Computing on quantum shared secrets

Yingkai Ouyang, Si-Hui Tan, Liming Zhao, and Joseph F. Fitzsimons

Phys. Rev. A **96**, 052333 — Published 27 November 2017

DOI: 10.1103/PhysRevA.96.052333

Computing on quantum shared secrets

Yingkai Ouyang,[1, *] Si-Hui Tan,[1] Liming Zhao,[1] and Joseph F. Fitzsimons[1, 2]
[1] *Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

A (k,n)-threshold secret-sharing scheme allows for a string to be split into n shares in such a way that any subset of at least k shares suffices to recover the secret string, but such that any subset of at most $k-1$ shares contains no information about the secret. Quantum secret-sharing schemes extend this idea to the sharing of quantum states. Here we propose a method of performing computation securely on quantum shared secrets. We introduce a (n,n)-quantum secret sharing scheme together with a set of protocols that allow quantum circuits to be evaluated securely on the shared secret without the need to decode the secret. We consider a multipartite setting, with each participant holding a share of the secret. We show that if there exists at least one honest participant, no group of dishonest participants can recover any information about the shared secret, independent of their deviations from the protocol.

The connected nature of modern computing infrastructure has led to the widespread adoption of distributed and delegated computation [1], with hard computational tasks routinely delegated to remote computers. In such a setting, the computation's security is a real concern. In the field of quantum cryptography, aside from quantum key distribution [2, 3], quantum protocols have appeared for secure computation tasks such as secure multi-party computation [4], blind computation [5–8] and verifiable delegated computation [9–13]. We focus on a different form of secure computation, namely the evaluation of quantum circuits on shared secrets.

A secret sharing scheme, keeps an r-bit string $\mathbf{r}$ as a secret, via encryption into an s-bit string $\mathbf{s}$. These s bits are subsequently distributed among n parties, with the intention that whenever the colluding parties are too few, they cannot perfectly recover the secret $\mathbf{r}$. Reversibility of the encryption allows the secret $\mathbf{r}$ to be recovered when all of the n-parties assemble the data that they were distributed. In a (k,n)-threshold scheme for classical secret sharing [14, 15], no group with fewer than k colluding parties can reconstruct the secret $\mathbf{r}$, and any k parties can reconstruct $\mathbf{r}$. Similarly in a (k,n)-threshold quantum secret sharing scheme, a secret quantum state of s qubits is shared among n parties such that no group fewer than k colluding parties can reconstruct the secret quantum state [16–20], and any k parties can reconstruct the secret quantum state. Here, we present an (n,n)-threshold quantum secret sharing scheme that also supports provably secure evaluation of quantum circuits on the shared secret, where the size of each share is independent of the number of parties.

Threshold secret sharing schemes that support computation in the classical context have been extensively studied. When the parties interact only via broadcast channels and if the size each party's share grows with n, arbitrary Boolean functions can be computed on (k,n)-classical threshold secret sharing schemes for any k [21]; if instead the size of each party's share must be equal to the secret's size, only linear functions can be computed whenever $k \geq 2$ [21]. The problem of only being able to compute linear functions in a theshold secret sharing scheme is often circumvented by assuming its verifiability [22]. However verifiable secret sharing [23] is impossible without an honest majority when only broadcast channels are permitted [24]. Indeed previous schemes for multipartite quantum computation build upon quantum verifiable sharing schemes which also require an honest majority [25, 26]. Since our scheme works with at least an honest party, it is not a generalization of any classically existing scheme to the quantum case, and is markedly different from previous schemes for secure multipartite quantum computation.

