Generalized Teleportation and Entanglement Recycling

Sergii Strelchuk,[1,*] Michał Horodecki,[2] and Jonathan Oppenheim[3]

[1]*Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom*
[2]*Institute for Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[3]*Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom, Department of Physics & Astronomy, University College of London, London WC1E 6BT, United Kingdom*

(Received 13 September 2012; published 4 January 2013; corrected 30 January 2013; corrected 13 March 2014)

We introduce new teleportation protocols which are generalizations of the original teleportation protocols that use the Pauli group and the port-based teleportation protocols, introduced by Hiroshima and Ishizaka, that use the symmetric permutation group. We derive sufficient conditions for a set of operations, which in general need not form a group, to give rise to a teleportation protocol and provide examples of such schemes. This generalization leads to protocols with novel properties and is needed to push forward new schemes of computation based on them. Port-based teleportation protocols and our generalizations use a large resource state consisting of N singlets to teleport only a single qubit state reliably. We provide two distinct protocols which recycle the resource state to teleport multiple states with error linearly increasing with their number. The first protocol consists of sequentially teleporting qubit states, and the second teleports them in a bulk.

DOI: 10.1103/PhysRevLett.110.010505 PACS numbers: 03.67.Hk, 03.65.Ta, 03.67.Ac

Teleportation lies at the very heart of quantum information theory, being the pivotal primitive in a variety of tasks. Teleportation protocols are a way of sending an unknown quantum state from one party to another using a resource in the form of an entangled state shared between two parties, Alice and Bob, in advance. First, Alice performs a measurement on the state she wants to teleport and her part of the resource state, then she communicates the classical information to Bob. He applies the unitary operation conditioned on that information to obtain the teleported state.

A notable use of teleportation is in relation to computing, where it plays a key role enabling universal quantum computation and establishing a strong link between a particular teleportation protocol and a kind of computation possible to be implemented using it [1–3].

Recently, Hiroshima and Ishizaka introduced *port-based teleportation* [2] which has the distinct property that Bob does not need to apply a correction after Alice's measurement. It is an important primitive for programmable quantum processors [2,4–6], which rely on an efficient way of storing a unitary transformation and acting it on an arbitrary quantum state. This protocol evades the fundamental limitations of the no-go theorem proved in Ref. [6], which states that universal deterministic programmable quantum processors cannot exist. Even though the protocol makes it possible to execute arbitrary instructions deterministically, the result will be inherently noisy.

Port-based teleportation has already found its use in instantaneous nonlocal quantum computation [7]. In the latter task, using it as the underlying teleportation routine dramatically reduced the amount of entanglement required to perform it. Such computations proved to be instrumental in attack schemes on position-based quantum cryptography [8–11]. Currently, it is known that the minimum amount of entanglement an adversary needs to perform a successful attack on the scheme must be at least linear in the number of communicated qubits [10]. Also, an adversary having access to at most an exponential amount of entanglement can successfully break any position-based cryptography scheme [7]. However, we do not know how much entanglement is necessary to break all schemes of this kind. Any improvement of the underlying teleportation protocol will invariably lead to the decrease of the amount of entanglement required to break them, and potentially render such attacks more feasible.

Port-based teleportation works as follows: at the beginning of the protocol Alice and Bob share a resource state, which consists of N singlets $|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, termed *ports*. Alice performs a measurement in the form of positive-operator valued measure (POVM) on the joint system, that includes the state she wants to teleport and her resource state. She obtains the measurement outcome i from 1 to N and communicates it to Bob, who traces out all the port subsystems except for the ith one, discarding the remaining entanglement. The ith port now contains the teleported state.

Although conceptually appealing, port-based teleportation relies on the properties of the symmetric permutation group, which limits its scope. In particular, it restricts the use of such teleportation protocols to implement gates specific to the underlying group. In the case of ordinary teleportation these gates correspond to Clifford-type computation [3]. Another drawback of port-based teleportation is that it requires an enormous amount of entanglement in the resource state to teleport a single quantum state with high fidelity. This makes it extremely ill-suited for practical

purposes. Decreasing the amount of entanglement required to teleport a sequence of quantum states will result in more efficient storage of the program encoded in unitary transformation as well as making efficient instantaneous nonlocal quantum computation, and tasks that depend on it.

