

## Erratum: Secure multiparty quantum computation with few qubits [Phys. Rev. A **102**, 022405 (2020)]

Victoria Lipinska, J  r  my Ribeiro, and Stephanie Wehner



(Received 14 June 2024; published 2 July 2024)

DOI: [10.1103/PhysRevA.110.019901](https://doi.org/10.1103/PhysRevA.110.019901)

We wish to correct an error in our article in the subprotocol verifying magic states. Specifically, the circuit used to implement the verification cannot be implemented transversally for the chosen family of codes. In this erratum, we explain the error in detail and propose a solution based on already existing techniques, i.e., distributed magic state distillation. This approach increases the operational qubit workspace per node from  $n^2 + 4n$  to  $n^2 + \Theta(s)n$ , where  $s$  is the security parameter. The increase is linear in  $n$ , which means that the main result of our paper remains intact: the number of qubits per node necessary to implement the multiparty quantum computation is still smaller than the previous protocol [1]. Moreover, the security proof in our manuscript does not change.

### I. THE ISSUE

In our article, we presented a protocol for distributed multiparty quantum computation (MPQC) of universal circuits. Our method is based on quantum error correction, and we choose a subfamily of Calderbank-Steane-Shor (CSS)  $\hat{\mathcal{C}}$  that allows for a transversal implementation of the Clifford gates. Transversality is essential since we require that any operation  $\Lambda$  implemented by the nodes locally should yield the same operation  $\bar{\Lambda}$  at a logical level.

To implement any circuit, we supplement the Clifford gates with logical magic states  $|\bar{m}\rangle$ , which need to be verified, i.e., the nodes must collectively agree that there are at most  $t$  errors in the logical magic state. After this step the nodes can use the magic state to implement the  $T$  gate transversally using gate teleportation.

The method we chose for the verification procedure is based on the so-called stabilizer measurement. Unfortunately, the controlled gate  $C\text{-}XP^\dagger$  implementing the stabilizer measurement is *not* a Clifford gate, and for our chosen family of codes  $\hat{\mathcal{C}}$  this gate is not transversal. This means that the procedure cannot be implemented transversally, and the magic state cannot be verified with this procedure.

### II. THE SOLUTION

To solve the problem, we propose a new protocol for the verification of magic states. Our new protocol is based on magic state distillation [2] and statistical testing of randomly selected states. We note that this is a method inspired by distillation of entangled pairs whose exact initial state is unknown [3]. A similar approach has recently been reported by [4]. In the following, we first describe the new protocol on a high level and then provide a detailed description.

In the magic state verification procedure, one node produces  $M$  copies of the magic state  $|m\rangle$ . The nodes share and verify the encoding of the state using the verifiable secret sharing protocol; see Protocol 1 in the original article. Then, using public randomness, the nodes pick a fraction of states to be statistically tested. For each picked state, the nodes select a random node who reconstructs the shared state and measures it in the  $\{|m\rangle, |m^\perp\rangle\}$  basis. If all of the measurement results yield  $|m\rangle$ , then the nodes have statistical evidence that the rest of the states are good with high probability. Next, the nodes perform dephasing in the  $\{|m\rangle, |m^\perp\rangle\}$  basis on the remaining states. This is done by randomly applying the  $PX$  gate, which is a Clifford gate, and therefore it can be implemented transversally with the code  $\hat{\mathcal{C}}$ . This step is necessary, since to perform magic state distillation the initial states must have a diagonal form in the  $\{|m\rangle, |m^\perp\rangle\}$  basis. After this, the nodes perform magic state distillation using the 15-to-1 Bravyi-Kitaev protocol [2]. Importantly, this protocol can also be realized using only Clifford gates and measurements, both of which can be implemented essentially transversally for the chosen family of codes. Note that the distillation procedure can be performed many times to get arbitrarily close to the perfect magic state.

We remark that the statistical testing is necessary to assess the quality of magic states before distillation, since the states can be produced by cheaters. If this were the case, performing the distillation straightforwardly would not give a guarantee on the quality of the final magic state.

### III. IMPLICATIONS FOR THE RESULTS

Here we point out the implications of the change we make to the overall results of our work.