Our secret sharing scheme with computation is closely related to quantum homomorphic encryption schemes [27–31], that allow the performed quantum computation to be public and require the decoding algorithm to be independent of the depth of the computation. Indeed, we are motivated by a quantum homomorphic encryption scheme [29] that supports transversal evaluations of Clifford gates, and present a secret sharing scheme that allows the evaluation of Clifford gates by requiring the n non-interacting parties to perform the corresponding Clifford operations in parallel. A constant number t of non-Clifford gates can also be implemented securely via a coordinated gate teleportation using logical magic states. Our encoding is based on a randomized stabilizer code, and indeed in a similar manner it is possible to derive a range of secret sharing schemes which allow for varying non-universal combinations of gates to be evaluated locally (and hence securely) based on error-correction codes which allow transversal evaluation of these gates. Our innovation is two fold: we show how to achieve an (n,n) threshold scheme, which is not possible based on any single quantum error-correction code due to upper bounds on the distance [32], and we show that universality can be achieved through the use of gate-teleportation using magic states. While this second claim may seem an obvious consequence of corresponding results in quantum fault-tolerance, this does not directly follow. Rather, it is important to show that the communication necessary to apply correction operators following gate teleportation cannot be used to compromise the security of the shared secret, even when all but one party behave dishonestly. Since the security of our scheme is independent of the security of the quantum homomorphic encryption scheme in Ref. [29], the no-go results for fully quantum homomorphic encryption schemes with both

[*] Electronic address: yingkai_ouyang@sutd.edu.sg

perfect [33] and imperfect [34] information theoretic security do not limit the class of circuits which can be evaluated.

Our secret sharing scheme comprises of four procedures as described in Protocol 1. We label qubits according to a 2-dimensional arrangement as depicted in Fig. 1. In the input procedure of Protocol 1, $N = s+t$ qubits are initialized on a single column, with the first s qubits containing the quantum secret, and the last t qubits each initialized in the magic state $\tau = \frac{I}{2} + \frac{X+Y}{2\sqrt{2}}$, where I, X, Y, and Z are the usual Pauli matrices. These magic states are consumed during the evaluation in reverse order, starting from the last row. We focus on the case where $n-1$ is divisible by 4. This is not a limiting factor, since one can prepare $\lceil \frac{n-1}{4} \rceil + 1$ shares and give multiple shares to a single party. In the encoding procedure of Protocol 1, $n-1$ additional columns of N qubits in the maximally mixed state are appended. This yields an Nn-qubit quantum state arranged in a grid with N rows and n columns. Subsequently a unitary encoding U is applied on the Nn qubits, which spreads the quantum secret from the first column to all the n columns. Here $U = U_1 \otimes \cdots \otimes U_N$ is a tensor product of the unitaries $U_1, \dots, U_N$, where each U_x acts only on the x-th row of qubits and comprises of only CNOT gates. Specifically $U_x = B_x A_x$, where (i) A_x comprises of $n-1$ commuting CNOT gates with controls all on the first column and targets on each of the remaining columns, and (ii) B_x comprises of $n-1$ commuting CNOT with targets all on the first column and controls on every other column. Although U_x is a fixed unitary, the induced encoding is random because $n-1$ of the qubits that U_x acts on are random; the qubits from the second column to the last column are initialized as either $|0\rangle$ or $|1\rangle$ with probability $1/2$. This random encoding maps the quantum secret into a highly mixed state [29]. In the sharing procedure of Protocol 1, the Nn-qubit quantum state is shared equally among n parties, with each party receiving a single column of N qubits. In decoding procedure of Protocol 1, the n shares are assembled, the inverse encoding circuit $U^\dagger$ is performed, and all but the first column of qubits are discarded, which leaves the quantum secret.

To evaluate a quantum circuit on the shared secret, each party performs quantum computation only on their share of the quantum state. We consider the approximately universal model of quantum computation based on a discrete set of gates composed of Clifford group gates and a single non-Clifford group gate, in this case $T = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$ although other choices are possible. Quantum circuits composed of arbitrarily many Clifford gates and up to some constant number t of T-gates can be evaluated on the shared secret. We consider the evaluation of a sequence $V = (V_1, \dots, V_L)$ of such gates on the s-qubit quantum secret shared by n parties. The gates $V_1, \dots, V_L$ are unitary matrices on s qubits and are assumed to be known to every party. Using the knowledge of V, each party implements a sequence of operations on their share of the qubits, as specified in Protocol 2. The computation is performed between the sharing and decoding procedure of Protocol 1, as we now describe.

Protocol 1 Secret sharing scheme

Here, $\mathscr{H}_{x,y}$ labels the qubit on the x-th row and the y-th column, and $\mathscr{R}_x$ labels the qubits on the x-th row.

