Exponential Communication Complexity Advantage from Quantum Superposition of the Direction of Communication

Philippe Allard Guérin,* Adrien Feix, Mateus Araújo, and Časlav Brukner
Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria
and Institute for Quantum Optics and Quantum Information (IQOQI),
Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria
(Received 24 May 2016; published 1 September 2016)

In communication complexity, a number of distant parties have the task of calculating a distributed function of their inputs, while minimizing the amount of communication between them. It is known that with quantum resources, such as entanglement and quantum channels, one can obtain significant reductions in the communication complexity of some tasks. In this work, we study the role of the quantum superposition of the direction of communication as a resource for communication complexity. We present a tripartite communication task for which such a superposition allows for an exponential saving in communication, compared to one-way quantum (or classical) communication; the advantage also holds when we allow for protocols with bounded error probability.

DOI: 10.1103/PhysRevLett.117.100502

Quantum resources make it possible to solve certain communication and computation problems more efficiently than what is classically possible. In communication complexity problems, a number of parties have to calculate a distributed function of their inputs while reducing the amount of communication between them [1,2]. The minimal amount of communication is called the *complexity of the problem*. For some communication complexity tasks, the use of shared entanglement and quantum communication significantly reduces the complexity as compared to protocols exploiting shared classical randomness and classical communication [3,4]. Important early examples for which quantum communication yields an exponential reduction in communication complexity over classical communication are the distributed Deutsch-Jozsa problem [5] and Raz's problem [6].

Quantum computation and communication are typically assumed to happen on a definite causal structure, where the order of the operations carried on a quantum system is fixed in advance. However, the interplay between general relativity and quantum mechanics might force us to consider more general situations in which the metric, and hence the causal structure, is indefinite. Recently, a quantum framework has been developed with no assumption of a global causal order [7–9]. This framework can also be used to study quantum computation beyond the circuit model, for instance using the "quantum switch" as a resource—a qubit coherently controlling the order of the gates in a quantum circuit [10]. It has recently been realized experimentally [11].

It was shown that this new resource provides a reduction in complexity to n black-box queries in a problem for which the optimal quantum algorithm with fixed order between the gates requires a number of queries that scales as n^2 [12]. The quantum switch is also useful in communication complexity; a task has been found for which the quantum switch yields an increase in the success probability, yet no advantage in the asymptotic scaling of the communication complexity was found [13]. Most generally, no information processing task is known for which the quantum switch (or any other causally indefinite resource) would provide an exponential advantage over causal quantum (or classical) algorithms.

Here we find a tripartite communication complexity task for which there is an exponential separation in communication complexity between the protocol using the quantum switch and any causally ordered quantum communication scheme. The task requires no promise on inputs and is inspired by the problem of deciding whether a pair of unitary gates commute or anticommute, which can be solved by the quantum switch with only one query of each unitary [14]. If the parties are causally ordered, the number of qubits that needs to be communicated to accomplish the task scales linearly with the number of input bits, whereas the protocol based on the quantum switch only requires logarithmically many communicated qubits. This shows that causally indefinite quantum resources can provide an exponential advantage over causally ordered quantum resources (i.e., entanglement and one-way quantum channels).

The tripartite causally ordered communication scenario we consider in this Letter is illustrated in Fig. 1. Alice and Bob are respectively given inputs $x \in X$ and $y \in Y$, taken from finite sets X, Y. There is a third party, Charlie, whose goal is to calculate a binary function $f(x, y)$ of Alice's and Bob's inputs, while minimizing the amount of communication between all three parties. We shall first assume that communication is one-way only: from Alice to Bob and

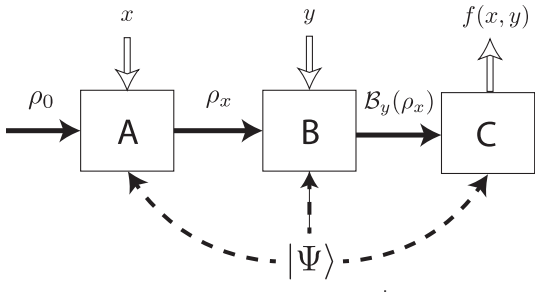

FIG. 1. Causally ordered quantum communication complexity scenario. Conditionally on their inputs x and y, Alice sends a state ρ_x to Bob, who then applies a CP map $\mathcal{B}_y$ and sends the system to Charlie. The unlimited entanglement shared between the parties is represented by $|\Psi\rangle$. The optimal causally ordered protocol is the one that minimizes the number of qubits in ρ_x (which is a lower bound for the communication complexity of the task).

from Bob to Charlie. Furthermore, we grant the parties access to unrestricted local computational power and unrestricted shared entanglement. We will also consider bounded error communication, in which the protocol must succeed on all inputs with an error probability smaller than ϵ.

