret message among n network nodes, in such a way that at least a certain number of nodes is asked to collaborate in order to reconstruct the secret. However, one also requires that a subset with less than a certain number of nodes cannot gain any information about the secret. This way one can hide highly confidential and sensitive information from being exposed, for example missile launch codes or numbered bank accounts. The splitting and sharing of the message is often performed by one designated node—the dealer. If the nodes do not trust the dealer, but they want a guarantee that a secret was indeed distributed, then they may wish to verify that at the end of the protocol there will be one well-defined secret that they can reconstruct. In this case, the secret sharing protocol involves an additional step of verification of the shares, and one talks about *verifiable* secret sharing [1,2].

Importantly, verifiable secret sharing is used as a subroutine for other cryptographic primitives, such as secure multipartite computation [3,4], byzantine agreement [5], end-to-end auditable voting systems [6], and atomic broadcast [7]. Likewise, a quantum analog, namely verifiable quantum secret sharing (VQSS), is a core subroutine for secure multiparty quantum computation [8,9] and fast quantum byzantine agreement [10]. Verifiable schemes, similarly to their nonverifiable counterparts, have the property that they hide information from a certain number of nodes. That is, any subset with p or less nodes does not gain any information about the secret throughout the protocol. We call this property *secrecy*.

So far, many protocols have been proposed for sharing a classical secret using purely classical shares [11–13], using classical and quantum shares [14–17], as well as for sharing a quantum secret with quantum shares [14,18–22]. This work concerns the last variant, namely schemes which share a quantum secret. Particularly, throughout this paper we will consider that the dealer shares a pure single-qubit state $|\psi\rangle$. In this scenario, numerous schemes for both nonverifiable quantum secret sharing [14,18,19,21–23] and verifiable quantum secret sharing [8,24] are known. Fundamentally, for any scheme sharing a quantum secret with only quantum resources, there exists a limit to how many nodes p cannot gain any information about the secret. This limit is given by $p \leqslant \lfloor \frac{n-1}{2} \rfloor$ and can be intuitively understood as a consequence of the no-cloning theorem [25]. Indeed, if less than half of the nodes can reconstruct the secret, then there must exist at least two groups of nodes able to reconstruct it, which violates the no-cloning theorem. Moreover, if the majority of nodes recovers the secret exactly, then the remaining nodes get no information about the secret (for more details see [19]). We will refer to schemes which saturate the above bound on p as schemes with *maximum secrecy*. In particular, for VQSS with maximum secrecy, the only current construction [8] requires that the dimension q of local shares scales with the number of nodes $q > n$. Therefore, using the existing construction, we cannot find a nontrivial example of such a VQSS scheme where the nodes hold single-qubit shares. The reason for this scaling is that, in general, quantum secret sharing schemes are directly connected to resource-intensive quantum error correcting codes [18,19]. Consequently, this leads to

*v.lipinska@tudelft.nl
†glauciamg.fis@gmail.com

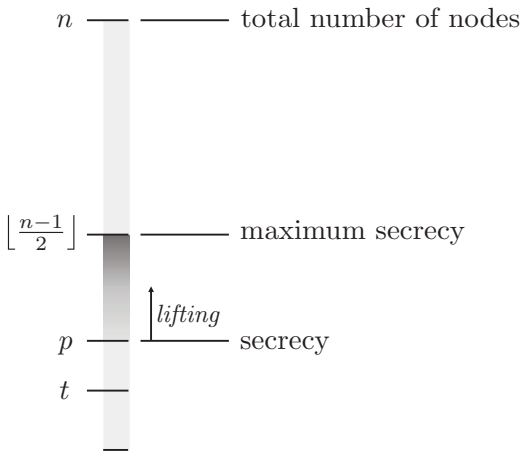

FIG. 1. Lifting the secrecy of an n-node secret sharing scheme of a quantum state, i.e., increasing the value p of nodes which gain no information about the secret state throughout the execution of the scheme. Here t denotes the number of nodes that can perform arbitrary operations on their shares throughout the protocol, and hence corrupt the secret (active cheaters).

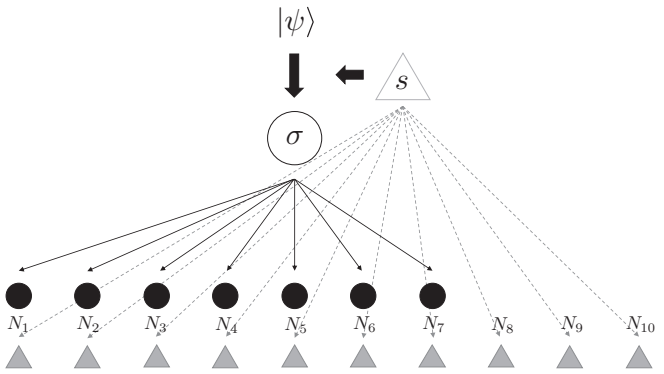

FIG. 2. A sketch of a verifiable hybrid secret sharing (VHSS) protocol for $n = 10$ nodes denoted $N_1, \ldots, N_{10}$, with $n_q = 7$ quantum (●) and $n_c = 10$ classical (▲) shares. The quantum secret state $|\psi\rangle$ of the dealer is encrypted using a classical key s. The resulting encrypted state σ and the key s are then distributed by the dealer as quantum and classical shares respectively.

secret sharing schemes which require $\Omega(\log n)$ of qubits per share.

In the area of nonverifiable quantum secret sharing, some investigations have been performed to reduce the number of required qubits, particularly, by exploring ramp secret sharing schemes [21,26] and classical encryption. In a ramp scheme one relaxes the constraint on the secrecy of the scheme, and therefore, allows some of the nodes to obtain partial information about the quantum state. This leads to schemes with less qubits per share. Additionally, the secrecy of a ramp scheme can be *lifted*, i.e., the value of p can be increased by encrypting the quantum state and then sharing the encryption key via classical secret sharing, see Fig. 1. Such a solution was dubbed hybrid secret sharing [27–30].

In early stages of quantum network development, it would be desirable to implement VQSS on a network with the ability to control only a small number of qubits. Since quantum resources are expensive, a lot of effort is being put in reducing them in many areas of a quantum information field, for example quantum computing or quantum simulation [31–35]. However, reducing the resource requirements in the domain of distributed systems, and in particular verifiable secret sharing, has not been considered so far. Here we address the question of whether a verifiable secret sharing scheme with the maximum secrecy property (i.e., $p = \lfloor \frac{n-1}{2} \rfloor$) can be realized on a quantum network with less qubits. We answer this question positively by presenting a scheme which reduces quantum resources necessary for sharing a quantum secret in a verifiable way.

II. RESULTS

Our contribution is threefold. First, our scheme realizes the task of verifiable secret sharing of a quantum state using a single qubit per share. Second, we show that the protocol can be realized in a setting where each node needs to store n qubits in a quantum memory and has a workspace of $3n$ qubits in total to verify the secret. For comparison, previous protocols [8,36] require shares with $\Omega(\log n)$ qubits and each node having simultaneous control over $\Omega[r^2 n \log(n)]$ qubits for verification, where r is the security parameter. Finally, our scheme preserves the maximum secrecy condition. This may enable qubit reductions for future implementations of cryptographic schemes, like multiparty computation or byzantine agreement, which use VQSS as a subroutine.

We extend the idea of a hybrid scheme to verifiable quantum secret sharing. Specifically, we present a protocol that achieves the task of sharing a single-qubit quantum state $|\psi\rangle$ in a verifiable way, where the dimension q of individual shares does not grow with the number of nodes n. In the spirit of [27–30], we make use of classical verifiable secret sharing [37,38] in order to obtain a verifiable hybrid scheme where each node holds at most $3n$ single-qubit shares at a time during the verification of the secret, see Outline below. Our scheme has a variety of consequences. Thanks to the classical encryption of the quantum state via a quantum one-time pad [39], our protocol can attain maximum secrecy, i.e., $p = \lfloor \frac{n-1}{2} \rfloor$. We show that by using a suitable classical scheme, one can beat the limit of maximum secrecy at the cost of tolerating less active cheaters (i.e., nodes that can perform arbitrary operations on their shares, see Adversary). Furthermore, motivated by nonverifiable schemes, we define the notion of strong threshold schemes in the context of verifiability, where any $p + 1$ nodes can reconstruct the secret, any p nodes do not gain any information about it, and t nodes can actively cheat in the protocol. We then show that according to our definition, it is impossible to construct a verifiable strong threshold scheme. Finally, we show how to achieve a ramp hybrid scheme allowing for sharing secrets in a verifiable way. The security proof of our protocol expands on the approach suggested in [8,36], see the Appendix for details.

Number of nodes. One key ingredient in our resource reduction is to combine quantum and classical resources in a hybrid scheme. In our model, some nodes hold quantum shares and some nodes hold classical shares. Note that nodes can have both quantum and classical shares, see Fig. 2. We

denote the number of nodes with classical shares and the nodes with quantum shares by n_c and n_q, respectively, and by n the total number of nodes.

Adversary. We allow for the existence of t malicious nodes (cheaters) in the protocol. We say that those cheaters are *active*, meaning that they can perform arbitrary joint operations on their state during the execution of the protocol, in order to learn $|\psi\rangle$. We say that a protocol *tolerates* t active cheaters if at the end of the protocol the reconstruction of the quantum state is possible despite the presence of those cheaters. The nodes who follow the protocol exactly are called honest. We follow the common assumption that the set of malicious quantum and classical nodes is determined at the beginning of the hybrid protocol and stays fixed throughout (*nonadaptive* adversary). We also assume that all nodes have access to an authenticated broadcast channel [40] and that each pair of nodes is connected by authenticated, private classical [41], and quantum [42] channels.

Definition 1 ($\{p,t,n\}$- VHSS). A $\{p,t,n\}$-VHSS verifiable hybrid secret sharing scheme is an n-node protocol with three phases: sharing, verification, and reconstruction, and two designated players, dealer D and reconstructor R. In the sharing phase D shares a pure single-qubit quantum state $|\psi\rangle$ using quantum and classical shares. In the verification phase all of the nodes verify that the set of shares defines a unique quantum state. In the reconstruction phase R receives all shares from all nodes, and reconstructs the unique state defined by these shares. We require that the scheme satisfies the following requirements despite the presence of t nonadaptive active cheaters, except with probability exponentially small in the security parameter r:

(1) Soundness: if R is honest and D passes the verification phase, then there is a unique state $|\psi\rangle$ that can be recovered by R.

(2) Completeness: if D is honest, then she always passes the verification phase. Moreover, if R is also honest, then the reconstructed state is exactly D's state $|\psi\rangle$.

(3) Secrecy: if D is honest, then any group of $p \geqslant t$ nodes cannot gain any information about the secret before reconstruction.