*Outline 1.* (Multiparty quantum computation, repeated from our article)

Input: single-qubit state  $\rho_i$  from each node, CSS code  $\hat{C}$  with transversal Cliffords, circuit  $\mathfrak{R}$ .

(1) *Sharing and verification*

Each node  $i = 1, \dots, n$  encodes her input  $\rho_i$  using code  $\hat{C}$  into an  $n$ -qubit logical state, and sends one qubit (i.e., one single-qubit share) of the logical state to every other node, while keeping one for herself. The nodes jointly verify the encoding done by node  $i$  using a verifiable quantum secret sharing protocol (see Protocol 1 in our article).

(2) *Computation*

(i) For every Clifford gate in circuit  $\mathfrak{R}$ :

The nodes apply transversal Clifford gates locally to qubits specified by the circuit  $\mathfrak{R}$ .

(ii) For every  $T$  gate in circuit  $\mathfrak{R}$  applied to qubit  $i$ , the nodes run Verification of Magic States, Protocol 3 (*the new protocol*). If the verification is successful, the nodes perform Distributed Gate Teleportation; see Protocol 2 in the original article.

Every  $|0\rangle$  ancilla state required for circuit  $\mathfrak{R}$ , which is prepared by node  $i$ , is jointly verified by the nodes using verifiable quantum secret sharing, Protocol 1 in our article.

If the verification of any step fails, the nodes substitute their shares for  $|0\rangle$  and abort the protocol at the end of the computation.

(3) *Reconstruction*

Each node  $i$  collects all shares of her part of the output. She corrects errors using code  $\hat{C}$  and reconstructs her output.

Let  $M$  be the number of magic states produced for each  $T$  gate of the circuit one wishes to execute throughout the MPQC. Let  $k$  be the number of these states that is measured in Testing of Protocol 3; see below.

(i) *Security of MPQC.* The security of our MPQC protocol remains unchanged. Theorem 1 below ensures that conditioned on not aborting and for  $M = \Theta(s)$  and  $k = \Theta(s)$ , the state after verification is  $2^{-\Omega(s)}$  close to a logical magic state, where  $s$  is the security parameter. This means that, as before, the overall security of the MPQC protocol can be quantified with a total error probability of  $\kappa 2^{-\Omega(s)}$ , where  $\kappa = n + \#T$  gates + #ancillas in a circuit executed in MPQC; see Theorem 1 in the original article.

(ii) *Qubit workspace.* The new scaling for the qubit workspace only has a linear overhead as compared to the previous version, and it remains lower than the previous result by [1]. The qubit workspace required per node is now  $n^2 + (M + 2)n = n^2 + \Theta(s)n$  as opposed to the previously derived  $n^2 + 4n$ . As before, sharing and verifying the  $n$  input qubits uses at most  $n^2 + 2n$  qubits. However, we must also consider the resources needed for the magic state verification. When sharing the magic state, the nodes already hold  $n^2$  qubits corresponding to the inputs, and the magic state distribution and verification requires  $(M + 2)n$  qubits.

(iii) *Quantum communication complexity.* The quantum communication complexity is essentially unchanged. With the new verification method each node sends  $[(M - 1)s^2 + k]n \cdot \#T = \Theta(s)ns^2 \cdot \#T$  extra qubits. This means that the communication complexity per node is now  $O((n + \#ancillas + M \cdot \#T)ns^2 + kn \cdot \#T) = O([n + \#ancillas + \Theta(s) \cdot \#T]ns^2)$ , as opposed to the previous  $O((n + \#ancillas + \#T)ns^2)$ , where  $\#T$  is the number of  $T$  gates.

In our MPQC protocol from our article, we introduced an “abort” event. That is, the protocol could abort if there were more than  $t$  errors introduced by the cheaters, accumulated over all inputs. For comparison, now our MPQC protocol can abort either because the verification of the magic state aborts or because more than  $t$  errors have been introduced by the cheaters, accumulated over all inputs. We remark that the verification procedure below can be repeated until successful in the following way. Every time the verification fails, two nodes are removed from the next execution: one node who created the state and one who measured  $|m^\perp\rangle$ . By repeating this  $t$  times, we would remove at most  $2t$  nodes, and with certainty remove all of the cheaters. In the next  $(t + 1)$ th execution, all the  $n - 2t$  remaining nodes would be honest and the procedure would necessarily succeed. This would leave the MPQC aborting only in the latter case, i.e., when more than  $t$  errors occur.