In quantum communication, the parties communicate with each other by sending quantum systems. Conditionally on their inputs, the parties may apply general quantum operations to the received system, and then send this system out. We require that the parties' local laboratories receive a system *only once* from the outside environment. We impose this requirement to exclude sequential communication, in which the parties communicate back and forth by sending quantum systems to each other at different time steps. Alice's laboratory has an input and output quantum state, consisting of N_{A_I} and N_{A_O} qubits, respectively; similar notation is used for Bob's and Charlie's systems. We seek to succeed at the communication task on all inputs with error probability lower than ϵ, while minimizing the number of communicated qubits $N := N_{A_O} + N_{B_O}$. The optimal causally ordered strategy is for Bob to calculate $f(x, y)$ and then communicate the result to Charlie using one bit of communication; in this case N_{A_O} is a good lower bound for N.

The communication complexity of any causally ordered tripartite communication complexity task can be bounded by considering the bipartite task obtained by identifying Bob and Charlie as a single party. Bearing this in mind, we prove a tight lower bound on the quantum communication complexity of an important family of one-way bipartite deterministic (error probability $\epsilon = 0$) communication tasks, which in turn implies a lower bound on the communication complexity of causally ordered tripartite tasks. This result appears in Theorem 5 of Ref. [15], but we present a different proof here.

Lemma 1: For deterministic one-way evaluation of any binary distributed function $f: X \times Y \to \{0, 1\}$ such that $\forall x_1, x_2 \in X$, with $x_1 \neq x_2$, $\exists y \in Y$ for which $f(x_1, y) \neq f(x_2, y)$, the minimum Hilbert space dimension of the system sent between two parties sharing an arbitrary amount of entanglement is $d = \lceil \sqrt{|X|} \rceil$. Equivalently, the minimum number of communicated qubits is $\lceil \log_2 d \rceil$.

Proof: We recall a well-known result of quantum information [16], establishing that if Alice and Bob share unlimited entanglement, the largest number of orthogonal (perfectly distinguishable) states that Alice can transmit to Bob by sending a d-dimensional system is d^2. Therefore, they can deterministically compute f if Alice sends a system of Hilbert space dimension $\lceil \sqrt{|X|} \rceil$.

Suppose by way of contradiction that the Hilbert space dimension of the communicated system is only $(\lceil \sqrt{|X|} \rceil - 1)$. The maximal number of orthogonal states that can be transmitted by Alice to Bob is $(\lceil \sqrt{|X|} \rceil - 1)^2 < |X|$. Therefore, there exist inputs $x_1, x_2 \in X$ such that the corresponding states ρ_1, ρ_2 transmitted to Bob are not orthogonal, and thus not perfectly distinguishable [17]. By our assumption about the function f, there exists an input $y \in Y$ such that $f(x_1, y) \neq f(x_2, y)$. Therefore, if Bob receives the input y, he will need to distinguish between ρ_1 and ρ_2 in order to output the function correctly, but this cannot be done with zero error probability. ∎

The previous lemma establishes that for a very large class of deterministic communication complexity tasks, it is necessary for Alice to communicate all of her input to Bob. In these cases, the only advantage achieved by causal one-way quantum communication is a reduction by a constant factor of 2 due to dense coding [18]. An important example of this form is the inner product game [19,20]. Note that Lemma 1 does not apply to relational tasks such as the hidden matching problem [21], for which there is an exponential separation between quantum and classical communication complexity.