The parameters of the scheme are determined by an underlying quantum error correcting code which we use as a building block. In particular, a relevant variable is the distance d of the code. We remark that our results generalize to multiqubit scenarios.

A. $\{p,t,n\}$-VHSS verifiable hybrid secret sharing protocol

Outline of the verifiable hybrid secret sharing (VHSS) protocol (see Protocol 1).

1. *Sharing*

The dealer D encrypts the secret quantum state $|\psi\rangle$ using a classical key $s = ab$ and quantum one-time pad [39],

$$\sigma_{QS} = \sum_{ab=\{0,1\}^2} \frac{1}{4} X^a Z^b |\psi\rangle\langle\psi|_Q Z^b X^a \otimes |ab\rangle\langle ab|_S,$$

where Q is the quantum register of the dealer and S is the classical register of the encryption key. She shares the encrypted state among the nodes using the quantum protocol and the key s using the classical protocol, see Protocol 1 "Sharing."

2. *Verification*

Nodes verify whether D is honest, i.e., that the shares held by the nodes are consistent and at the end of the protocol a state will be reconstructed. For this, each node encodes the qubit received from the dealer into further n qubits and sends $n-1$ of them to other nodes. Then, each node uses at most additional $2n$ ancilla qubits for one iteration of the verification procedure. There are $O(r^2)$ iterations of verification, where r is the security parameter. If the dealer passes the verification phase the protocol continues. Otherwise it aborts.

3. *Reconstruction*

One designated node R collects all shares of σ and reconstructs it. She also reconstructs the classical key s and decrypts $|\psi\rangle$.

Remark. Throughout the protocol each of the nodes needs to simultaneously store n single-qubit shares corresponding to the encoded secret state. In the verification phase each node creates at most $2n$ ancilla qubits, performs a joint operation between these ancillas and the shares of the secret, and then measures only the ancilla qubits. This means that the nodes require a workspace of at most $3n$ qubits in total for verification.

We revisit the VQSS scheme introduced in [8] and explore its extension to a verifiable scheme which uses single-qubit shares. The construction we use is based on Calderbank-Shor-Steane (CSS) error correcting codes [45,46]. Then we use the existing verifiable classical secret sharing schemes [37,38] to combine classical encryption of the quantum secret with the VQSS scheme to achieve an n-node verifiable hybrid secret sharing scheme (VHSS), see Outline. In $\{p,t,n\}$-VHSS the number p of nodes who cannot gain any information about the quantum state is determined by the classical scheme. Moreover, $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ cheaters are active and constrained by the distance d of the underlying CSS code. In our scheme the secret state of the dealer $|\psi\rangle$ is encrypted using quantum one-time pad with a classical key s, and then both objects are shared and verified in parallel. It is, therefore, impossible to reconstruct the quantum secret without reconstructing the classical key. In the case when $n = n_q = n_c$ we achieve the following functionalities:

(1) We construct a scheme which attains maximum secrecy using single qubit shares. Specifically, thanks to using classical encryption, we show that in our $\{p,t,n\}$-VHSS scheme any $p \leqslant \lfloor \frac{n-1}{2} \rfloor$ nodes coming together before reconstructing the secret do not gain any information about it. Our $\{p,t,n\}$-VHSS scheme tolerates up to $t < \frac{n}{4}$ active cheaters. Reconstruction of the secret occurs with all of the shares.

TABLE I. Examples of verifiable hybrid secret sharing schemes using one qubit shares coming from this work. The secret is shared among n nodes. A $\{\lfloor\frac{n-1}{2}\rfloor, t, n\}$-VHSS scheme uses shares from all of the nodes to reconstruct the secret, whereas $\{\lfloor\frac{n-1}{2}\rfloor, t, t', n\}$-ramp VHSS scheme can reconstruct the secret without any t' nodes. Both schemes tolerate t active cheaters and are based on error correcting codes of [43,44].

	$\{\lfloor\frac{n-1}{2}\rfloor, t, n\}$-VHSS		$\{\lfloor\frac{n-1}{2}\rfloor, t, t', n\}$-ramp VHSS	
Number of nodes n	$t=2$	$t=4$	$t=1$	$t=2$
$2(t+1)^2$	{8, 2, 18}	{24, 4, 50}	{8, 1, 1, 18}	{24, 2, 2, 50}
$3t^2+3t+1$	{9, 2, 19}	{30, 4, 61}	{9, 1, 1, 19}	{30, 2, 2, 61}
$6t^2+1$	{12, 2, 25}	{48, 4, 97}	{12, 1, 1, 25}	{48, 2, 2, 97}
$8t^2+4t+1$	{20, 2, 41}	{72, 4, 145}	{20, 1, 1, 41}	{72, 2, 2, 145}

(2) We show how to achieve a $\{p, t, n\}$-VHSS scheme for $p > \lfloor\frac{n-1}{2}\rfloor$ by choosing an appropriate classical verifiable scheme [38]. In this case, however, there exists a trade-off between the number of active cheaters and secrecy, such that $n \geqslant p + 3t + 1$. Therefore, in order to achieve higher secrecy we tolerate less active cheaters t. As before, reconstruction of the secret occurs with all of the shares.

(3) We define a strong threshold scheme (see Definition 2) where shares from any group of $n - t'$ nodes are sufficient for the reconstruction, and no group of $p = n - t' - 1$ nodes gains any information about the state. Importantly, we show that according to our definition, it is impossible to achieve a verifiable strong threshold scheme, namely, a scheme which satisfies the two above constraints and tolerates t active cheaters at the same time.

(4) We relax the secrecy constraint of the strong threshold scheme and construct a ramp VHSS scheme (see Definition 3). In our ramp verifiable scheme any $n - t'$ nodes can reconstruct the secret, but any group of at most $p \leqslant \lfloor\frac{n-1}{2}\rfloor$ does not have any information about it. The scheme tolerates t active cheaters, where $t + t' \leqslant \lfloor\frac{d-1}{2}\rfloor$ are constrained by the distance of the underlying quantum error correcting code. We denote it with $\{p, t, t', n\}$-ramp VHSS.

In the case when $n = n_c > n_q$, our VHSS scheme allows us to construct a scheme which extends verifiable quantum secret sharing onto nodes with purely classical capabilities, see Fig. 2. That is, we use VQSS to share a quantum secret with n_q nodes, but we extend the sharing of the classical key s onto $n_c > n_q$ nodes. Therefore, some of the nodes hold only classical shares but still participate in hiding of the quantum secret. Due to the properties of our protocol, this scheme can also lift the secrecy, such that no set with $p \leqslant \lfloor\frac{n-1}{2}\rfloor$ nodes can learn the quantum state before the reconstruction.

B. Implications for resource reduction

Our scheme allows us to exploit CSS quantum error correcting codes which encode a single-qubit quantum state into single-qubit shares. Such codes are well studied in the literature and therefore, numerous schemes with defined encoding and decoding exist [43,44]. In the next section we present examples of VHSS schemes based on such codes. We remark that one could use approximate error correction codes and in this way increase the number of active cheaters to $2t$ [24,42]. However, this solution requires significantly more resources, see Sec. V.

III. RESOURCE REDUCTION

Our protocol reduces the number of qubits that need to be controlled simultaneously by each node. To do so, we adapt the protocol of [8], where the verification procedure requires ancillas used in parallel, to a setting where they can be used sequentially, i.e., one by one. This way, each node needs control over $3n$ operational qubits at a time. For comparison, the parallel execution of [8] requires simultaneous control over $\Omega[r^2 n \log(n)]$ qubits per node, where r is the security parameter.

Here we list a few examples of CSS codes leading to VHSS schemes with single-qubit shares (also see Table I). We express our examples in terms of a maximum tolerable number of active cheaters t. Note that for a particular code there exists a trade-off between the number of active cheaters and the total number of nodes.

For $t = 1$:

(1) $\{3, 1, 7\}$-VHSS. In this scheme $n = n_c = n_q = 7$ nodes hold both quantum and classical shares. The scheme achieves maximum secrecy, i.e., no group of $p = \lfloor\frac{7-1}{2}\rfloor = 3$ shares acquires any information about the secret. All of the quantum shares are single-qubit shares, and each node requires control over 21 qubits at a time for the verification procedure. This example is based on the Steane's $[[7, 1, 3]]_2$ code, encoding 1 qubit into 7 qubits, with distance $d = 3$ [46]. In this scheme all shares are necessary to reconstruct the secret.

Note that the Steane's code without the classical encryption would generate a VQSS scheme, where no two nodes could gain any information about the secret. However, due to the properties of the code, a *specific* group of three nodes could still reconstruct the secret. To compare, the existing construction to achieve a purely quantum scheme with maximum secrecy, requires individual shares of dimension $q > 7$.

(2) $\{\lfloor\frac{n-1}{2}\rfloor, 1, n\}$-VHSS. In this scheme $n_q = 7$ out of n nodes hold quantum single-qubit shares and $n = n_c > 7$ hold classical shares. The scheme achieves maximum secrecy. For the construction we use the Steane's $[[7, 1, 3]]_2$ code and a classical scheme of [37]. Therefore, in our scheme only seven nodes need to have quantum resources, but all of the n nodes can participate in verifiable secret sharing of a quantum state.

For $t \geqslant 1$:

(1) $\{\lfloor\frac{n-1}{2}\rfloor, t, n\}$-VHSS. We construct VHSS schemes which tolerate more than one active cheater and achieve maximum secrecy. All of the nodes hold both quantum and classical shares ($n_q = n_c = n$), and the quantum shares contain a single

qubit. For the construction we use higher-distance quantum error correcting codes, for example toric codes and color codes [43,44], and VCSS scheme of [37]. We present specific examples in Table I. Note that each of those schemes can be expanded onto even larger total number of nodes, by using a verifiable classical secret sharing scheme with $n_c > n_q$.

(2) $\{p, t, t', n\}$-ramp VHSS. Based on the same higher-distance quantum error correcting codes [43,44], we construct examples of ramp schemes, see Table I. All of the nodes hold quantum and classical shares, however, only $n - t'$ are used to reconstruct the secret.

IV. METHODS

A. Protocol

Our protocol is a hybrid between a classical scheme (VCSS) and a quantum scheme (VQSS) to share the classical key s and the encrypted quantum state σ_{QS}, respectively. In the following we summarize the principles of these two protocols.

1. Verifiable classical secret sharing

A verifiable classical secret sharing scheme is a scheme which shares a classical secret of the dealer among n_c nodes in a verifiable way, using classical shares. The scheme is such that p_c nodes cannot gain any information about the classical secret after coming together (secrecy) and there are at most t_c active nonadaptive cheating nodes that the scheme tolerates. We represent the classical verifiable secret sharing protocol with a triple (p_c, t_c, n_c)-VCSS. Here we treat the VCSS scheme as a secure black box which leaks no information about the classical key s, even if the adversary has access to quantum side information during the execution of VCSS. VCSS schemes that are information theoretically secure in the context of classical adversary have been presented in for example [3,37,38]. Here we add it as an assumption that any VCSS protocol used to build Protocol 1 is secure against a quantum adversary in the information-theoretic sense.