In this Letter we address the two issues above. First, we find sufficient condition for the generalized teleportation protocols, which is needed to push forward new schemes of computation based on them. Second, we introduce a recycling scheme, which drastically reduces the amount of entanglement used in port-based teleportation, and therefore allows for efficient attacks on position based cryptography.

To tackle the first problem, we find sufficient condition that Alice's operations have to satisfy in order to make them amenable to be used in more general teleportation protocols and provide examples. From a group-theoretic perspective all currently known teleportation protocols can be classified into two kinds: those that exploit the Pauli group [1] and those, which use the symmetric permutation group [2]. Such a simple change of the underlying group structure leads to two protocols with striking differences in the properties: the former protocol uses a finite resource state to teleport the state perfectly, but the receiver must make the correction to obtain the state, whereas the latter protocol requires an infinitely big resource state to teleport the state perfectly, while not needing a correction on the receiver's side. The former teleportation scheme was used in the celebrated result of Gottesman and Chuang [3] to perform universal Clifford-based computation using teleportation over the Pauli group. The generalized teleportation protocol introduced in this Letter embraces both known protocols, and paves the way for protocols which lead to programmable processors capable of executing new kinds of computation beyond Clifford-type operations. The operations in the generalized teleportation protocol need not form a group. Also, because teleportation is known to be intimately connected to the variety of other fundamental tasks in quantum information processing [12], its generalized version brings the potential for protocols with new properties, which depend on its implementation.

To address the second problem we introduce two distinct protocols, which recycle the entanglement available in the resource state. Using a single resource state comprised of N ports, they teleport any number of systems which is sublinear in N with an error that linearly increases with the number of teleported states. The first protocol amounts to sequentially teleporting qubit states, recycling the original resource state. This can be viewed as the application of the original port-based teleportation with the resource state, followed by a resource recycling step. The resource degrades with every teleported state. In the second protocol Alice teleports her states in one go, performing the POVM, which randomly assigns each of the teleported states to one of the ports. The latter protocol, rather remarkably, provides the same finite case and asymptotic performance as the former: both of the protocols operate with an error, which is linear in the number of systems teleported. The similar idea about recycling the entangled state was used in the context of a remote state preparation protocol [13]. The ability to recycle entanglement in such protocols has an immediate effect on the entanglement consumption of the instantaneous computation and position-based cryptography: an adversary may conduct an attack on any position-based cryptography scheme using a linear amount of entanglement in the number of communicated qubits for the case when communicating parties are constrained to product measurements.

Generalized teleportation.—Until now, group-theoretic aspects of the teleportation protocols were largely overlooked. Currently, there are two distinct groups, which undergird different teleportation protocols. The first one is the Pauli group, which appeared in the first teleportation protocol of Bennett *et al.* [1]. Another one, the symmetric permutation group $\mathcal{S}_N$ was implicitly used in the port-based teleportation protocol of Refs. [2,5]. Therefore, we recast the description of the port-based teleportation protocol to elicit its connection with $\mathcal{S}_N$, and provide the basis for generalized teleportation protocols.

This port-based teleportation protocol [2] can be equivalently viewed as such where Alice applies a measurement, which corresponds to the action of some element g from some set G on her total state. In the next step, Alice sends the description of g to Bob who then applies the unitary transformation $U_g^\dagger$ conditioned on g to his overall state, to reach some predefined terminating state. We say that the teleportation protocol $\mathcal{P}$ successfully *terminates* when Bob obtains the state $\sigma_B \otimes \phi_{B_0}$, where ϕ_{B_0} is the teleported state, and σ_B is the state of the remaining ports. In the case of port-based teleportation U_g acts as a swap operation between the port where the state was teleported and the first port.

Now we consider the generalized form of the teleportation protocol where all the operations on Alice are members of some set G, $|G| = K$, which in general need not form a group. The protocol that is able to teleport an unknown quantum state reliably under Alice's operations which belong to the set G is denoted as $\mathcal{P}^G$. Recall that the task of teleportation is in correspondence with the problem of signal discrimination for qudits [7]: the probability $p_s(G)$ of successfully discriminating a set of signals $\{\eta_g\}_{g\in G}$, where

$$\eta_g = U_g(\mathrm{Tr}_{B_1\ldots B_N\setminus B_g}|\Psi_{\mathrm{in}}\rangle\langle\Psi_{\mathrm{in}}|_{AB})U_g^\dagger \tag{1}$$

after Alice applied her operation is related to the fidelity of teleportation protocols in the qudit case as $F(\mathcal{P}) = \frac{K}{d^2}p_s(G)$.