We now seek to establish a communication complexity task for which indefinite causal order can be used as a resource. In the following we assume that the parties have local laboratories, and that they receive a quantum system from the environment only once. They then perform a general quantum operation on their system, and send it out. An example of a noncausally ordered process is the quantum switch [10], whose use in the context of communication complexity is shown in Fig. 2. Charlie is in the causal future of both Alice and Bob, and an ancilla qubit coherently controls the causal ordering of Alice and Bob; both the target state and the control qubit are prepared externally. Assume that Alice and Bob apply unitary gates U_A and U_B to their respective input systems of N qubits. The global unitary describing the evolution of the system from Charlie's point of view is

$$V(U_A, U_B) = |0\rangle\langle 0|_c \otimes (U_B U_A)_t + |1\rangle\langle 1|_c \otimes (U_A U_B)_t, \quad (1)$$

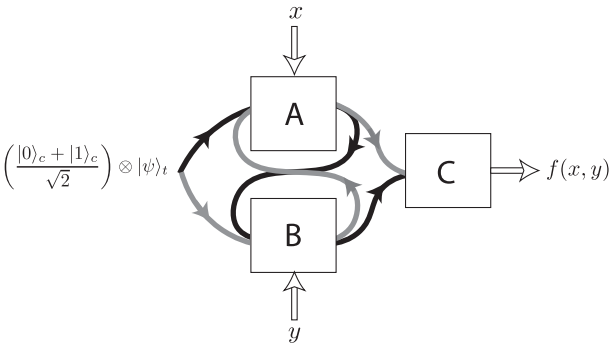

FIG. 2. Communication complexity setup using the quantum switch. A qubit in the state $1/\sqrt{2}(|0\rangle_c + |1\rangle_c)$ coherently controls the path taken by a system of N qubits in initial state $|\psi\rangle_t$. One path goes first through Alice's lab and then Bob's, while the other path goes first through Bob's lab and then Alice's. Alice and Bob are given classical inputs $x \in X$, $y \in Y$, and Charlie (using the control qubit) computes a binary function of their inputs $f(x, y)$.

where the index c denotes the control qubit, and the unitaries U_A and U_B act on the target Hilbert space of N qubits.

Using the quantum switch, one can determine whether two unitaries U_A, U_B commute or anticommute with a single query of each unitary, while at least one unitary must be queried twice in the causally ordered case [14]. Explicitly, consider the quantum switch with the control qubit initially in state $|+\rangle_c = 1/\sqrt{2}(|0\rangle_c + |1\rangle_c)$ and with initial target state $|\psi\rangle_t$. If A and B apply local unitaries U_A and U_B, the resulting state after applying $V(U_A, U_B)$ is

$$\frac{1}{\sqrt{2}}(|0\rangle_c \otimes U_B U_A|\psi\rangle_t + |1\rangle_c \otimes U_A U_B|\psi\rangle_t). \quad (2)$$

If Charlie subsequently applies a Hadamard gate to the control qubit, the resulting state is

$$\frac{1}{2}(|0\rangle_c \otimes \{U_A, U_B\}|\psi\rangle_t - |1\rangle_c \otimes [U_A, U_B]|\psi\rangle_t). \quad (3)$$

Suppose that Alice and Bob randomly choose unitaries from a set $\mathcal{U}$ and that there exists a state $|\psi\rangle_t$ such that $\forall U$, $V \in \mathcal{U}$, either $[U, V]|\psi\rangle_t = 0$ or $\{U, V\}|\psi\rangle_t = 0$. Then Eq. (3) shows that the quantum switch with initial target state $|\psi\rangle_t$ and control qubit $|+\rangle_c$ as inputs allows Charlie to discriminate between these two possibilities with certainty by measuring the control qubit in the computational basis.

We now define a communication complexity task, the exchange evaluation game EE_n, for any integer n. In this game, Alice and Bob are respectively given inputs $(\mathbf{x}, f), (\mathbf{y}, g) \in \mathbb{Z}_2^n \times F_n$, where F_n is the set of functions over $\mathbb{Z}_2^n$ that evaluate to zero on the zero vector

$$F_n = \{f : \mathbb{Z}_2^n \to \mathbb{Z}_2 | f(\mathbf{0}) = 0\}. \quad (4)$$

Charlie must output

$$\mathrm{EE}_n(\mathbf{x}, f, \mathbf{y}, g) = f(\mathbf{y}) \oplus g(\mathbf{x}), \quad (5)$$

where the symbol $\oplus$ denotes addition modulo 2. This game can be interpreted as the sum modulo 2 of two parallel random access codes [22,23].