Assumption 1. The VCSS scheme used to build Protocol 1 does not leak any information about the secret key s to any set of p_c nodes, except with probability exponentially small in the security parameter r, even in the presence of quantum side information. That is, the scheme is information theoretically secure in the presence of a quantum adversary.

Formally, VCSS is a classical protocol in which the dealer inputs a classical message s, which is shared among the nodes. Let P be a set of size at most p_c, and let $\mathcal{Q}_P$ denote any quantum side information held by the nodes in set P at the end of the verification phase of the VHSS. In principle, $\mathcal{Q}_P$ could be arbitrarily correlated with the classical secret key s. However, Assumption 1 implies that the state held by nodes in P carries no information about the key s, other than what was known prior to the beginning of the protocol.

To the best of our knowledge, security of protocols of [3,38] against an adversary with quantum side information was never formalized. We note that in Theorem 13 of [47] it was proven that any classical protocol which is statistically secure in a universal composable (UC) sense, is also statistically UC secure against a quantum adversary. Furthermore, [48,49] discuss the possibility of strengthening the security of [37] to UC security. As a consequence [37] could be conjectured statistically UC secure against a quantum adversary.

In what follows, unless specified otherwise, we will consider a classical VCSS protocol of [37]. This scheme is secure with exponentially small probability of error $2^{-\Omega(r')}$, where r' is the security parameter. Here, for convenience, we choose r' such that $r' = r$, where r is the security parameter of VHSS. The protocol can tolerate up to $t_c < \frac{n_c}{2}$ malicious nodes. In particular, it also implies that $p_c = t_c < \frac{n_c}{2}$.

2. Verifiable quantum secret sharing

To construct our hybrid scheme we employ a VQSS scheme which uses single-qubit shares. The VQSS scheme summarized here is based on the results of [8].

A verifiable quantum secret sharing scheme is a scheme which shares a quantum state of the dealer among n_q nodes in a verifiable way, using quantum shares. The scheme is such that p_q nodes cannot gain any information about the secret (secrecy) and there are at most t_q nonadaptive active cheating nodes that the scheme tolerates. We denote such a scheme with a triple (p_q, t_q, n_q)-VQSS. To share a pure qubit state among n_q nodes in a VQSS, the nodes agree on (an efficiently decodable) $[[n_q, 1, d]]_2$ Calderbank-Shor-Steane (CSS) error correcting code $\mathcal{C}$. Such a code encodes 1 qubit into n_q qubits and has distance d. This means that the chosen CSS code is able to correct $t_q \leqslant \lfloor \frac{d-1}{2} \rfloor$ arbitrary errors and $p_q \leqslant d - 1$ erasure errors.

The CSS code $\mathcal{C}$ used to perform the protocol is defined through two binary classical linear codes V and W, satisfying $V^* \subseteq W$, where V^* is the dual code. Then, $\mathcal{C} = V \cap \mathcal{F}W$ is a set of states of n_q qubits which yield a codeword in V when measured in the standard basis, and a codeword in W when measured in the Fourier basis [50]. An important property of a CSS code, which is useful for the VQSS protocol, is the fact that certain logical operations $\bar{\Lambda}$ can be implemented by applying local operations Λ on the individual qubits held by the nodes and encoded with $\mathcal{C}$, i.e., $\bar{\Lambda} = \Lambda^{\otimes n_q}$. This property, called transversality, means that specific logical operations can be applied qubit-wise. In particular, the protocol uses the fact that (i) applying a CNOT gate is tranversal; (ii) applying the Fourier transform qubit-wise maps codewords of the code $\mathcal{C}$ onto codewords of the dual code $\tilde{\mathcal{C}}$; and (iii) measurements can be performed qubit-wise, but measurement outcome of every qubit must be communicated classically to obtain the result of the logical measurement.

In the VQSS protocol the dealer D encodes the quantum secret state $|\psi\rangle$ using the code $\mathcal{C}$ and distributes it to n_q nodes. Next, each node i encodes her qubit into n_q further qubits and distributes those to every other node, see Fig. 3. This way the nodes create two levels of encoding which can be represented as a tree. The second level of encoding gives each node some control over all the other shares, which allows honest nodes to check consistency of all the shares.

The protocol aims to verify whether the shares (the tree) create a codeword for which decoding is well defined with respect to the code $\mathcal{C}$, without revealing any information about the secret state of the dealer. This property is formally defined in [8,36] and is dubbed 2-GOOD. Intuitively, a 2-GOOD$_V$ tree means that for all branches of the tree which are held

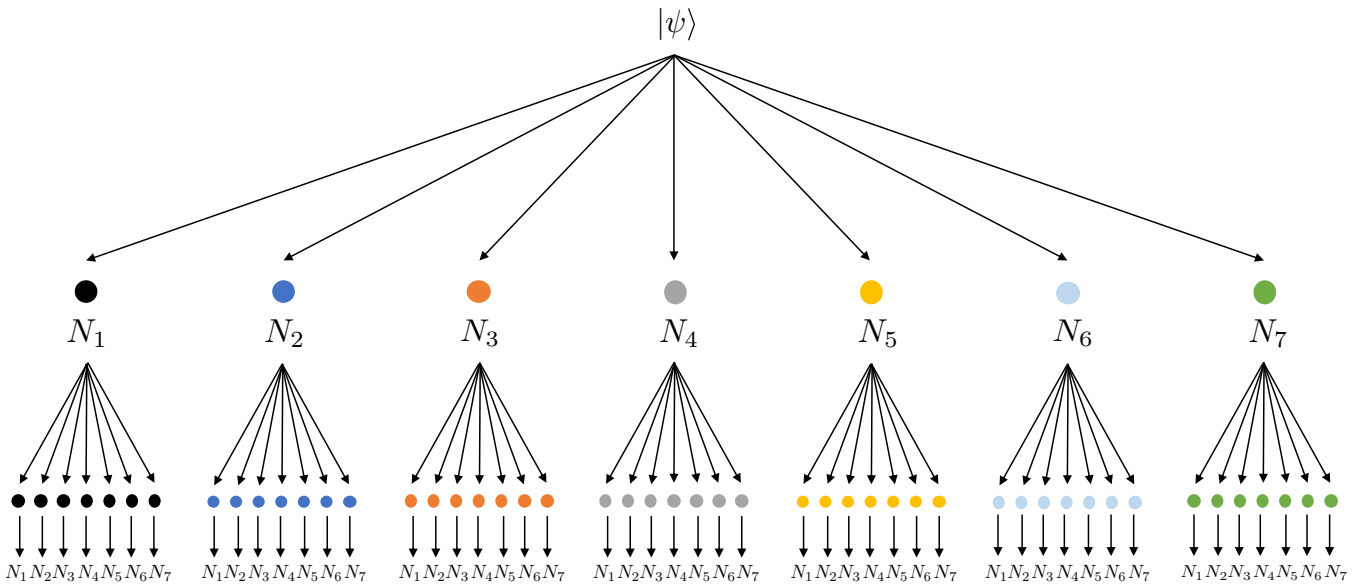

FIG. 3. The encoding tree for (2,1,7)-VQSS protocol with seven nodes $N_1, \ldots, N_7$, based on the Steane's $[[7, 1, 3]]_2$ code. The figure represents the encoding done in the sharing phase by each of the nodes.

by honest nodes, upon measuring their shares of the tree, there exists a unique codeword in the code V that can be recovered. Since $\mathcal{C} = V \cap \mathcal{F}W$, to verify that the encoded tree is 2-GOOD$_{\mathcal{C}}$, the verification procedure first verifies that the tree is 2-GOOD$_V$ when measured in the standard basis, and then that it is 2-GOOD$_W$ when measured in the Fourier basis.

We adapt the verification procedure from the work of [8,36] to run in a sequential way. In our procedure, to verify that the encoded secret is 2-GOOD$_V$ in the standard basis, the dealer and the nodes create auxiliary trees initiated in a logical $|\bar{+}\rangle$ state of the code $\mathcal{C}$. Importantly, these systems are distributed one at a time. Therefore, each node needs to control $2n$ qubits at a time: n single-qubit shares for the encoded secret state, and n single-qubit shares for the auxiliary $|\bar{+}\rangle$ state. We perform r such checks, where r is the security parameter.

After this step, our protocol verifies that the encoded secret is 2-GOOD$_W$ in the Fourier basis. To do so, the dealer and the nodes create new auxiliary trees initiated in a logical $|\bar{0}\rangle$ state of the code $\mathcal{C}$. Here an important difference is that each of the auxiliary $|\bar{0}\rangle$ states is first verified to be 2-GOOD$_V$ as well, before applying the Fourier transform. This step is necessary, because one wants to make sure that the check in the Fourier basis does not introduce bit flips in the standard basis (at this point the check in standard basis for the secret state $|\psi\rangle$ has already been performed). Verifying each $|\bar{0}\rangle$ requires using extra n single-qubit shares per node and is repeated r times. Therefore, each node needs to control $3n$ qubits at this step: n single-qubit shares for the encoded secret, n single-qubit shares for a $|\bar{0}\rangle$ state, and additional n single-qubit shares for the verification of $|\bar{0}\rangle$. In comparison, in [8,36] all of the above steps are performed in parallel, and effectively, each node needs to control $\Omega[r^2 n \log(n)]$ at once.

In the verification phase the nodes publicly identify a set of *apparent* cheaters B with probability exponentially close to 1 in the security parameter r. Set B includes all of the errors introduced by the dealer and errors introduced by the cheating nodes until the end of the verification phase. Note that there is no way to distinguish the errors introduced by the dealer and those introduced by the cheaters at this point. The dealer will pass verification as "honest" if $|B| \leqslant t_q$. On the other hand, if $|B| \geqslant t_q$, then the protocol aborts.

After the verification phase, the cheating nodes can still corrupt their shares. Therefore, the reconstructor R runs an error correction circuit and measures syndromes, so that she can correct arbitrarily located errors introduced by the cheaters after the verification. If for a branch encoded by a particular node i there have been more than t_q errors, then R adds that node to the set B of cheaters. Otherwise, R corrects errors and reconstructs branch i. After reconstructing all branches, she randomly picks $n - 2t_q$ shares which she has left, and reconstructs the state of the dealer. Importantly, the size of set B cannot be larger than $2t_q$ at the end of the protocol. This is because the dealer D and cheaters can introduce at most t_q errors at the first level of encoding before verification (otherwise the protocol aborts). Before the reconstruction, the cheaters may introduce up to t_q extra errors at the second level of each branch they hold. This may create extra errors at the first level, but never more than t_q, since the cheaters have some control over at most t_q branches.