In the generalized protocol, parties start with the resource state $|\Psi_{\mathrm{in}}\rangle_{AB} = \otimes_{i=1}^N |\Psi^-\rangle_{A_iB_i}$, and perform the following steps: 1. Alice applies $\Pi_g \otimes \mathbb{1}_B(\phi_{A_0} \otimes (\Psi_{\mathrm{in}})_{AB}) = \theta_{A_0AB}$, where $\Pi_g = |\eta_g\rangle\langle\eta_g|$, $g \in G$. 2. Alice communicates the

identity of the element g to Bob. 3. Bob applies $U_g^\dagger$ to his subsystems.

The following Lemma presents the sufficient condition which Alice's operations must satisfy in order to induce the reliable teleportation scheme:

Lemma 1: Define $\eta_{\text{avg}} = \frac{1}{K}\sum_{g\in G}\eta_g$. For all G, the protocol $\mathcal{P}^G$ reaches terminal state Ω_B such that $\|\Omega_B - \sigma_B \otimes \phi_{B_0}\|_1 \leq \epsilon$ with $\epsilon \to 0$ in the limit $N \to \infty$ if

$$\text{Tr}[\eta_{\text{avg}}]^2 \leq \frac{1}{(1-\epsilon)d^{N+1}}, \tag{2}$$

where d denotes the dimension of each of the subsystem.

The proof of Lemma 1 is located in Section 1 of the Supplemental Material [14].

A particular example of the unitaries, which possess the property required by Lemma 1 is any 2 design [15] $\{U_g \otimes U_g\}_{g\in G}$ based on some group G. Another example of the set $\{U_g\}_{g\in G}$ that induces $\{\eta_g\}_{g\in G}$ is the set of random unitaries introduced in [16]. Also, an example of the set $\{U_g\}_{g\in G}$ that induces $\{\eta_g\}_{g\in G}$ is the set of random unitaries introduced in Ref. [16], and it is easy to construct plenty of others.

Recycling of the resource state.—We now introduce two schemes that recycle entanglement in the resource state. Our first protocol consists of sequentially teleporting a sequence of qubits using a preshared resource state, which is made of N singlets. One can view it as the multiple application of the port-based teleportation protocol introduced in Ref. [2], where instead of getting rid of the resource state in the end of the protocol, the parties keep it. For the programmable processor, this corresponds to executing instructions using a simple queue. To ensure that the protocol is indeed capable of teleporting multiple states while recycling the original resource state, it suffices to show that the latter does not degrade much. We do so by finding that the upper bound on the amount of distortion the resource state incurs after the next teleportation round is small, or, equivalently, we find that the fidelity of the resource state with the maximally entangled state does not change much with recycling. More formally, consider Alice and Bob who start with the initial state $|\rho_{\text{port}}\rangle = \otimes_{i=1}^N |\Psi^-\rangle_{A_iB_i}$. We will henceforth refer to each A_iB_i as a *port*, with the subsystems A_i, B_i being held by Alice and Bob, respectively. In addition, they hold a state $\rho_{A_0R_0} = |\Psi^-_{A_0R_0}\rangle\langle\Psi^-_{A_0R_0}|$, and Alice wants to teleport the state of subsystem A_0 to Bob with R_0 serving as a reference system which neither party has access to. The total state (resource state together with the state to be teleported) they share at the beginning of the protocol is $|\Psi_{\text{in}}\rangle = |\Psi^-_{A_0R_0}\rangle \otimes |\rho_{\text{port}}\rangle$.

We define the recycling protocol $\mathcal{P}_{\text{rec}}$ to be the following sequence of actions: 1. Alice performs a measurement Π_i with $\sum_{i=1}^N \Pi_i = \mathbb{1}_{A_0\ldots A_N}$, getting an outcome $z = 1\ldots N$. Port z now contains the teleported state. 2. Alice communicates z to Bob. 3. Bob applies a SWAP operator to ports z and 1. 4. Alice and Bob mark port 1 and do not use it in the next rounds of teleportation. 5. Alice and Bob repeat steps 1–4 using unmarked ports.