We first construct an encoding of the inputs $(\mathbf{x}, f), (\mathbf{y}, g)$ in terms of local n-qubit unitaries that all commute or anticommute; we then use the previous observation to conclude that the switch succeeds deterministically at this task with n qubits of communication. We start with some definitions. The group of Pauli X operators on n qubits is defined as

$$X(\mathbf{x}) = X_1^{x_1} \otimes X_2^{x_2} \otimes \cdots \otimes X_n^{x_n}, \quad (6)$$

where x_i is the ith component of the binary vector $\mathbf{x} \in \mathbb{Z}_2^n$. Here, X_i is the single qubit Pauli X operator acting on the ith qubit, and $X_i^0 = \mathbb{I}_i$ is the single qubit identity matrix.

We associate to every $f \in F_n$ a diagonal matrix

$$D(f) = \sum_{\mathbf{z} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{z})} |\mathbf{z}\rangle\langle\mathbf{z}|, \quad (7)$$

where $|\mathbf{z}\rangle$ is the state such that $Z_i|\mathbf{z}\rangle = (-1)^{z_i}|\mathbf{z}\rangle$, with Z_i the single qubit Pauli Z operator acting on qubit i. The set $\{D(f)\}_{f \in F_n}$ consists of all diagonal matrices with entries ± 1 in the computational basis, such that the first entry is $+1$.

We define the set of unitaries

$$\mathcal{U}_n = \{X(\mathbf{x})D(f) | (\mathbf{x}, f) \in \mathbb{Z}_2^n \times F_n\}, \quad (8)$$

which has dimension

$$|\mathcal{U}_n| = 2^{2^n+n-1}. \quad (9)$$

This superexponential scaling of $|\mathcal{U}_n|$ is essential to establish a communication advantage with the quantum switch. Also note that

$$X(\mathbf{x})D(f)X(\mathbf{y})D(g)|\mathbf{0}\rangle = (-1)^{f(\mathbf{y})}|x \oplus y\rangle. \quad (10)$$

Therefore, when acting on the n-qubit input state $|\mathbf{0}\rangle$, the elements of $\mathcal{U}_n$ all commute or anticommute with each other, and

$$\begin{aligned} &[X(\mathbf{x})D(f), X(\mathbf{y})D(g)]|\mathbf{0}\rangle = 0, \quad \text{if } (-1)^{f(\mathbf{y})} = (-1)^{g(\mathbf{x})} \\ &\{X(\mathbf{x})D(f), X(\mathbf{y})D(g)\}|\mathbf{0}\rangle = 0, \quad \text{if } (-1)^{f(\mathbf{y})} = (-1)^{g(\mathbf{x})+1}. \end{aligned} \quad (11)$$

Therefore, the game is equivalent to determining whether the corresponding unitaries $X(\mathbf{x})D(f)$ and $X(\mathbf{y})D(g)$

commute or anticommute *when applied to the state* $|\mathbf{0}\rangle$. By the discussion following Eq. (3), this problem can be solved deterministically by Charlie using the quantum switch with $O(n)$ qubits of communication from Alice to Bob, with a strategy consisting of applying the unitary corresponding to their input according to Eq. (8).

We now show that the exchange evaluation game satisfies the conditions of Lemma 1; this will allow us to conclude that for deterministic ($\epsilon = 0$) evaluation in the one-way causally ordered case, EE_n requires an amount of communicated qubits that grows exponentially with n.

Proposition 2: For every $(\mathbf{x_1}, f_1)$, $(\mathbf{x_2}, f_2) \in \mathbb{Z}_2^n \times F_n$, such that $(\mathbf{x_1}, f_1) \neq (\mathbf{x_2}, f_2)$, there exists $(\mathbf{y}, g) \in \mathbb{Z}_2^n \times F_n$ such that $\mathrm{EE}_n(\mathbf{x_1}, f_1, \mathbf{y}, g) \neq \mathrm{EE}_n(\mathbf{x_2}, f_2, \mathbf{y}, g)$.

Proof: First note that $\mathrm{EE}_n(\mathbf{x_1}, f_1, \mathbf{y}, g) \neq \mathrm{EE}_n(\mathbf{x_2}, f_2, \mathbf{y}, g)$ if and only if

$$f_1(\mathbf{y}) \oplus f_2(\mathbf{y}) \oplus g(\mathbf{x_1}) \oplus g(\mathbf{x_2}) = 1. \tag{12}$$

Then, since $(\mathbf{x_1}, f_1) \neq (\mathbf{x_2}, f_2)$, either $\mathbf{x_1} \neq \mathbf{x_2}$ or $f_1 \neq f_2$ holds. We check that the conditions of the lemma are satisfied in both cases.