*Protocol 3 (Verification of Magic States (VMagic), new protocol).* Input: set of apparent cheaters  $B$ , number  $M$  of magic states to be created, number  $k$  of magic states to be measured.

Output: verified logical state  $|\bar{m}\rangle$

**Testing**

(1) A randomly selected node  $i$  creates  $M$  copies of the magic state  $|m\rangle$ .

(2) The nodes run a verifiable secret sharing protocol using code  $\hat{C}$  (VQSS, Protocol 1 in our article)  $M$  times, every time with  $|m\rangle$  as an input and with dealer  $i$ . They update the set  $B$  with apparent cheaters  $B_m$  revealed in verifying each copy of  $|m\rangle$ .

(3) The nodes use public randomness to decide

(i) which  $k$  of the  $M$  copies will be measured;

(ii) which node will measure each of the selected  $k$  copies.

(4) The nodes send the shares according to the division in the previous step, and use the reconstruction of the VQSS [1] to reconstruct a state.

(5) Each node measures the reconstructed state in the  $\{|m\rangle, |m^\perp\rangle\}$  basis. They announce the results of the measurement.

(i) If all measurements yield  $|m\rangle$ , continue.

(ii) If any measurement yields  $|m^\perp\rangle$ , set  $B = [n]$  (this will cause the MPQC protocol to abort after the computation phase).

**Distillation** ([4], Circuit 2.8)

(1) The nodes use public randomness to apply  $PX$  to each share of the remaining  $M - k$  logical states with probability  $\frac{1}{2}$  (n.b. this brings the logical states into a form diagonal in the  $\{|m\rangle, |m^\perp\rangle\}$  basis).

(2) The nodes use public randomness to permute the remaining  $M - k$  logical states.

(3) The nodes apply the 15-to-1 magic state distillation protocol [2]. Any measurements throughout the protocol are broadcast and the logical value is reconstructed using verifiable classical secret sharing (like in the verification phase of the VQSS; see Protocol 1 in our article).

#### IV. PARAMETER ANALYSIS

In this section, we give technical details of the magic state verification protocol, Protocol 3. We point out that the security proof in our manuscript does not change. The only alteration is in the derivation of the error that can be introduced by the verification of the magic state (this corresponds to a different error in the “real protocol” at the end of Appendix A in our article). In the following, we derive this error explicitly. We will first state a few useful lemmas necessary to prove the security of our new verification protocol. Then we will proceed with stating the desired security in Theorem 1.

Let  $M$  be the number of magic states distributed by a randomly selected node; let  $k < M$  be the number of copies chosen to be measured by all nodes, and  $k' \leq k$  out of all of the measured copies be measured by the honest nodes. Note that selecting a random node and selecting which copies to measure can be done using an already assumed public source of randomness and classical multiparty computation; see our original article. The lemma below states that if a state is close to the subspace of a state with a small “Hamming weight,” then Protocol 3 can distill it to a state close to a pure magic state. Since  $\{|m\rangle, |m^\perp\rangle\}$  is a basis of a qubit space, it follows that any  $M - k$  qubit pure state can be written as a superposition of tensor products of vectors in  $\{|m\rangle, |m^\perp\rangle\}$ . The Hamming weight then needs to be understood as the maximum number of  $|m^\perp\rangle$  showing in any term of the superposition [5].

**Lemma 3** (Lemma 2.7 of [4]). Let  $V_\delta := \text{span}\{P_\pi(|T\rangle^{\otimes(M-k)-w}|T^\perp\rangle^{\otimes w}) : \frac{w}{M-k} \leq \delta, \pi \in S_{M-k}\}$ , where  $S_{M-k}$  is the set of permutations of  $M - k$  elements, and  $P_\pi$  is the operator that permutes  $M - k$  qubits according to the permutation  $\pi$ . Let  $\Pi_{V_\delta}$  be a projector onto  $V_\delta$ . Let  $\Xi$  be the CPTP map describing the action of Distillation of Protocol 3. Let  $\rho$  be an  $M - k$  qubit state such that  $\text{Tr}(\Pi_{V_\delta}\rho) \geq 1 - \epsilon$ ; then,

$$\|\Xi(\rho) - |T\rangle\langle T|\|_1 \leq O((M - k)(\sqrt{35}\delta)^{(M-k)^c/2} + \epsilon), \quad (1)$$

where  $c \approx 0.406$  and  $\delta$  is chosen such that  $\delta \leq 0.14$ .