What is more, let $C_{\texttt{VQSS}}$ be the set of cheaters in the VQSS and $C_{\texttt{VCSS}}$ the set of cheaters in VCSS. We assume that if a node behaves maliciously in VQSS, it can also behave maliciously in VCSS, and moreover $C_{\texttt{VQSS}} = C_{\texttt{VCSS}}$. Therefore, we put $t = t_c = t_q$. Moreover, in our VHSS protocol we assume that the nodes have access to shared public source of randomness. This can be realized, for example, by running a classical verifiable secret sharing protocol or multipartite coin flipping. We remark that [36] points out solutions to reduce the classical communication complexity of generating public randomness. In the following we will write $[1, n]$ to denote registers of nodes from 1 to n.

Protocol 1: Verifiable Hybrid Secret Sharing (VHSS)

Input: a qubit secret system $|\psi\rangle$ to share, CSS error correcting code $\mathcal{C} = V \cap \mathcal{F}W$.

SHARING

Encryption

1. The dealer D encrypts her secret state $|\psi\rangle$ using quantum one-time pad with a classical key s, creating the state σ_{QS}, see Eq. (5).
2. D shares the classical key s among n nodes using a verifiable classical secret sharing VCSS protocol.

Encoding

1. D encodes σ_Q using $\mathcal{C}$ into $\Phi^{0,0}_{[1,n_q]}$, where σ_Q is the reduced state of σ_{QS}.
2. for $i = 1, \ldots, n_q$:
   D sends $\Phi^{0,0}_i$ to node i.
   Each node i encodes received systems using $\mathcal{C}$ into $\Phi^{0,0}_{i_{[1,n_q]}}$ and sends jth component $\Phi^{0,0}_{i_j}$ to node j.

VERIFICATION

Z basis

for $\ell = 0, m = 1, \ldots, r$:

1. D prepares $|\bar{+}\rangle^{0,m}_{[1,n_q]} = \sum_{v\in V} |v\rangle$ using $\mathcal{C}$.
2. for $i = 1, \ldots, n_q$:
   D sends $|\bar{+}\rangle^{0,m}_i$ to node i.
   Each node i encodes received systems using $\mathcal{C}$ into $|\bar{+}\rangle^{0,m}_{i_{[1,n_q]}}$ and sends jth component $|\bar{+}\rangle^{0,m}_{i_j}$ to node j.
3. Nodes use shared public randomness source and get public random value $b_{0,m} \in_R \{0, 1\}$. Each node j:
   (a) applies the controlled NOT (CNOT) gate to her shares depending on the value of $b_{0,m}$ ($\text{CNOT}^{b_{0,m}}$). That is, for every qubit i, if $b_{0,m} = 0$ the node does nothing, and if $b_{0,m} = 1$ the node applies a CNOT gate with a qubit indexed by $m = 0$ as a control to a qubit indexed by $m = 1, \ldots, r$ as a target:
   $$\forall i = 1, \ldots, n_q : \quad \text{CNOT}^{b_{0,m}}\left(\Phi^{0,0}_{i_j}, |\bar{+}\rangle^{0,m}_{i_j}\right)$$
   (b) measures all systems indexed $\ell = 0,\ m = 1, \ldots, r$ in the Z basis and broadcasts the result of the measurement.

X basis

for $\ell = 1, \ldots, r$:

4. D prepares $|\bar{0}\rangle^{\ell,0}_{[1,n_q]} = \sum_{w\in W^\perp} |w\rangle$ using $\mathcal{C}$.
5. for $i = 1, \ldots, n_q$:
   D sends $|\bar{0}\rangle^{\ell,0}_i$ to node i.
   Each node i encodes received systems using $\mathcal{C}$ into $|\bar{0}\rangle^{\ell,0}_{i_{[1,n_q]}}$ and sends jth component $|\bar{0}\rangle^{\ell,0}_{i_j}$ to node j.
   for $m = 1, \ldots, r$:
6. D prepares $|\bar{0}\rangle^{\ell,m}_{[1,n_q]} = \sum_{w\in W^\perp} |w\rangle$ using $\mathcal{C}$.
7. for all $i = 1, \ldots, n_q$:
   D sends $|\bar{0}\rangle^{\ell,m}_i$ to node i.
   Each node i encodes received systems using $\mathcal{C}$ into $|\bar{0}\rangle^{\ell,m}_{i_{[1,n_q]}}$ and sends jth component $|\bar{0}\rangle^{\ell,m}_{i_j}$ to node j.
8. Nodes use shared public randomness source and get public random values $b_{\ell,m} \in_R \{0, 1\}$. Each node j:
   (a) applies the CNOT gate to her shares depending on the value of $b_{\ell,m}$ ($\text{CNOT}^{b_{\ell,m}}$):
   $$\forall i = 1, \ldots, n_q : \quad \text{CNOT}^{b_{\ell,m}}\left(|\bar{0}\rangle^{\ell,0}_{i_j}, |\bar{0}\rangle^{\ell,m}_{i_j}\right)$$
   (b) measures the mth system in the Z basis and broadcasts the result of the measurement.
9. Nodes apply the Fourier transform $\mathcal{F}$ to all of their remaining shares, resulting in $\Phi^{\mathcal{F}0,0}_{[1,n_q]_j}$ and $|\bar{0}^{\mathcal{F}}\rangle^{\ell,m}_{[1,n_q]_j}$ for each node j. Note that $|\bar{0}^{\mathcal{F}}\rangle = \sum_{w\in W} |w\rangle$.
10. Nodes use shared public randomness source and get public random values $b_{\ell,0} \in_R \{0, 1\}$. Each node j:
    (a) applies the CNOT gate to her shares depending on the value of $b_{\ell,0}$ ($\text{CNOT}^{b_{\ell,0}}$):
    $$\forall i = 1, \ldots, n_q : \quad \text{CNOT}^{b_{\ell,0}}\left(\Phi^{\mathcal{F}0,0}_{i_j}, |\bar{0}^{\mathcal{F}}\rangle^{\ell,0}_{i_j}\right)$$
    (b) measures ℓth system in the Z basis and broadcasts the result of the measurement.

11. (Decoding leaves Z basis) Broadcasted values in steps 3(b) and 8(b) yield words $\mathbf{v}_{\ell,m,i}$ from code V, corresponding to the second level of shares encoded by each node i. For each of the words, using classical decoding, the nodes:
    (a) obtain a decoded value $a_{\ell,m,i}$
    (b) publicly check on which positions the errors have occurred, denote these positions by $B_{\ell,m,i}$. Nodes update sets $B_i = \cup_{\ell,m} B_{\ell,m,i}$ from the positions of errors which occurred in the systems encoded by node i. If $|B_i| > t$ then add i to a global set B.
12. (Decoding the root Z basis) The nodes arrange values $a_{\ell,m,i}$ into $\mathbf{a}_{\ell,m} = \{a_{\ell,m,1}, \ldots, a_{\ell,m,n_q}\}$. Word $\mathbf{a}_{\ell,m}$ yields a classical codeword from the code V and the nodes decode it using classical decoder of code V. They add the positions on which an error occurred to the global set B.
13. (Decoding leaves X basis) Broadcasted values in step 10(b) yield words $\mathbf{w}_{\ell,0,i}$ from code W, corresponding to the second level of shares encoded by each node i. For each of the words, using classical decoding, the nodes:
    (a) obtain a decoded value $a_{\ell,0,i}$
    (b) publicly check on which positions the errors have occurred, and update sets B_i and B as before. Sets B_i and B are cumulative throughout the protocol.
14. (Decoding the root X basis) Nodes create a codeword $\mathbf{a}_{\ell,0} = \{a_{\ell,0,1}, \ldots, a_{\ell,0,n_q}\}$ and decode it using classical decoder of code W. They add the positions on which an error occurred to the global set B. If $|B| > t$ then reject the dealer and abort. Otherwise continue.
15. Nodes apply an inverse Fourier transform $\mathcal{F}^{-1}$ to their remaining system and obtain global sharing of D secret, i.e., each node j holds $\Phi^{0,0}_{[1,n_q]_j}$.

RECONSTRUCTION

1. Each quantum node $j = 1, \ldots, n_q$ sends their shares to the reconstructor R. Moreover, all of the n_c classical nodes send their classical shares to R.
2. R reconstructs the classical secret key s using a decoder of VCSS.
3. For each share $\Phi^{0,0}_{i_{[1,n]}}$ coming from encoding of node $i \notin B$, R runs a circuit for code $\mathcal{C}$ which identifies errors. R creates a set $\tilde{B}_i$ such that it contains B_i, $B_i \subseteq \tilde{B}_i$. If $|\tilde{B}_i| \leqslant t$ then errors are correctable, R corrects them and decodes the ith share, obtaining $\Phi^{0,0}_i$. Otherwise, R adds i to the global set B.
4. For all $i \notin B$, R randomly chooses $n_q - 2t$ shares $\Phi^{0,0}_i$ and applies an erasure-recovery circuit to them. R obtains σ_R.
5. R decrypts σ_R using the classical key s and obtains $|\psi\rangle$.

B. Security

As discussed in previous sections, in the task of verifiable secret sharing we want to ensure that the dealer is honest and that at the end of the protocol there will be a well-defined state to be reconstructed. In this section we prove the security of Protocol 1 against t nonadaptive active cheaters. First we state useful lemmas about the security of the VQSS protocol of [8], which we use as a subroutine. For a detailed discussion we refer the reader to [36]. We remark that we use an adapted version of VQSS in the setting where we run the verification phase sequentially, i.e., one ancilla at a time, whereas in [8] the verification is performed in a parallel setting, i.e., all ancillas together. In the Appendix we prove that this fact does not change security statements of the original VQSS.

Lemma 1 (soundness of VQSS*).* In the verifiable quantum secret sharing protocol [8], either the honest parties hold a consistently encoded secret or dealer is caught and the protocol aborts with probability at least $1 - 2^{-\Omega(r)}$ [see Eq. (A26) in the Appendix].

Lemma 2 (completeness of VQSS*).* In the verifiable quantum secret sharing protocol [8], if D is honest then she passes the verification phase. Moreover, if R is also honest she reconstructs D's secret with probability at least $1 - 2^{-\Omega(r)}$, where r is the security parameter [see Eq. (A27) in the Appendix].

Using the above lemmas we now show that our VHSS protocol, Protocol 1, is sound and complete.

Theorem 1 (soundness). In the verifiable hybrid secret sharing protocol, Protocol 1, either the honest parties hold a consistently encoded secret or dealer is caught and the protocol aborts with probability at least $1 - 2^{-\Omega(r)}$.