1. **Input:** From the s-qubit quantum secret, assign the x-th qubit to $\mathscr{H}_{x,1}$ for $x = 1, \dots, s$. Assign τ to each of $\mathscr{H}_{N-k+1,1}, \dots, \mathscr{H}_{N,1}$.
2. **Encoding:** To prepare the x-th logical qubit for $x = 1, \dots, N$:
   (a) Prepare each of $\mathscr{H}_{x,2}, \dots, \mathscr{H}_{x,n}$ in state $\frac{I}{2}$.
   (b) Apply A_x: Perform a CNOT with control on $\mathscr{H}_{x,1}$ and target on $\mathscr{H}_{x,y}$ for every $y = 2, \dots, n$.
   (c) Apply B_x: Perform a CNOT with target on $\mathscr{H}_{x,1}$ and control on $\mathscr{H}_{x,y}$ for every $y = 2, \dots, n$.
3. **Sharing:** Assign the qubits in the y-th column to the y-th share for $y = 1, \dots, n$.
4. **Decoding:**
   (a) Assemble the n shares.
   (b) For each $x = 1, \dots, N$, implement B_x followed by A_x on $\mathscr{R}_x$.
   (c) Output the qubits in the first column, discarding all other qubits.

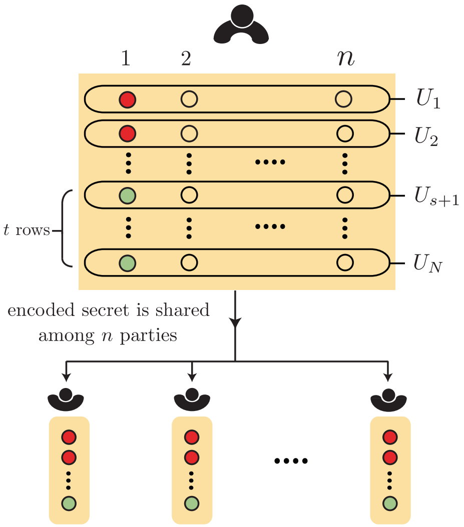

FIG. 1. The upper portion of the figure shows the secret and the magic states, located on the first column, and shaded red and green respectively. The unshaded qubits are initialized in the maximally mixed state. The unitaries $U_1, \dots, U_N$ spread the states from qubits in the first column to qubits in the remaining columns, such that the encoded secret resides in the first s rows of qubits. Each party receives a single column of qubits.

When V_i is a Clifford gate applying non-trivially on some set of logical qubits, each party performs V_i on the corresponding subset of their column of qubits, thereby collectively implementing $V_i^{\otimes n}$. This procedure is depicted in Fig. 2A for single qubit Clifford gates, and Fig. 2B for a CNOT gate. Let $\mathscr{P} = \{I, X, Y, Z\}$ denote the set of the Pauli matrices. Then the divisibility of $n-1$ by 4 implies that for $\sigma \in \mathscr{P}$,

$$U_x(\sigma \otimes I^{\otimes n-1})U_x^\dagger = \sigma^{\otimes n}. \tag{1}$$

Protocol 2 Gate evaluation on shared quantum secret

Given a gate V_i to be evaluated on the shared secret:

- **Clifford group:** If V_i is in the Clifford group each party applies V_i to their share.
- **T-gates:** If V_i is a T-gate on qubit j, each party y does as follows
  1. Apply a CNOT gate controlled by qubit j and targeted on qubit $N-k+1$.
  2. Apply a CNOT gate controlled by qubit $N-k+1$ and targeted on qubit j.
  3. Measure qubit $N-k+1$ in the computational basis, and broadcast the result m_y.
  4. If the parity of $\mathbf{m} = (m_1, \ldots, m_n)$ is odd, apply the correction operator SX to qubit j.