Now we will prove a lemma lower-bounding the number of copies of the magic state that must be measured in Testing, Protocol 3, such that at least some minimum number  $s'$  of them is measured by honest nodes with high probability.

**Lemma 4.** Let  $\mu \in (0, 1)$ , let  $s' \geq 1$  be some integer. Let  $H := (1 - \frac{1}{n} \lfloor \frac{n-1}{4} \rfloor) \in [3/4, 1]$ . In the testing procedure Protocol 3, if the number of measured copies of the magic state  $k$  satisfies the following:

$$k \geq \frac{2Hs' + \ln(\mu^{-1})/2 + \sqrt{2Hs' \ln(\mu^{-1}) + \ln^2(\mu^{-1})/4}}{2H^2}, \quad (2)$$

then

$$\Pr(k' < s') \leq \mu, \quad (3)$$

where  $k'$  is the number of copies of the magic state measured by the honest nodes.

*Proof.* For a sequence of IID Bernoulli random variables  $X_1, \dots, X_n$ , and some  $\lambda \in [0, 1]$ , Hoeffding’s inequality [6] ensures that

$$\Pr\left[\sum_1^k X_i \leq \mathbb{E}\left(\sum_1^k X_i\right) - \lambda k\right] \leq e^{-2\lambda^2 k}. \quad (4)$$

In other words, Hoeffding’s inequality bounds the probability that the fraction of observed 1’s in the sequence of random variables deviates from its expectation value by more than  $\lambda k$ . In Protocol 3, we can define a Bernoulli variable for each measured copy of the magic state as follows: The random variable  $X_i$  takes value 1 if and only if the copy  $i$  is sent to an honest node. Therefore, we have  $k' = \frac{1}{k} \sum_1^k X_i$  and  $\mathbb{E}(\frac{1}{k} \sum_1^k X_i) = (1 - \frac{1}{n} \lfloor \frac{n-1}{4} \rfloor) = H$ . Plugging this into Hoeffding’s inequality, we get

$$\Pr[k' \leq (H - \lambda)k] \leq e^{-2\lambda^2 k}. \quad (5)$$

Then by choosing  $\lambda$  and  $k$  such that  $\lambda = \frac{\mathbb{E}(\sum_1^k X_i) - s'}{k} = \frac{Hk - s'}{k}$  and  $e^{-2\lambda^2 k} = \mu$ , we get

$$\Pr(k' < s') \leq \mu, \quad (6)$$

and that  $k$  must satisfy

$$H^2 k^2 - [2Hs' + \ln(\mu^{-1})/2]k + s'^2 \geq 0, \quad (7)$$

from which, by solving the inequality for  $k$ , we get inequality (2). Note that since  $\mu$  can take any value in  $(0, 1)$ , the probability  $\Pr(k' < s')$  can be made arbitrarily small.

Finally we restate a Theorem from [5] saying that if Testing of Protocol 3 does not abort, then the state *before* Testing was already close to a space of states with a small Hamming weight.

*Lemma 5* (from Theorem 3 of [5]). Let  $|\phi_{AE}\rangle \in (\mathbb{C}^2)^M \otimes \mathcal{H}_E$  be a quantum state and let  $\beta = \{|v_0\rangle, |v_1\rangle\}$  be a fixed single-qubit basis. If we measure  $k$  random qubits of  $\text{Tr}_E(|\phi_{AE}\rangle\langle\phi_{AE}|)$  in the  $\beta$ -basis and all of the outcomes are  $|v_0\rangle$ , then with probability  $1 - e^{-\delta^2 k}$ , we have

$$|\phi_{AE}\rangle \in \text{span}\{P_\pi(|T\rangle^{\otimes M-w}|T^\perp\rangle^{\otimes w}) \otimes |\psi\rangle : \frac{w}{M} \leq \delta, \pi \in S_M, |\psi\rangle \in \mathcal{H}_E\}. \quad (8)$$

The lemma above has a useful corollary, namely that the state of remaining unmeasured qubits *after* Testing in Protocol 3 is close to a space of states with a small Hamming weight.