Proof. The soundness of the hybrid protocol is a combination of soundness statements for the VQSS and VCSS protocols. Formally, we need to bound the probability that one of the protocols fails,

$$\Pr[\text{fail}_{\text{VQSS}} \vee \text{fail}_{\text{VCSS}}] \leqslant \Pr[\text{fail}_{\text{VQSS}}] + \Pr[\text{fail}_{\text{VCSS}}]. \quad (1)$$

Let us first consider $\Pr[\text{fail}_{\text{VCSS}}]$. Consider the protocol of [37] whose probability of failure scales exponentially with a security parameter r'. We choose r' such that it is equal to the security parameter of VQSS, $r' = r$, and therefore, $\Pr[\text{fail}_{\text{VCSS}}] \leqslant 2^{-\Omega(r)}$.

On the other hand, by Lemma 1, the VQSS protocol can fail with probability $\Pr[\text{fail}_{\text{VQSS}}] \leqslant 2^{-\Omega(r)}$. Therefore, we obtain

$$\Pr[\text{fail}_{\text{VQSS}} \vee \text{fail}_{\text{VCSS}}] \leqslant 2^{-\Omega(r)}. \quad (2)$$

■

Theorem 2 (completeness). In the verifiable hybrid secret sharing protocol, Protocol 1, if D is honest, then she passes the verification phase. Moreover, if R is also honest, she reconstructs D's secret with probability at least $1 - 2^{-\Omega(r)}$, where r is the security parameter.

Proof. For the first part of the theorem, observe that an honest dealer always passes the verification phase. Indeed,

if the dealer is honest, she does not introduce any errors, neither in the VQSS, nor in the VCSS protocol. Moreover, by the assumption that active cheaters t are always bounded by the number of tolerable errors, the VHSS protocol can always correct the arising errors and the verification phase always accepts an honest dealer.

For the second part of the theorem, as in the soundness statement, we calculate the probability that the VHSS protocol fails with an honest dealer,

$$\Pr[\text{fail}'_{\text{VQSS}} \vee \text{fail}'_{\text{VCSS}}] \leqslant \Pr[\text{fail}'_{\text{VQSS}}] + \Pr[\text{fail}'_{\text{VCSS}}]. \tag{3}$$

For the classical VCSS protocol, as before, we consider the protocol of [37]. By choosing the security parameter of the classical protocol such that $r' = r$, we obtain $\Pr[\text{fail}'_{\text{VCSS}}] \leqslant 2^{-\Omega(r)}$. For the VQSS protocol, if R is also honest, by Lemma 2 the probability that the verification phase fails to identify the set B of apparent malicious nodes, occurs with probability $2^{-\Omega(r)}$, see the Appendix for details. Therefore,

$$\Pr[\text{fail}'_{\text{VQSS}} \vee \text{fail}'_{\text{VCSS}}] \leqslant 2^{-\Omega(r)}. \tag{4}$$

■

The encryption of the secret with a classical key has significant consequences for the secrecy of the VHSS scheme. We expand on it in the theorem below. Note that in a VQSS [8] the secrecy property holds for any $p_q \leqslant 2t_q$ nodes not being able to learn any information about the dealer's secret. However, in our VHSS scheme we choose a classical scheme such that $p_c = p > 2t_q$, and therefore, we lift the secrecy of the VQSS scheme (for a detailed discussion see Sec. IV C 1 below).

Theorem 3 (secrecy). In the verifiable hybrid secret sharing protocol, Protocol 1, when D is honest and there is at most t active cheaters in the verification phase, no group of at most $p = p_c$ nodes learns anything about D's secret state throughout the protocol, where p_c is the secrecy of the underlying classical scheme, except with probability exponentially small in the security parameter r.

Proof. The state describing the dealer's encrypted quantum secret and the randomly chosen classical encryption key $s = ab$ is

$$\sigma_{QS} = \sum_{ab=\{0,1\}^2} \frac{1}{4} X^a Z^b |\psi\rangle\langle\psi|_Q Z^b X^a \otimes |ab\rangle\langle ab|_S, \tag{5}$$

where Q is the quantum register of the dealer and S is the classical register of the encryption key. By Assumption 1 the classical VCSS scheme is secure and does not leak any information about the key $s = ab$ to any set of p_c nodes, even in the presence of a quantum adversary, except with probability exponentially small in the security parameter r. Therefore, without the knowledge of the encryption key s, the quantum state shared by the dealer as seen by the rest of the nodes is maximally mixed,

$$\sigma_Q = \text{tr}_S(\sigma_{QS}) = \sum_{ab=\{0,1\}^2} \frac{1}{4} X^a Z^b |\psi\rangle\langle\psi|_Q Z^b X^a = \frac{\mathbb{1}_Q}{2}. \tag{6}$$

Before sending out the shares, the dealer applies an encoding $\mathcal{E}_Q$ to the quantum register Q, so that

$$\forall\, |\psi\rangle \quad \text{tr}_S[(\mathcal{E}_Q \otimes \mathbb{1}_S)(\sigma_{QS})] = \mathcal{E}_Q[\text{tr}_S(\sigma_{QS})] \tag{7}$$

$$= \mathcal{E}_Q(\sigma_Q) =: \rho_{[1,n_q]}, \tag{8}$$

where $\rho_{[1,n_q]}$ is an n_q-qubit state sent by the dealer to n_q nodes. Importantly, since $\mathcal{E}_Q$ and σ_Q, Eq. (6), are independent of $|\psi\rangle$, $\rho_{[1,n_q]}$ is also independent of $|\psi\rangle$. Subsequently, the honest nodes do their encoding $\mathcal{E}$, and the malicious nodes can perform any (CPTP) operation $\mathcal{A}$ that they desire. After this step, since $\mathcal{E}$ and $\mathcal{A}$ do not depend on $|\psi\rangle$, the state of the n_q nodes $\rho'_{[1,n_q]}$ is independent of $|\psi\rangle$. In the classical scheme any group of p_c or fewer nodes has no information about s. Hence, the partial state of any $p = p_c$ or fewer nodes in VHSS does not depend on $|\psi\rangle$ and no information about the dealer's secret can be obtained, except with probability exponentially small in r.

C. Verifiable hybrid schemes

Our protocol for VHSS, Protocol 1, leads to a variety of schemes, depending on the parameters of the underlying VQSS and VCSS protocols. In this section we discuss the trade-offs between those parameters and specify what schemes can be achieved with our protocol.

1. Verifiable schemes with maximum secrecy

In any VQSS scheme based on an error correcting code with distance d, any group of at most $d-1$ nodes cannot recover information about the secret. As mentioned before, this is due to the fact that a code of distance d can correct up to $d-1$ erasures, and therefore any $n-(d-1)$ nodes can recover the state perfectly. In particular, it implies that $d-1$ nodes do not have any information about the encoded state [19]. Quantum Singleton bound [51] allows that $n \leqslant 2d-1$ for codes encoding a single qubit. The construction of [8] saturates this inequality, and therefore allows for attaining $p = \lfloor \frac{n-1}{2} \rfloor$, which we refer to as maximum secrecy. However, this construction uses systems of local dimension $q > n$ and is based on quantum Reed-Solomon codes [52].

To remedy this problem, we use a VQSS scheme based on CSS codes with single-qubit shares, at the cost of reducing secrecy. However, in our VHSS scheme, we combine this with a classical scheme for which $p_c > 2t_q$. Specifically, the VCSS protocol of [37] tolerates up to $\lfloor \frac{n-1}{2} \rfloor$ cheaters. This allows us to maximally lift the secrecy of the quantum scheme to the one attainable by the VQSS of [8].

*Lemma 3 (*VHSS *with maximum secrecy).* Given a $[[n, 1, d]]_2$ CSS error correcting code and a VCSS scheme tolerating up to $\lfloor \frac{n-1}{2} \rfloor$ classical active cheaters, Protocol 1 provides a way to construct a $\{\lfloor \frac{n-1}{2} \rfloor, t, n\}$-VHSS scheme with maximum secrecy $p = \lfloor \frac{n-1}{2} \rfloor$, tolerating $t \leqslant \lfloor \frac{d-1}{2} \rfloor$ active cheaters, where all of the shares are used to recover the quantum secret state.

Furthermore, we can explore other classical verifiable schemes in the context of lifting secrecy in VHSS. In [38] a classical VCSS scheme was presented, which has a strong secrecy property: any $p_c > t_c$ nodes cannot learn any information about the classical secret (for comparison, in the scheme of [37] $p_c = t_c$). However, this scheme is able to tolerate up to $t_c \leqslant \lfloor \frac{n_c-1}{4} \rfloor$ active classical cheaters. Additionally, there exists a trade-off between the number of nodes n, and the numbers of cheaters, i.e., $n_c \geqslant p_c + 3t_c + 1$ (for details see Sec. 3.2 of [38]). Consequently, this allows us to construct a VHSS scheme lifting the secrecy beyond $\frac{n}{2}$, but at the cost

of tolerating less active cheaters t. Note that the classical scheme was proven to be information theoretically secure against a classical adversary, and by Assumption 1 we assume it remains information theoretically secure against quantum adversary. Moreover, the protocol was shown to be perfectly secure, i.e., with zero probability of error. Therefore, secrecy achieved in a VHSS, which uses this protocol as a subroutine, is exact and does not depend on the security parameter r.

Lemma 4. Given a $[[n, 1, d]]_2$ CSS error correcting code and a VCSS scheme with $n \geqslant p + 3t + 1$, Protocol 1 provides a way to construct a $\{p, t, n\}$-VHSS scheme. In particular, to achieve $p > \lfloor \frac{n-1}{2} \rfloor$ the scheme tolerates $t < \frac{1}{3}(n - p - 1)$ active cheaters. All of the shares are used to recover the quantum secret state.

2. Threshold verifiable schemes

In the literature of secret sharing schemes, one often considers schemes which have a property called *threshold* [11,12]. This property can be stated as the requirement that there exists $p > 0$, such that no subset of less than p shares reveals any information about the state of the dealer, while any subset of $p + 1$ shares allows us to perfectly reconstruct the state. Importantly, in such schemes, there are no actively cheating nodes in the protocol.

Since in Protocol 1 we allow for the existence of active cheaters, let us consider a definition of a threshold scheme when there are $t > 0$ active cheaters. We will call it a strong threshold scheme. In this case, in the reconstruction phase the reconstructor R receives shares from $p + 1 = n - t'$ of the nodes. Among those, up to t of them can be arbitrarily corrupted.

Definition 2 (strong threshold scheme). A strong threshold (verifiable) secret sharing scheme is a scheme where:

(1) Any set of shares held by $p = n - t' - 1$ nodes does not reveal any information about the secret state.

(2) The reconstructor is able to perfectly reconstruct the secret state with the set of shares from any $n - t'$ nodes.

The above conditions hold in the presence of $t > 0$ active cheaters.