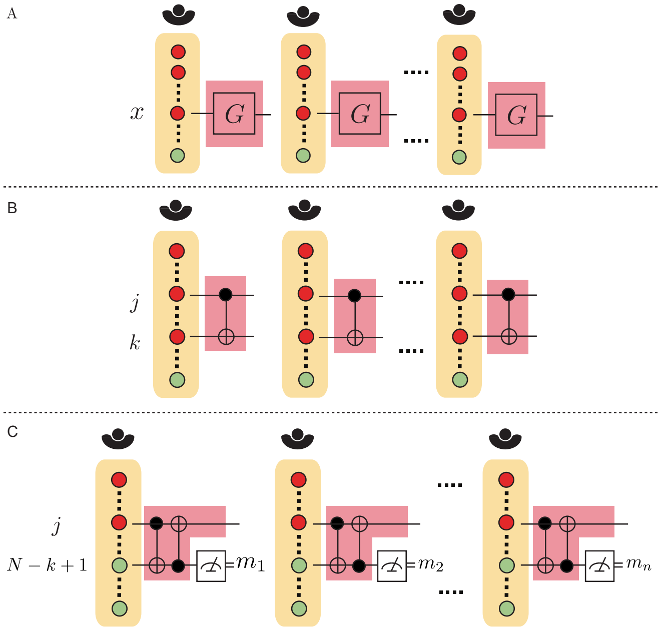

FIG. 2. The secret qubits are shaded red and the others in green. A) Multipartite implementation of a logical Clifford gate G on the x-th row. B) Multipartite implementation of a logical CNOT operator. C) A logical gate teleportation protocol that implements a logical T-gate on the j-th logical qubit without the Clifford correction. Collectively, the qubits on the subsequently measured row are initialized in a logical magic state. Correction proceeds by broadcasting the measurement outcomes, and having each party apply a single Clifford gate SX on the j-th qubit only when $\mathbf{m}$ has odd parity.

Since V_i is in the Clifford group, it maps the Pauli group onto itself,

$$U_x(V_i\sigma V_i^\dagger \otimes I^{\otimes n-1})U_x^\dagger = V_i^{\otimes n}\sigma^{\otimes n}\left(V_i^\dagger\right)^{\otimes n}. \tag{2}$$

Hence the transversal Clifford group gates correspond to the logical Clifford group gates on our random codespace [29].

Via gate teleportation, one can perform a constant number t of T-gates on the quantum secret. For each T-gate to be performed, a logical magic state $\widetilde{\tau} = \frac{I^{\otimes n}}{2^n} + \frac{X^{\otimes n}+Y^{\otimes n}}{2^n\sqrt{2}}$ is prepared. This is achieved by the input and encoding procedures of Protocol 1, however one could replace this pre-sharing of magic states with a procedure for the parties to interactively prepare states on demand without the involvement of the initial sharer. Each of these logical magic states is located on the last t rows. To prepare $\widetilde{\tau}$ on the x-th row, the first qubit in the x-th row is initialized as $TH|0\rangle$ with the remaining qubits maximally mixed. The encoding unitary U_x is subsequently applied. To evaluate the k-th T-gate on qubit j of the shared secret, each party applies a CNOT with control on the j-th qubit and target on the k-th last qubit of their share. They then apply a CNOT with control on the k-th last qubit and target on the j-th qubit. Each party y then measures the k-th last qubit in the $\{|0\rangle, |1\rangle\}$ basis and broadcasts the measurement result m_y to every other party over a public classical channel. Lastly, if the parity of the measurement results $\mathbf{m}$ is odd, each party applies a single-qubit Clifford gate SX on the j-th qubit. If the parity is even, no such correction is necessary. Fig. 2C depicts this procedure. This method of evaluating each T-gate amounts to implementing a logical gate teleportation protocol consuming one magic state [35].