*Corollary 1* (from Lemma 5). Let  $|\phi_{AE}\rangle \in (\mathbb{C}^2)^M \otimes \mathcal{H}_E$  be a quantum state and let  $\beta = \{|v_0\rangle, |v_1\rangle\}$  be a fixed single-qubit basis. If among  $k$  randomly chosen qubits of  $\text{Tr}_E(|\phi_{AE}\rangle\langle\phi_{AE}|)$ ,  $k'$  of them are correctly measured in the  $B$ -basis and all of the outcomes are  $|v_0\rangle$  while  $k - k'$  are measured with an arbitrary positive operator-valued measure, then the state  $\rho$  on the remaining  $(M - k)$  qubits of  $\text{Tr}_E(|\phi_{AE}\rangle\langle\phi_{AE}|)$  is  $e^{-\delta^2 k'}$ —close to the subspace

$$V_\delta = \text{span}\left\{P_\pi(|T\rangle^{\otimes (M-k)-w}|T^\perp\rangle^{\otimes w}) : \frac{w}{M-k} \leq \delta, \pi \in S_{M-k}\right\}. \quad (9)$$

In other words, if  $\Pi_{V_\delta}$  is a projector on the above subspace, then  $\text{Tr}(\Pi_{V_\delta}\rho) \geq 1 - e^{-\delta^2 k'}$ .

Now we are ready to state the security of our new verification procedure.

*Theorem 1.* Let  $\Gamma$  be the completely positive trace-preserving (CPTP) map describing the action of Testing, Protocol 3, and let  $\Xi$  be a CPTP map describing the action of Distillation, Protocol 3. Then we have

$$\|\Xi \circ \Gamma(\rho)_{\text{not abort}} - |T\rangle\langle T|\|_1 \leq O((M - k)(\sqrt{35}\delta)^{(M-k)^c/2} + e^{-\delta^2 s'} + \mu), \quad (10)$$

where  $c \approx 0.406$ . Recall that  $s$  is the security parameter of the whole MPQC protocol. By setting  $M - k = s$ ,  $s' = s$ , and  $\mu = 2^{-s}$ , Eq. (10) becomes

$$\|\Xi \circ \Gamma(\rho)_{\text{not abort}} - |T\rangle\langle T|\|_1 \leq O(2^{-\Omega(s)} + e^{-\delta^2 s} + 2^{-s}) = 2^{-\Omega(s)}. \quad (11)$$

Note that, by Lemma 4, setting  $s' = s$  and  $\mu = 2^{-s}$  forces  $k$  to satisfy

$$k \geq \frac{2Hs + s/2 + \sqrt{2Hs^2 + s^2/4}}{2H^2} = \left(\frac{2H + 1/2 + \sqrt{2H + 1/4}}{2H^2}\right)s = \Theta(s). \quad (12)$$

Overall, we have that Eq. (11) holds for  $M = (M - k) + k = \Theta(s)$ .

#### ACKNOWLEDGMENTS

We thank J. G. Hölting for point us to the error in the original article. We thank J. Helsen and B. Dirkse for useful comments and feedback on this erratum.

- 
- [1] C. Crépeau, D. Gottesman, and A. Smith, in *Advances in Cryptology—EUROCRYPT 2005*, edited by R. Cramer (Springer, Berlin, 2005), pp. 285–301.
- [2] S. Bravyi and A. Kitaev, *Phys. Rev. A* **71**, 022316 (2005).
- [3] A. Pirker, V. Dunjko, W. Dür, and H. J. Briegel, *New J. Phys.* **19**, 113012 (2017).
- [4] Y. Dulek, A. B. Grilo, S. Jeffery, C. Majenz, and C. Schaffner, in *Advances in Cryptology—EUROCRYPT 2020*, edited by A. Canteaut and Y. Ishai (Springer International, Cham, 2020), pp. 729–758.
- [5] N. J. Bouman and S. Fehr, in *Advances in Cryptology—CRYPTO 2010*, edited by T. Rabin (Springer, Berlin, 2010), pp. 724–741.
- [6] W. Hoeffding, *J. Am. Stat. Assoc.* **58**, 13 (1963).