In the literature of classical verifiable secret sharing a similar definition of threshold is satisfied in the presence of cheaters. For example, the scheme of [53] considers a situation when honest shares are flagged. Therefore, the reconstructor knows which $n - t'$ honest shares to pick for the reconstruction. However, in our case, the reconstructor *does not* know which shares are honest and which are not. In such a situation, this definition cannot be satisfied, which we show in the following proposition.

Proposition 1. It is impossible to construct a strong threshold secret sharing scheme according to Definition 2.

Proof. From point 2 of Definition 2 we have that R must be able to reconstruct the secret state from any $n - t'$ shares, in particular, she must be able to do so when receiving $n - t' - t$ honest shares and t arbitrary ones. This implies that she is able to recover the state from the $n - t' - t$ honest shares alone. On the other hand, from point 1 of Definition 2 no $n - t' - 1$ shares reveal any information, which implies that we must have $n - t' - t > n - t' - 1$. The only way to satisfy this inequality is when $t = 0$. ■

Remark. Similarly to [53], it is possible to add a flagging system to Protocol 1 using techniques from [24,42]. Indeed, there, one uses a quantum authentication scheme to flag whether the shares are honest or not. However, as mentioned before, this happens at a significant qubit cost. Since our objective is to reduce the number of qubits, we explore a alternative direction in the next section.

3. Ramp verifiable schemes

In the previous section we have seen that it is impossible to construct a strong threshold scheme which tolerates active cheaters according to Definition 2. In particular, this result also applies to verifiable schemes. Therefore, here we allow for a gap between the number of nodes p that obtain no information about the secret and the number of nodes $n - t'$ necessary to reconstruct the secret, and we introduce a definition of a ramp verifiable scheme.

Definition 3. A ramp verifiable secret sharing scheme is a scheme where any $n - t'$ nodes can reconstruct the secret, but any p nodes cannot gain any information about the secret state, for some $p < n - t' - 1$. The scheme can verify the dealer in the presence of t active cheaters. We denote such a scheme with $\{p, t, t', n\}$-ramp.

Relating to discussion in Sec. IV C 1, we see that the purely quantum VQSS scheme of [8] allows for constructing a ramp scheme with secrecy $p \leqslant \lfloor \frac{n-1}{2} \rfloor$. However, for qubit CSS codes this equality is not saturated. Therefore, as before we use a classical scheme [37] to increase the value of p (lift the secrecy) as compared to the purely quantum ramp scheme. We obtain the following result.

Lemma 5 (Ramp VHSS*).* Given a $[[n, 1, d]]_2$ CSS error correcting code and a VCSS scheme tolerating up to $\lfloor \frac{n-1}{2} \rfloor$ classical active cheaters, Protocol 1 provides a way to construct a $\{p, t, t', n\}$-ramp VHSS scheme with $p = \lfloor \frac{n-1}{2} \rfloor$, where the quantum state can be recovered with shares from any $n - t'$ nodes in the presence of t active cheaters, and $t + t' \leqslant \lfloor \frac{d-1}{2} \rfloor$.

By putting $t' = 0$ we require reconstruction with all of the shares and recover the result of Lemma 3. Note that if we are interested in maximizing the number of cheaters and minimizing the number of the shares necessary for reconstruction, we can put $t = t' = \lfloor \frac{d-1}{4} \rfloor$.

V. OUTLOOK

We presented a protocol which achieves the task of sharing a quantum secret in a verifiable way, which reduces the number of qubits necessary to realize the protocol. In our scheme each node requires an n-qubit quantum memory and a workspace of at most $3n$ qubits in total. By combining classical encryption with a quantum scheme we showed that we can construct a variety of verifiable hybrid schemes attaining maximum secrecy. We proved that our protocol is secure in the presence of active nonadaptive adversary.

We remark that there is a dependence between the number of cheaters tolerated by a verifiable secret sharing protocol and quantum resources necessary to realize it. The number of cheaters can be increased to $2t$ by using approximate quantum error correction based on quantum authentication

schemes [24,42]. Indeed, in [9] the authors showed that by employing quantum authentication techniques, the VQSS scheme of [8] can tolerate up to $\frac{n}{2}$ malicious nodes. In this case, the power of the verification scheme increases up to the number of tolerable erasures of the code, and one can effectively tolerate twice as many malicious nodes. However, authentication schemes typically require another level of error correction, where the size of the code scales exponentially in the security parameter of the authentication. Therefore, such schemes increase the number of qubits required to realize the protocol.

ACKNOWLEDGMENTS

We thank J. Helsen, B. Dirkse, and P. Mazurek for valuable discussions and insights. This work was supported by STW Netherlands, NWO VIDI grant, ERC Starting grant, and NWO Zwaartekracht QSC. G.M. was also funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1-390534769.

APPENDIX: SECURITY OF THE VQSS SCHEME [8] IN THE SEQUENTIAL SETTING

Proof of Lemma 1. Here we state the soundness of the VQSS protocol. Since we use the VQSS in the sequential setting instead of the original parallel one, we restate security in the sequential setting. Our techniques are inspired by the approach suggested in [8,36].

To prove the soundness of the VQSS protocol, we bound the probability that the state held by the nodes after the verification phase is close to a codeword in $\mathcal{C} = V \cap \mathcal{F}W$ with at most t errors on the first level of encoding in the verification phase, or that the protocol aborts, and therefore, the dealer is caught. V denotes a space spanned by $\{|v\rangle : v \in V^C\}$, where V^C is a classical code space. Similarly, $\mathcal{F}W$ is spanned by $\{\mathcal{F}|w\rangle : w \in W^C\}$, where $\mathcal{F}$ is the Fourier transform and W^C is a classical code space such that the dual code $V^{C*} \subseteq W^C$.

Recall that in the protocol we encode the secret of the dealer into two levels of encoding. We will argue that performing verification on the second level of encoding is equivalent to verification on the first level of encoding. If a state is encoded once using $\mathcal{C}$, and has at most t errors, then the encoding defines a unique state. Therefore, it is enough to count the number of errors present in the first level of encoding and verify that there are at most t. However, the protocol requires two levels of encoding to make sure that no node has complete control over all shares. This implies that we cannot perform the verification directly at the first level. But since all the operations we use for verification are (essentially) transversal for code $\mathcal{C}$, we can argue about the verification as if it was performed on the first level.

In order to check for errors, it is enough to check for errors in the Z basis and errors in the X basis. Let V_t be the space of words that have at most t errors in the Z basis as compared to a codeword in V. In particular, if one measures a state $|v\rangle \in V_t$ in the Z basis, the outcome is a word in the space V_t^C, where V_t^C is the space of strings having at most t compared to a string in the classical code V^C. Similarly, we can define $(\mathcal{F}W)_t$ as the space of words that have at most t errors in the X basis as compared to a codeword in W. This means that if one measures a state $|w\rangle \in (\mathcal{F}W)_t$ in the X basis, the outcome is a word in the space W_t^C, where W_t^C is the space of strings having at most t compared to a string in the classical code W^C.

Considering the above argument, now we proceed with proving soundness of verification of the state in the Z basis and as if we were considering only one level of encoding.

Without loss of generality, we can decompose the state of the nodes after the sharing phase in spaces V_t and $V_t^\perp$,

$$\rho_{\text{sh}} = \sum_i q_i |\psi_i\rangle\langle\psi_i|, \tag{A1}$$

with $|\psi_i\rangle = a_i|\tilde{\psi}_i\rangle + b_i|\tilde{\psi}_i^\perp\rangle$, where $|\tilde{\psi}_i\rangle \in V_t$ and $|\tilde{\psi}_i^\perp\rangle \in V_t^\perp$. In words, the state after the sharing phase is a mixture of pure states which have components in V_t and $V_t^\perp$.

Moreover, let $\rho_{\text{ver}(Z)}$ be the state of all the nodes after the verification phase in the Z basis. We will show that "conditioned on not aborting, the state $\rho_{\text{ver}(Z)}$ is close to a codeword in the space V_t or the verification phase aborts with high probability."

By definition of the space V_t, $\rho_{\text{ver}(Z)}$ belongs to V_t, if by measuring it in the Z basis one obtains with certainty an outcome corresponding to a string $v \in V_t^C$. Therefore, we will quantify "the state $\rho_{\text{ver}(Z)}$ is close to a codeword in the space V_t" with a high probability of getting an outcome $v \in V_t^C$ when measuring $\rho_{\text{ver}(Z)}$. Alternatively, one can think of a situation in which first a measurement on the initial state is performed and then the verification takes place. To prove the security statement we will use a tool called "quantum-to-classical" reduction, which relates the statistics obtained in the two situations. That is, in order to compute the probability of aborting in the verification phase of the VQSS protocol or the probability that the resulting state is in $V \cap \mathcal{F}W$, we will analyze the situation in which the state is measured *before* the verification.

Probability of aborting. In order to evaluate probability of aborting, we will follow the solution suggested in [36] for the parallel execution of the VQSS and we will show how to use this result for the sequential setting. To do so, let us fix a round $(0, m)$, with $m > 0$. For this round we can use the quantum-to-classical reduction. It states that the two following situations are equivalent: (i) the honest nodes measure their shares of $\rho_{\text{ver}(Z)}$ in the standard basis at the end of the verification phase; and (ii) the honest nodes measure their shares of ρ_{sh} and an mth ancilla right after they have been distributed, i.e., before running the verification of round $(0, m)$. Formally,

$$\forall m\, \mathcal{M}_0\mathcal{M}_m \text{CNOT}_{0,m}^{b_{0,m}} = \mathcal{M}_m \text{CNOT}_{0,m}^{b_{0,m}} \mathcal{M}_m\mathcal{M}_0, \tag{A2}$$

where $\mathcal{M}_0$ and $\mathcal{M}_m$ denote measurements of the state of the nodes and mth ancilla, respectively. $\text{CNOT}_{0,m}^{b_{0,m}}$ denotes a CNOT gate performed with ρ_{sh} as a control and the mth ancilla as target. Note that if the nodes perform measurements right after the shares are distributed [situation (ii)] they only need to handle classical data from that moment on. Therefore, quantum-to-classical reduction means that the verification phase of the quantum VQSS protocol (Q protocol) can be reduced to a corresponding verification in a classical protocol

(C protocol). That is to say, measurement outcomes in Q protocol and C protocol are exactly the same and the moment when the measurement is performed does not change the behavior of the protocol. Since the measurement is performed in the standard basis and the CNOT gate acts as a bit flip in the standard basis, the two operations commute.