Denoting $\bar{I} = I^{\otimes n}$, $\bar{X} = X^{\otimes n}$, $\bar{Y} = Y^{\otimes n}$ and $\bar{Z} = Z^{\otimes n}$, the correct implementation of a logical T-gate on the state $\widetilde{\rho} = 2^{-n}(\bar{I} + a\bar{X} + b\bar{Y} + c\bar{Z})$ shared by the j-th qubit of each party must yield $\frac{1}{2^n}\left(\bar{I} + \frac{(a-b)}{\sqrt{2}}\bar{X} + \frac{(a+b)}{\sqrt{2}}\bar{Y} + c\bar{Z}\right)$. This follows from the conjugation relations for the T-gate given by $TXT^\dagger = \frac{1}{\sqrt{2}}(X+Y)$, $TYT^\dagger = \frac{Y-X}{\sqrt{2}}$, and $TZT^\dagger = Z$. Every party then performs the CNOT gates and performs the measurements as depicted in Fig. 2C. The parity of $\mathbf{m} = (m_1, \ldots, m_n)$ is equivalent to the observable $\bar{Z}$ on the k-th last qubit of each share. If the parity is even, the resultant state on the j-th qubit of every party is collectively

$$\widetilde{\rho}_{even} = \frac{\bar{I}}{2^n} + \frac{(a-b)\bar{X}}{2^n\sqrt{2}} + \frac{(a+b)\bar{Y}}{2^n\sqrt{2}} + \frac{c\bar{Z}}{2^n}, \tag{3}$$

and the evaluation of the T-gate is successful. If the parity is odd, however, the resultant state of these qubits is

$$\widetilde{\rho}_{odd} = \frac{\bar{I}}{2^n} + \frac{(a+b)\bar{X}}{2^n\sqrt{2}} + \frac{(a-b)\bar{Y}}{2^n\sqrt{2}} - \frac{c\bar{Z}}{2^n}. \tag{4}$$

Applying SX to each qubit transforms the state into $\widetilde{\rho}_{even}$, resulting in a correct evaluation of the T-gate.

A (k,n)-threshold quantum secret-sharing scheme [17, 18] is a quantum operation that maps a secret quantum density matrix to an encoded state that can be divided among n parties such that (1) any k or more parties can perfectly reconstruct the secret quantum state, and (2) any $k-1$ or fewer parties can collectively deduce no information about the secret quantum state. Protocol 1 satisfies the first property when $k=n$, since the encoding procedure is perfectly reversible with inverse operation given by the specified decoding procedure. For the second property, consider the result of encoding a state

$$\rho_{\text{secret}} = 2^{-s}\sum_{\sigma\in\mathscr{P}^{\otimes s}} w_\sigma \sigma \tag{5}$$

according to Protocol 1. Here $\sigma = \sigma_1 \otimes \ldots \otimes \sigma_s$ and $w_\sigma = 1$ when σ is the trivial Pauli operator, $\sigma = I^{\otimes s}$. It is the coefficients w_σ for the non-trivial Pauli operators σ in $\mathscr{P}^{\otimes s}$ that collectively define the quantum secret. From Eq. 1, the resulting state is

$$\tilde{\rho}_{\text{secret}} = 2^{-s} \left(\sum_{\sigma \in \mathscr{P}^{\otimes s}} w_\sigma \sigma^{\otimes n} \right) \otimes \tilde{\tau}^{\otimes t}, \tag{6}$$

where the tensor product in $\sigma^{\otimes n}$ is taken across different shares of the secret. Property (2) follows, since the reduced density matrix for any subsystem of $n-1$ shares (i.e. $n-1$ columns) is necessarily the maximally mixed state, because all non-trivial σ are traceless.

Regarding the security of Protocol 2, we consider the state of the system across a bipartition between a single honest party, who follows the protocol, and the remaining $n-1$ parties who are unrestricted in their actions. We show that the bits broadcast by the honest party are uniformly random and independent of the other parties' actions. Given a sequence of gates $(V_1, \ldots, V_L)$ with the honest party acting as described by Protocol 2, our strategy is to show that after evaluation of the ℓ-th gate, the state of the system has the form

$$\rho_{\text{joint}}^{(\ell)} = \sum_{\substack{\sigma \in \mathscr{P}^{\otimes s} \\ \theta \in \{I,X,Y\}^{\otimes t-k}}} b_{\sigma,\theta}^{(\ell)} \left(\frac{\sigma \otimes \theta}{2^N} \right) \otimes \chi_{\sigma,\theta}^{(\ell)}, \tag{7}$$

where $k \leq \ell$ is the number of T-gates in $(V_1, \ldots, V_\ell)$, $\{b_{\sigma,\theta}^{(\ell)}\}$ is a set of scalars, and $\{\chi_{\sigma,\theta}^{(\ell)}\}$ is a set of operators on the dishonest parties' system. We have excluded the honest party's measured qubits, as these are in a product state with the rest of the system.