As in the original deterministic teleportation protocol from Ref. [2], in step 1 Alice performs a measurement (POVM) on $A_0\ldots A_N$ with elements $\Pi_i = \rho^{-(1/2)}\sigma^{(i)}\rho^{-(1/2)}$, where $\rho = \sum_{i=1}^N \sigma^{(i)}$, and $\sigma^{(i)} = \frac{1}{2^{N-1}} P^-_{A_0A_i} \otimes \mathbb{1}_{\overline{A_0A_i}}$; $P^-_{A_0A_i}$ is the projector onto $\Psi^-_{A_0A_i}$. We will further adopt the notation $\overline{A_i} = A_1\ldots A_N \backslash A_i$. To determine the success of the subsequent rounds of teleportation we compare the state of all of the ports $|\Psi^i_{\text{out}}\rangle$ after Alice measures Π_i with the special reference state $|\Psi^i_{id}\rangle = |\Psi^-_{A_0A_i}\rangle|\Psi^-_{R_0B_i}\rangle \otimes_{j=1,j\neq i}^N |\Psi^-_{A_jB_j}\rangle$, which corresponds to the idealized situation when the successful teleportation is carried out without any disturbance to the remaining ports.

To show that after the first three steps of $\mathcal{P}_{\text{rec}}$ the state of the remaining ports is sufficiently good to be recycled in further teleportation rounds, it is enough to demonstrate that the output state $\rho^i_{\text{out}} = |\Psi^i_{\text{out}}\rangle\langle\Psi^i_{\text{out}}|$ has high average fidelity with $\Psi^i_{id} = |\Psi^i_{id}\rangle\langle\Psi^i_{id}|$:

$$F(\mathcal{P}_{\text{rec}}) = F(\rho_{\text{out}}, \Psi^i_{id}) = \sum_{i=1}^N p_i F(\rho^i_{\text{out}}, \Psi^i_{id}), \tag{3}$$

where the superscripts in ρ^i_{out}, Ψ^i_{id} denote the corresponding states after the teleported state goes to port i, and the last term denotes the probability that the teleportation fails.

Our first result is that the protocol $\mathcal{P}_{\text{rec}}$ does not degrade the total resource state by much.

Theorem 1: After the steps 1–4 of $\mathcal{P}_{\text{rec}}$:

$$F(\mathcal{P}_{\text{rec}}) \geq 1 - \frac{11}{4N} + O\left(\frac{1}{N^2}\right). \tag{4}$$

The proof of the Theorem is located in Section 2 of the Supplemental Material [14]. We will further omit the quadratic terms in the bounds.

Once we have established that it is possible to recycle the resource state, it is important to understand how the error accumulates after each round of teleportation. When the number of ports N and rounds k is relevant we denote it together with the protocol as $\mathcal{P}_{\text{rec}}(N, k)$. It turns out that Alice and Bob can guarantee that the error is at most additive in the number of rounds:

Lemma 2: After teleporting k qubits the resulting fidelity is lower bounded as

$$F(\mathcal{P}_{\text{rec}}(N, k)) \geq 1 - \frac{11k}{2N}. \tag{5}$$

The proof of Lemma 2 is located in Section 2 of the Supplemental Material [14].

Simultaneous teleportation.—We now present the second protocol, which recycles the entanglement in the resource state much differently to that of the first one. Consider Alice, wishing to teleport k qubits simultaneously to Bob. Parties share the resource state $|\rho_{\text{port}}\rangle = \otimes_{i=1}^N |\Psi^-\rangle_{A_iB_i}$, and Alice

wants to teleport the systems $A_0 \dots A_k$. The protocol for simultaneous teleportation is similar to steps 1–3 of $\mathcal{P}_{\text{rec}}$, with the following changes. Instead of N POVM elements, there are $N!/(N-k)!$ of them, each corresponding to the possible ports that the teleported states could appear in. After the measurement, instead of a single port number Alice reveals the identity of k ports where the k states went to. We denote the protocol that uses N ports and teleports k qubits simultaneously as $\mathcal{P}_{\text{sim}}(N, k)$.

Theorem 2 shows that this protocol can indeed teleport $k > 1$ states at once efficiently. From the Theorem it follows that the resource state degrades proportionally to the number of qubits teleported.