Let us look now at the sequential execution of Q protocol and C protocol. Expanding the above dependence onto m sequential rounds, we obtain

$$\begin{aligned}&\mathcal{M}_0\mathcal{M}_r\mathrm{CNOT}_{0,r}^{b_{0,r}}\cdots\mathcal{M}_1\mathrm{CNOT}_{0,1}^{b_{0,1}}\\&\quad=\mathcal{M}_r\mathrm{CNOT}_{0,r}^{b_{0,r}}\mathcal{M}_r\cdots\mathcal{M}_1\mathrm{CNOT}_{0,1}^{b_{0,1}}\mathcal{M}_1\mathcal{M}_0.\end{aligned}\tag{A3}$$

In particular, this means that the probability of aborting in the sequential Q protocol can be reduced to considering the probability of aborting in the sequential C protocol,

$$\Pr[\neg\mathrm{abort}_Q]=\Pr[\neg\mathrm{abort}_C].\tag{A4}$$

Consider the corresponding C protocol for round ($\ell=0$, m): the nodes have *classical* bit strings $v_{0,0}$ and $v_{0,m}$. They wish to verify whether $v_{0,0}$ is a string in the space V_t^C. To do so the (honest) nodes compute bit-wise $v_{0,m}+b_{0,m}v_{0,0}$ according to public random bit $b_{0,m}$. They broadcast the result and create the set of apparent cheaters B.

In the C protocol, the string $v_{0,0}$ can either be a string in V_t^C or not. This depends on the shared state (A1), and therefore happens with probabilities

$$\Pr\left[v_{0,0}\in V_t^C\right]=\sum_i q_i|a_i|^2=:a,\tag{A5}$$

$$\Pr\left[v_{0,0}\notin V_t^C\right]=\sum_i q_i|b_i|^2=:b,\tag{A6}$$

respectively. Indeed, the probability that any of the $|\psi_i\rangle$ from (A1) yields a string from V_t^C (not in V_t^C) is given by $|a_i|^2$ ($|b_i|^2$). In the case when $v_{0,0}$ is a string in V_t^C, the verification always passes and we have that $\Pr[\neg\mathrm{abort}_C|v_{0,0}\in V_t^C]=1$. On the other hand, if $v_{0,0}$ is not a string in V_t^C, then for all bit strings $v_{0,m}$ there exists at most one bit $b_{0,m}$ such that $v_{0,m}+b_{0,m}v_{0,0}$ is a string in V_t^C. Since $b_{0,m}$ is chosen independently of $v_{0,m}$ and $v_{0,0}$, and uniformly at random, the probability that $v_{0,m}+b_{0,m}v_{0,0}$ a codeword is at most $\frac{1}{2}$. Since the above is true for any value of $v_{0,m}$, in particular it must be true even if $v_{0,m}$ depends on the previous rounds $1,\ldots,m-1$. Therefore, the overall probability p that the verification phase of the C protocol does not abort given that $v_{0,0}$ is not a string in V_t^C, is at most

$$p=\Pr\left[\neg\mathrm{abort}_C|v_{0,0}\notin V_t^C\right]\leqslant 2^{-r}.\tag{A7}$$

The above consideration allows us to write that the probability of the C protocol not aborting is

$$\begin{aligned}\Pr[\neg\mathrm{abort}_C]=\Pr\left[v_{0,0}\in V_t^C\right]&\Pr\left[\neg\mathrm{abort}_C|v_{0,0}\in V_t^C\right]\\&+\Pr\left[v_{0,0}\notin V_t^C\right]\Pr\left[\neg\mathrm{abort}_C|v_{0,0}\notin V_t^C\right].\end{aligned}\tag{A8}$$

Since $\Pr[\neg\mathrm{abort}_Q]=\Pr[\neg\mathrm{abort}_C]$, Eq. (A4), in the Q protocol we have

$$\Pr[\neg\mathrm{abort}_Q]=a+pb.\tag{A9}$$

Probability of measuring a string in V_t^C. Now our objective is to evaluate $\Pr[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q]$. By quantum-to-classical reduction argument (A3), we know that the C protocol should yield the same statistics as the Q protocol,

$$\Pr\left[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q\right]=\Pr\left[v_{0,0}\in V_t^C|\neg\mathrm{abort}_C\right].\tag{A10}$$

From the considerations about the probability of aborting, using the rules of probability, we can compute

$$\Pr\left[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q\right]=\frac{a}{a+pb}.\tag{A11}$$

Now let us combine the statements about probability of aborting and probability of measuring a string in V_t^C. Using the quantum-to-classical reduction, we can formally reformulate the initial statement "conditioned on not aborting, the state $\rho_{\mathrm{ver}(Z)}$ is close to a codeword in the space V_t, or the verification phase aborts with high probability" as

$$\begin{cases}\Pr\left[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q\right]>1-\delta\\ \text{or}\\ \Pr\left[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q\right]\leqslant 1-\delta\\ \qquad\text{and }\Pr[\mathrm{abort}_Q]\geqslant 1-\frac{2^{-r}}{\delta},\end{cases}\tag{A12}$$

where δ is a threshold for probability of measuring a string from V_t^C. Indeed, using Eqs. (A9) and (A11) we can express $\Pr[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q]$ as a function of $\Pr[\neg\mathrm{abort}_Q]$,

$$\Pr\left[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q\right]=\frac{\Pr[\neg\mathrm{abort}_Q]-p}{\Pr[\neg\mathrm{abort}_Q](1-p)}.\tag{A13}$$

Now, either $\Pr[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q]>1-\delta$ and the first condition is satisfied, or $\Pr[v_{0,0}\in V_t^C|\neg\mathrm{abort}_Q]\leqslant 1-\delta$ and using (A13) we get

$$\Pr[\neg\mathrm{abort}_Q]\leqslant\frac{p}{\delta}\leqslant\frac{2^{-r}}{\delta},\tag{A14}$$

and therefore $\Pr[\mathrm{abort}_Q]\geqslant 1-\frac{2^{-r}}{\delta}$.

In analogy to the above reasoning, one can construct an argument for a check in the X basis. Therefore, we can write

$$\begin{cases}\Pr\left[w_{0,0}\in W_t^C|\neg\mathrm{abort}_Q\right]>1-\delta'\\ \text{or}\\ \Pr\left[w_{0,0}\in W_t^C|\neg\mathrm{abort}_Q\right]\leqslant 1-\delta'\\ \qquad\text{and }\Pr[\mathrm{abort}_Q]\geqslant 1-\frac{2^{-r}}{\delta'},\end{cases}\tag{A15}$$

where δ' is a threshold for probability of measuring a string from W_t^C.

Furthermore, in the protocol we verify that each of the $|\bar{0}\rangle$ ancilla states is sufficiently close to space V_t before running the verification in the X basis. Let V_t^{0C} be a subspace of the code V_t^C whose codewords are entries in the logical $|\bar{0}\rangle$, i.e., $0+(W^{C*})_t$, where the dual code $(W^{C*})_t\subseteq V_t^C$. Then V_t^0 is a subspace of V_t, such that V_t^0 is spanned by $\{|v\rangle : v\in V_t^{0C}\}$. Formally, we verify that conditioned on not aborting, the actual state of the ancilla is close to a codeword in V_t^0, or the verification phase aborts with high probability,

$$\begin{cases}\Pr\left[v\in V_t^{0C}|\neg\mathrm{abort}_Q\right]>1-\delta''\\ \text{or}\\ \Pr\left[v\in V_t^{0C}|\neg\mathrm{abort}_Q\right]\leqslant 1-\delta''\\ \qquad\text{and }\Pr[\mathrm{abort}_Q]\geqslant 1-\frac{2^{-r}}{\delta''},\end{cases}\tag{A16}$$

where δ'' is a threshold for probability of measuring a string from V_t^{0C}. Since there are r of ancilla checks, the probability that measuring all of the $|\bar{0}\rangle$ states yield a codeword from space V_t^{0C} can be written as

$$\Pr\left[\bigwedge_{\ell=1}^{r} v_{\ell,0} \in V_t^{0C} \middle| \neg\text{abort}_Q\right] \geqslant 1 - r\delta''. \tag{A17}$$

The purpose of having $|\bar{0}\rangle \in V_t^0$ is that using these ancillas for verification in the X basis will not introduce bit flip errors in the Z basis. In other words, any state in V_t remains in V_t after its verification in the X basis, as long as we use ancillas $|\bar{0}\rangle \in V_t^0$.

We will now make a statement about the whole verification phase. Let the state of the nodes after the verification in the Z basis have the form

$$\rho_{\text{ver}(Z)|b_Z\neq 0} = \alpha\rho_{V_t} + \beta\rho_{V_t^\perp} \tag{A18}$$

where ρ_{V_t} is a mixture of pure states in V_t and $\rho_{V_t^\perp}$ is a mixture of pure states in $V_t^\perp$. Here we condition the state on the fact that the public random bits b_Z used in the verification in the standard basis (i.e., $b_{0,m}$ for $m = 1, \ldots, r$) are all different than 0, i.e., that at least one CNOT gate is performed. In this case, measuring the state of the nodes after the CNOT, projects it either on V_t or $V_t^\perp$. It happens with probabilities α and β, respectively.

Similarly, after the consecutive verification in the X basis, the state of the nodes will be

$$\begin{aligned}\rho_{\text{ver}(Z,X)|b_Z,b_X\neq 0,|\bar{0}\rangle\in V_t^0} &= \alpha\alpha'\rho_{V_t\cap\mathcal{F}W_t} + \alpha\beta'\rho_{V_t^\perp\cap\mathcal{F}W_t} \\ &\quad + \beta\left(\alpha''\rho_{V_t\cap\mathcal{F}W_t^\perp} + \beta''\rho_{V_t^\perp\cap\mathcal{F}W_t^\perp}\right),\end{aligned} \tag{A19}$$

where we additionally condition the state on the fact that bits b_X used for verification in the X basis are all different than zero (i.e., at least one CNOT was performed in the X basis). Moreover, we condition it on the fact that $|\bar{0}\rangle$ ancillas used for verification in the X basis are in V_t^0. Assuming the first lines of Eqs. (A12) and (A15), we get that

$$\alpha\alpha' + \alpha\beta' > 1 - \delta, \tag{A20}$$

$$\alpha\alpha' + \beta\alpha'' > 1 - \delta'. \tag{A21}$$

The first line implies that $\beta(\alpha'' + \beta'') \leqslant \delta$ and therefore, $\beta \leqslant \delta$. Using this in the second line we get that $\alpha\alpha' \geqslant 1 - \delta - \delta'$. Now, $\alpha\alpha'$ is exactly the probability that measuring $\rho_{\text{ver}(Z,X)|b_Z,b_X\neq 0,|\bar{0}\rangle\in V_t^0}$ in the Z basis yields a string in V_t^C *and* measuring it in the X basis yields a string in W_t^C. Therefore, we get

$$\begin{aligned}&\Pr\left[v_{0,0} \in V_t^C \wedge w_{0,0} \in W_t^C | \neg\text{abort}, b_Z,\right. \\ &\left. b_X \neq 0, |\bar{0}\rangle \in V_t^0\right] \geqslant 1 - \delta - \delta'.\end{aligned} \tag{A22}$$