Our proof is inductive. We assume that the system is in a state $\rho_{\text{joint}}^{(\ell-1)}$ of the form of Eq. 7 after evaluating the first $\ell-1$ gates. If V_ℓ is a Clifford group gate, the honest party applies V_ℓ on some subset of the first s qubits of their share, while the dishonest parties may perform any completely positive and trace preserving map on their side of the bipartition. Since $V_\ell I^{\otimes s} V_\ell^\dagger = I^{\otimes s}$ and $V_\ell \mathscr{P}^{\otimes s} V_\ell^\dagger = \mathscr{P}^{\otimes s}$, linearity of the operation applied by the dishonest parties on their side of the bipartition results in the state $\rho_{\text{joint}}^{(\ell)}$ in the form of Eq. 7 as claimed. When V_ℓ is a T-gate on qubit j, the situation is more complicated. Since honest party's actions only affect the j-th qubit and k-th last qubit of his share, the effect of these actions on all combinations of Pauli operators on these two qubits which can have non-zero coefficients in $\rho_{\text{joint}}^{(\ell-1)}$ is given by the first column of Table I. By applying CNOT operations as prescribed by the first two steps of the T-gate procedure in Protocol 2, the honest party transforms these operators into the corresponding Pauli operators given by the second column of Table I. The absence of $I \otimes Z$ implies that the expectation for m_{H}, the measurement result of the honest party's measurement, is precisely zero. Hence m_{H} is uniformly random and independent of the non-trivial weights $\{b_{\sigma,\theta}\}$. The measurement's effect on the Pauli operators is given by the third column of Table I, which implies that the resulting state is in the form of Eq. 7. Since the correction SX is a local Clifford group operator, the final state $\rho_{\text{joint}}^{(\ell)}$ is of the correct form independent of the parity of $\mathbf{m}$. Since the initial state after sharing, given by Eq. 6 is of the form of Eq. 7, the induction hypothesis holds for all $0 \leq \ell \leq L$, and the measurement results of the honest party convey no information usable by the dishonest participants to recover ρ_{secret}.

$\sigma_j \otimes \theta_k$	$\tau_{j,k}$	$(I \otimes \langle m_{\text{H}}\|)\tau_{j,k}(I \otimes \|m_{\text{H}}\rangle)$
$I \otimes I$	$I \otimes I$	I
$I \otimes X$	$X \otimes X$	0
$I \otimes Y$	$Y \otimes X$	0
$X \otimes I$	$I \otimes X$	0
$X \otimes X$	$X \otimes I$	X
$X \otimes Y$	$Y \otimes I$	Y
$Y \otimes I$	$Z \otimes Y$	0
$Y \otimes X$	$Y \otimes Z$	$(-1)^{m_{\text{H}}} Y$
$Y \otimes Y$	$-X \otimes Z$	$(-1)^{m_{\text{H}}+1} X$
$Z \otimes I$	$Z \otimes Z$	$(-1)^{m_{\text{H}}} Z$
$Z \otimes X$	$Y \otimes Y$	0
$Z \otimes Y$	$X \otimes Y$	0

TABLE I. The values of (i) $\sigma_j \otimes \theta_k$, (ii) the resulting operator $\tau_{j,k}$ after applying steps 1 and 2 of the T-gate procedure of Protocol 2, and (iii) $(I \otimes \langle m_{\text{H}}|)\tau_{j,k}(I \otimes |m_{\text{H}}\rangle)$ for $\sigma_k \in \mathscr{P}$, $\theta_k \in \{I, X, Y\}$.

Our scheme therefore represents an (n,n)-threshold secret sharing scheme that also allows evaluation of quantum circuits on the shared secret without lowering the threshold. While the complexity of such circuits is limited in terms of the number of T-gates to the number of corresponding magic states incorporated in the initial sharing, the possibility of creating such states as needed without involving the initial sharer presents an interesting avenue for future research. Intuitively, the security of our scheme is based on a randomized error correction code which leaves only weight n operators constant while admitting transversal Clifford gates. This suggests that the use of less random error-correction codes will allow for (k,n)-threshold schemes for other values of k.