Theorem 2: The fidelity of simultaneous teleportation of k qubits using steps 1–5 of the port-based teleportation protocol above is

$$F(\mathcal{P}_{\text{sim}}(N, k)) \geq 1 - \frac{4k}{N}. \tag{6}$$

The proof of the Theorem is located in the Section 3 of the Supplemental Material [14].

One can see that in the limit $N \rightarrow \infty$ the teleportation scheme works with perfect fidelity when the number of systems that Alice can teleport is sublinear in N.

Parallel repetition of the port-based protocol.—In addition to the two protocols above, we introduce the protocol, which makes it possible for concurrent teleportation of the states from Alice to Bob which does not require recycling of the original state. It does so by means of partitioning the resource state into smaller parts and running the original port-based teleportation [2] on each of the parts independently. More precisely, the protocol, denoted as $\mathcal{P}^{\circ k}_{\text{par}}(N)$, consists of teleporting k qubits by running port-based teleportation protocol k times in parallel each utilizing $\frac{N}{k}$ ports each time to teleport a single qubit. We will see that this protocol is substantially worse than the previous two.

Performance of the port-based protocols.—Let us now bring together $\mathcal{P}_{\text{rec}}(N, k)$, $\mathcal{P}_{\text{sim}}(N, k)$ and $\mathcal{P}^{\circ k}_{\text{par}}(N)$, in order to compare their performance in the task of teleporting k states when the resource state consists of N ports. To show how they stack up against each other we introduce a common measure of the performance of the protocols in the following definitions:

Definition.—The port-based teleportation protocol $\mathcal{P}(N, q)$ is said to be *reliable* if it requires N ports (singlets) to teleport a sequence $q \equiv q(N)$ of qubits with fidelity of teleportation satisfying

$$\lim_{N\rightarrow\infty} F(\mathcal{P}(N, q)) = 1. \tag{7}$$

Definition.—We say that the reliable protocol $\mathcal{P}(N, q)$ is *efficient* if it can teleport $Q_{\mathcal{P}}(N) = \text{argmax}_q \mathcal{P}(N, q)$.

One can establish a partial order on the set of efficient protocols: the protocol $\mathcal{A} = \mathcal{P}(N, q_1)$ is more efficient than $\mathcal{B} = \mathcal{P}(N, q_2)$ (denoted as $\mathcal{A}(N, q_1) \geq \mathcal{B}(N, q_2)$) if there exist sequences $Q_{\mathcal{A}}(N)$, $Q_{\mathcal{B}}(N)$ such that $\exists\ N_0 \forall\ N \geq N_0 : Q_{\mathcal{A}}(N) \geq Q_{\mathcal{B}}(N)$.

The Lower bounds.—The achievable fidelity of the total teleportation of $\mathcal{P}^{\circ k}_{\text{par}}(N)$ is

$$F(\mathcal{P}^{\circ k}_{\text{par}}(N)) = \left(1 - \frac{3k}{4N}\right)^k \geq 1 - \frac{3k^2}{4N}. \tag{8}$$

Therefore, the lower bound for the performance of the protocol is

$$Q_{\mathcal{P}^{\circ k}_{\text{par}}}(N) \geq o(\sqrt{N}). \tag{9}$$

From Lemma 2 it follows that by using $\mathcal{P}_{\text{rec}}$ we can teleport at least a sublinear number of qubits in the number of ports reliably; thus,

$$Q_{\mathcal{P}_{\text{rec}}}(N) \geq g(N), \tag{10}$$

where $g(N) \in o(N)$. Lastly, for $\mathcal{P}_{\text{sim}}(N, k)$ using the result of Theorem 2 we get

$$Q_{\mathcal{P}_{\text{sim}}}(N) \geq g(N), \tag{11}$$

where $g(N) \in o(N)$. Even though $\mathcal{P}_{\text{rec}}(N, k)$ and $\mathcal{P}_{\text{sim}}(N, k)$ are the protocols with completely dissimilar modes of operation, and being, strictly speaking, incomparable, they achieve the same asymptotic figure of merit—teleporting a sublinear number of systems. While both protocols achieve perfect fidelity of teleportation in the limit, one cannot be reduced to another, as they use the resource state for teleportation in an entirely different way. In the former protocol Alice applies a POVM that induces a permutation, which assigns the teleported state to one of the ports and communicates its identity to Bob via the classical channel. In the latter one, she applies a single ''large'' permutation that assigns each of the k teleported qubits to some unique port, followed by a single round of classical communication. The action of the permutation in $\mathcal{P}_{\text{sim}}(N, k)$ cannot always be simulated by the repeated application of the permutation and classical communication from $\mathcal{P}_{\text{rec}}(N, k)$, because permutations do not commute in general.