Now we will lower bound the probability $\Pr[v_{0,0} \in V_t^C \wedge w_{0,0} \in W_t^C | \neg\text{abort}]$, i.e., remove the conditioning on b_Z, $b_X \neq 0$, $|\bar{0}\rangle \in V_t^0$ from the above probability expression. Let us evaluate

$$\begin{aligned}&\Pr\left[v_{0,0} \in V_t^C \wedge w_{0,0} \in W_t^C | \neg\text{abort}\right] \\ &= \Pr\left[b_Z, b_X \neq 0 \wedge |\bar{0}\rangle \in V_t^0 | \neg\text{abort}\right] \Pr\left[v_{0,0} \in V_t^C \wedge w_{0,0} \in W_t^C | \neg\text{abort}, b_Z, b_X \neq 0, |\bar{0}\rangle \in V_t^0\right] \\ &\quad + \underbrace{\Pr\left[\neg(b_Z, b_X \neq 0) \vee |\bar{0}\rangle \notin V_t^0 | \neg\text{abort}\right]}_{\leqslant r2^{-r} + \Pr\left[|\bar{0}\rangle\notin V_t^0 | \neg\text{abort}\right] \leqslant r2^{-r} + r\delta''} \underbrace{\Pr\left[v_{0,0} \in V_t^C \wedge w_{0,0} \in W_t^C | \neg\text{abort}, \neg(b_Z, b_X \neq 0), |\bar{0}\rangle \notin V_t^0\right]}_{\leqslant 1},\end{aligned} \tag{A23}$$

where we assumed the first line of Eq. (A16) to bound $\Pr[|\bar{0}\rangle \notin V_t^0 | \neg\text{abort}]$. To sum up, the conjunction of

$$\begin{aligned}&\Pr\left[v_{0,0} \in V_t^C | \neg\text{abort}_Q\right] > 1 - \delta, \\ &\Pr\left[w_{0,0} \in W_t^C | \neg\text{abort}_Q\right] > 1 - \delta', \\ &\Pr\left[\bigwedge_{\ell=1}^{r} v_{\ell,0} \in V_t^{0C} \middle| \neg\text{abort}_Q\right] \geqslant 1 - r\delta'',\end{aligned} \tag{A24}$$

implies that

$$\begin{aligned}&\Pr\left[v_{0,0} \in V_t^C \wedge w_{0,0} \in W_t^C | \neg\text{abort}\right] \\ &\quad \geqslant (1 - \delta - \delta') + r(2^{-r} + \delta'')(\delta + \delta').\end{aligned} \tag{A25}$$

Therefore, either Eq. (A25) is satisfied or at least one of the equations in (A24) is not satisfied. In the latter case, Eqs. (A12), (A15), and (A16) imply that

$$\Pr[\text{abort}] \geqslant 1 - \max\left\{\frac{2^{-r}}{\delta}, \frac{2^{-r}}{\delta'}, \frac{2^{-r}}{\delta''}\right\}. \tag{A26}$$

■

Proof of Lemma 2. If the dealer is honest, the size of set B must be at most t—there is at most t malicious nodes and only real malicious nodes are accused of cheating. Therefore, the verification phase will always lead to accepting an honest dealer.

If R is also honest then we must calculate the probability that the verification phase fails to identify the set B of apparent malicious nodes. In this case, the reconstruction phase could take inconsistent shares to reconstruct the original state of the dealer. We can use the quantum-to-classical reduction argument again (see [36] and the argument above) and argue about the probability of error for the classical protocol. An error in the classical case can occur when any of the checks for Z or X basis, or checks of $|\bar{0}\rangle$, lead to consistent strings on V_t^C, $\mathcal{F}W_t^C$, or V_t^{C0}. Similarly to the argument above, the probability of that occurring is

$$\epsilon_c = (2 + r)2^{-r}. \tag{A27}$$

Let us now look at the reconstruction phase of the quantum protocol to bound the fidelity of the output state. When the reconstructor is honest, she first applies a decoding operator to each branch i corresponding to node $i \notin B$. The operator corrects errors without knowledge of the positions which carry errors (i.e., it corrects arbitrary errors). Therefore, whenever in qubits corresponding to branch $i \notin B$ there is no more than t errors, the decoding will identify the errors and correct them. In the case when there are more than t errors in a branch i, the procedure will leave that branch untouched and the reconstructor will update the set B with position i. Second, the honest reconstructor applies an erasure-recovery circuit to randomly chosen $n - 2t$ positions from $i \notin B$. In the case when all of the errors are correctly identified in B, the erasure-recovery corrects for $n - 2t$ erasure errors, i.e., missing qubits of the dealer and malicious nodes, and outputs the original state of the dealer. Since the verification phase can fail to identify the set B with probability ϵ_c, we have

$$\rho_{\text{rec}} = (1 - \epsilon_c)|\psi\rangle\langle\psi| + \epsilon_c \tilde{\rho}_R, \tag{A28}$$

where $\tilde{\rho}_R$ is an arbitrary state that depends on the action of the malicious nodes. Let us define the fidelity of the reconstructed state as $F = \text{Tr}[\rho_{\text{rec}}|\psi\rangle\langle\psi|_R]$. Using linearity properties of the trace together with the fact that quantum states have nonzero trace, we have that

$$\begin{aligned} F &= \text{Tr}[((1 - \epsilon_c)|\psi\rangle\langle\psi| + \epsilon_c \tilde{\rho})\,|\psi\rangle\langle\psi|] \\ &= (1 - \epsilon_c)\text{Tr}[|\psi\rangle\langle\psi||\psi\rangle\langle\psi|] + \underbrace{\epsilon_c \text{Tr}[\tilde{\rho}\,|\psi\rangle\langle\psi|]}_{\geqslant 0} \\ &\geqslant 1 - \epsilon_c. \end{aligned} \tag{A29}$$

[1] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, in *Proceedings of the 26th Annual Symposium on Foundations of Computer Science, SFCS '85* (IEEE Computer Society, Washington, DC, 1985), pp. 383–395.

[2] P. Feldman, in *Proceedings of the 28th Annual Symposium on Foundations of Computer Science (sfcs 1987)* (IEEE, Los Angeles, CA, 1987), pp. 427–438.

[3] D. Chaum, C. Crépeau, and I. Damgard, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC '88* (ACM Press, New York, 1988), pp. 11–19.

[4] W. Du and M. J. Atallah, in *Proceedings of the 2001 Workshop on New Security Paradigms, NSPW '01* (ACM Press, New York, 2001), pp. 13–22.

[5] P. Feldman and S. Micali, SIAM J. Comput. **26**, 873 (1997).

[6] P. Y. A. Ryan, S. Schneider, and V. Teague, IEEE Security Privacy **13**, 59 (2015).

[7] X. Défago, A. Schiper, and P. Urbán, ACM Comput. Surv. **36**, 372 (2004).

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

[9] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, in *Proceedings of the 2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)* (IEEE, Berkeley, CA, 2006), pp. 249–260.

[10] M. Ben-Or and A. Hassidim, in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, STOC '05* (ACM Press, New York, 2005), pp. 481–485.

[11] A. Shamir, Commun. ACM **22**, 612 (1979).

[12] G. R. Blakley, in *Proceedings of the International Workshop on Managing Requirements Knowledge* (IEEE Computer Society, Los Alamitos, CA, 1979), p. 313.

[13] H. Krawczyk, in *Advances in Cryptology—CRYPTO' 93*, edited by D. R. Stinson (Springer, Berlin, 1994), pp. 136–146.

[14] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[15] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[16] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).

[17] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).

[18] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[19] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[20] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[21] A. Marin and D. Markham, Phys. Rev. A **88**, 042332 (2013).

[22] J. Javelle, M. Mhalla, and S. Perdrix, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by K. Iwama, Y. Kawano, and M. Murao (Springer, Berlin, 2013), pp. 1–12.

[23] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Nat. Commun. **5**, 5480 (2014).

[24] C. Crépeau, D. Gottesman, and A. Smith, in *Advances in Cryptology—EUROCRYPT 2005*, edited by R. Cramer (Springer, Berlin, 2005), pp. 285–301.

[25] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[26] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, Phys. Rev. A **72**, 032318 (2005).

[27] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).

[28] V. Gheorghiu, Phys. Rev. A **85**, 052309 (2012).

[29] B. Fortescue and G. Gour, IEEE Trans. Inf. Theory **58**, 6659 (2012).

[30] S. Kumar Singh and R. Srikanth, Phys. Rev. A **71**, 012328 (2005).

[31] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016).

[32] M. Steudtner and S. Wehner, New J. Phys. **20**, 063010 (2018).

[33] N. Moll, A. Fuhrer, P. Staar, and I. Tavernelli, J. Phys. A **49**, 295301 (2016).

[34] S. Bravyi, J. M. Gambetta, A. Mezzacapo, and K. Temme, arXiv:1701.08213.

[35] T. Peng, A. Harrow, M. Ozols, and X. Wu, arXiv:1904.00102.

[36] A. Smith, arXiv:quant-ph/0111030.

[37] T. Rabin and M. Ben-Or, in *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, STOC '89* (ACM Press, New York, 1989), pp. 73–85.
[38] D. R. Stinson and R. Wei, in *Selected Areas in Cryptography*, edited by H. Heys and C. Adams (Springer, Berlin, 2000), pp. 200–214.
[39] M. Mosca, A. Tapp, and R. de Wolf, arXiv:quant-ph/0003101.
[40] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, in *Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM '99*, The Future is Now (Cat. No. 99CH36320) (IEEE, New York, NY, 1999), Vol. 2, pp. 708–716.
[41] R. Canetti, in *Proceedings of the 17th IEEE Computer Security Foundations Workshop* (IEEE, Pacific Grove, CA, 2004), pp. 219–233.
[42] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Vancouver, Canada, 2002), pp. 449–458.
[43] A. J. Landahl, J. T. Anderson, and P. R. Rice, arXiv:1108.5738.
[44] S. B. Bravyi and A. Y. Kitaev, arXiv:quant-ph/9811052.
[45] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[46] A. Steane, Proc. R. Soc. London Ser. A **452**, 2551 (1996).
[47] D. Unruh, in *Advances in Cryptology—EUROCRYPT 2010*, edited by H. Gilbert (Springer, Berlin, 2010), pp. 486–505.
[48] M. M. Prabhakaran and A. Sahai, *Secure Multi-party Computation* (IOS Press, London, 2013), Vol. 10.
[49] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai, in *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing, STOC '02* (ACM Press, New York, 2002), pp. 494–503.
[50] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, 2011).
[51] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[52] D. Aharonov and M. Ben-Or, in *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, STOC '97* (ACM Press, New York, 1997), pp. 176–188.
[53] B. Schoenmakers, in *Advances in Cryptology—CRYPTO' 99*, edited by M. Wiener (Springer, Berlin, 1999), pp. 148–164.