The authors thank Mahboobeh Houshmand and Monireh Houshmand for useful discussions. The authors acknowledge support from Singapore's Ministry of Education and National Research Foundation. JFF and ST acknowledge support from the Air Force Office of Scientific Research under AOARD grant FA2386-15-1-4082. This material is based on research funded in part by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01.

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., Communications of the ACM **53**, 50 (2010).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (New York, 1984), vol. 175.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991), URL `http://link.aps.org/doi/10.1103/PhysRevLett.67.661`.

[4] C. Crépeau, D. Gottesman, and A. Smith, in *Proceedings of the Thiry-fourth Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, USA, 2002), STOC '02, pp. 643–652, ISBN 1-58113-495-9, URL `http://doi.acm.org/10.1145/509907.510000`.

[5] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on* (IEEE, 2009), pp. 517–526.

[6] T. Morimae and K. Fujii, Nature communications **3**, 1036 (2012).

[7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[8] A. Broadbent, Canadian Journal of Physics **93**, 941 (2015).

[9] D. Aharonov, M. Ben-Or, and E. Eban, Proceedings of Innovations in Computer Science (2010).

[10] B. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 7446 (2013).

[11] J. F. Fitzsimons and E. Kashefi, arXiv preprint arXiv:1203.5217 (2012).

[12] T. Morimae, Physical Review A **89**, 060302 (2014).

[13] M. Hayashi and T. Morimae, Physical Review Letters **115**, 220502 (2015).

[14] A. Shamir, Commun. ACM **22**, 612 (1979), ISSN 0001-0782, URL `http://doi.acm.org/10.1145/359168.359176`.

[15] G. R. Blakley, Proc. of the National Computer Conference1979 **48**, 313 (1979).

[16] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999), URL `http://link.aps.org/doi/10.1103/PhysRevA.59.1829`.

[17] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999), URL `http://link.aps.org/doi/10.1103/PhysRevLett.83.648`.

[18] D. Gottesman, Phys. Rev. A **61**, 042311 (2000), URL `http://link.aps.org/doi/10.1103/PhysRevA.61.042311`.

[19] Z.-j. Zhang, Y. Li, and Z.-X. Man, Physical Review A **71**, 044301 (2005).

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

[21] A. Beimel, M. Burmester, Y. Desmedt, and E. Kushilevitz, SIAM Journal on Discrete Mathematics **13**, 324 (2000).

[22] R. Cramer, I. Damgård, and U. Maurer, in *Advances in CryptologyEUROCRYPT 2000* (Springer, 2000), pp. 316–334.

[23] T. Rabin and M. Ben-Or, in *Proceedings of the twenty-first annual ACM symposium on Theory of computing* (ACM, 1989), pp. 73–85.

[24] M. Hirt and V. Zikas, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, 2010), pp. 466–485.

[25] C. Crépeau, D. Gottesman, and A. Smith, in *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing* (ACM, 2002), pp. 643–652.

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

[27] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, Phys. Rev. Lett. **109**, 150501 (2012), URL `http://link.aps.org/doi/10.1103/PhysRevLett.109.150501`.

[28] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, Scientific Reports **6**, 33467 (2016).

[29] Y. Ouyang, S.-H. Tan, and J. Fitzsimons, arXiv preprint arXiv:1508.00938 (2015).

[30] A. Broadbent and S. Jeffery, in *Annual Cryptology Conference* (Springer, 2015), pp. 609–629.

[31] Y. Dulek, C. Schaffner, and F. Speelman, pp. 3–32 (2016).

[32] A. Ashikhmin and S. Litsyu, IEEE Transactions on Information Theory **45**, 1206 (1999).

[33] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. A **90**, 050303 (2014), URL `http://link.aps.org/doi/10.1103/PhysRevA.90.050303`.

[34] M. Newman and Y. Shi (2016), private communication.

[35] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000), URL `http://link.aps.org/doi/10.1103/PhysRevA.62.052316`.