Upper bound.—The way we approached the calculation of the fidelity of teleportation in all of the protocols enabled us to find lower bounds for each of the protocols, but it gave no insight as to whether they are optimal. In what follows, we present a simple protocol-independent upper bound based on no-signaling principle.

Observation 3: For any port-based teleportation protocol $\mathcal{P}(N, k)$ we have

$$Q_{\mathcal{P}}(N) \leq \frac{N}{2}. \tag{12}$$

To justify this bound, consider a generalized port-based teleportation protocol where at the beginning Alice randomly picks one of two states to teleport: $|\Psi_0\rangle = |0\rangle^{\otimes k}$ or $|\Psi_1\rangle = |1\rangle^{\otimes k}$. She performs a measurement prescribed

by the protocol and is yet to communicate its outcome to Bob. If the protocol succeeds in transmitting $k > \frac{N}{2}$ states reliably, then there is no need to send any classical communication to Bob because he could measure each of the ports getting outcomes 0 and 1, and taking the majority vote to determine the teleported message with certainty. However, this is impossible, as it violates the no-signaling principle, which prohibits superluminal communication between Alice and Bob. Therefore, the maximum number of qubits that Alice can reliably communicate to Bob using the port-based protocol is

$$k \leq \frac{N}{2}. \tag{13}$$

It is an intriguing open question—which structures satisfy the sufficient condition of the Lemma 1, and, more importantly, what novel forms of computation might lead from here. In other words, what sets of unitaries $\{U_g\}_{g\in G}$ lead to interesting computation schemes. An important open question is whether one can find a set of such unitaries which allow for new teleportation based computation schemes beyond those considered in Ref. [3].

Finally, having established the possibility of recycling and simultaneous teleportation in the port-based protocols, makes the implementation of the programmable processors more feasible, as one can now carry out the operations using less entanglement. The true potential of these protocols is yet to be fully explored.

We thank Fernando Brandão for suggesting the protocol of simultaneous teleportation $\mathcal{P}_{\text{sim}}$. Along with Matthias Christandl, he independently performed a similar calculation for its lower bound. S. S. thanks Trinity College, Cambridge, for its support throughout his Ph.D. studies. M. H. is supported by EU Grant QESSENCE, NCBiR-CHIST-ERA Project QUASAR, and Polish Ministry of Science and Higher Education Grant No. IdP2011 000361. J. O. acknowledges the support of the Royal Society.

*ss870@cam.ac.uk

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] S. Ishizaka and T. Hiroshima, Phys. Rev. Lett. **101**, 240501 (2008).
[3] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[4] Č. Brukner, J.-W. Pan, C. Simon, G. Weihs, and A. Zeilinger, Phys. Rev. A **67**, 034304 (2003).
[5] S. Ishizaka and T. Hiroshima, Phys. Rev. A **79**, 042306 (2009).
[6] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[7] S. Beigi and R. König, New J. Phys. **13**, 093036 (2011).
[8] G. Brassard, Nature (London) **479**, 307 (2011).
[9] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, in *Advances in Cryptology—CRYPTO 2011*, Lecture Notes in Computer Science Vol. 6841, edited by P. Rogaway (Springer, Berlin Heidelberg, 2011), p. 429.
[10] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, arXiv:1109.2563.
[11] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).
[12] R. F. Werner, J. Phys. A **34**, 7081 (2001).
[13] C. Bennett, P. Hayden, D. Leung, P. Shor, and A. Winter, IEEE Trans. Inf. Theory **51**, 56 (2005).
[14] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.110.010505 for detailed treatment and proofs.
[15] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).
[16] Patrick Hayden, Debbie Leung, Peter W. Shor, and Andreas Winter, Commun. Math. Phys. **250**, 371 (2004).