(i) *Case where* $\mathbf{x_1} \neq \mathbf{x_2}$: Suppose without loss of generality that $\mathbf{x_1} \neq \mathbf{0}$ and define g as the function such that $g(\mathbf{x_1}) = 1$ and $g(\mathbf{z}) = 0$, $\forall \mathbf{z} \neq \mathbf{x_1}$. Also, because f_1, $f_2 \in F_n$, $f_1(\mathbf{0}) = f_2(\mathbf{0}) = 0$. Therefore, the function g we just defined and $\mathbf{y} = \mathbf{0}$ satisfy Eq. (11).

(ii) *Case where* $f_1 \neq f_2$: Let $\mathbf{y} \in \mathbb{Z}_2^n$ be a vector for which f_1 and f_2 differ, so that $f_1(\mathbf{y}) + f_2(\mathbf{y}) = 1$. Then this $\mathbf{y}$ and the zero function $g(\mathbf{x}) = 0 \forall \mathbf{x}$ satisfies Eq. (11). ∎

According to Eq. (9), the dimension of the set of inputs to EE_n is $|\mathcal{U}_n| = 2^{2^n+n-1}$. Direct application of Proposition 2 with Lemma 1 establishes that the number of qubits of communication required for deterministic success in the causally ordered case is $\frac{1}{2}\log_2|\mathcal{U}_n| = \frac{1}{2}(2^n + n - 1) = \Omega(2^n)$, using dense coding. In comparison, we have seen that with the quantum switch as a resource, we need only n qubits of communication between Alice and Bob to calculate this function. We thus conclude that for the exchange evaluation game, there is an exponential separation in the deterministic communication complexity of EE_n.

Note that with two-way (classical) communication, it is possible to solve the exchange evaluation game with $2n + 2$ bits of communication, simply by having Alice and Bob send their vectors $\mathbf{x}$, $\mathbf{y}$ to the other party, followed by local evaluation of $f(\mathbf{y})$ and $g(\mathbf{x})$ by the parties and communication of the result to Charlie. We emphasize that once we allow two-way communication, the quantum advantage can also disappear in traditional quantum communication complexity (comparing causally ordered quantum communication with classical communication): this is the case for the distributed Deutsch-Jozsa problem [5], but not for Raz's problem [24].

For causally ordered communication complexity tasks, the exponential quantum-classical separation does not always continue to hold when allowing for protocols to have a small but nonzero error probability $\epsilon > 0$. Indeed, looking at early examples of tasks, the advantage disappears for the distributed Deutsch-Jozsa problem [5], while it remains for Raz's problem [6]. The Supplemental Material [25] presents a proof, based on VCdimension [26], that the one-way quantum communication complexity with bounded error for EE_n scales as $\Omega(2^n)$, and thus that the exponential separation in communication complexity due to superposition of causal ordering persists when allowing for a nonzero error probability.

To show that it is possible to operationally distinguish quantum control of causal order from two-way communication one could introduce counters at the output ports of Alice's and Bob's laboratories, whose role is to count the number of uses of the channels. Such an argument has already been made in Ref. [12] to justify a computational advantage. We can model a counter as a qutrit initially in the state $|0\rangle$, whose evolution when a system exits the laboratory is $|i\rangle \to |i + 1 \bmod 3\rangle$, where $i \in \{0, 1, 2\}$. Then, for both one-way communication and the quantum switch, the counters of Alice and Bob will be in the state $|1\rangle$ at the end of the protocol; for genuine two-way communication, at least one of these counters will be in the final state $|2\rangle$. Therefore, the expectation value of the observables $N = \sum_{i=0}^{2} |i\rangle\langle i|$ for the counters allows us to distinguish realizations of the quantum switch, such as [11], from two-way quantum communication.

In conclusion, we have found a communication complexity task, the exchange evaluation game, for which a quantum superposition of the direction of communication—the quantum switch—results in an exponential saving in communication when compared to causally ordered quantum communication. An interesting feature of this game is that it is not a promise game, as are most known tasks for which quantum resources have an exponential advantage [4].

In future work, it would be interesting to explore other information processing tasks for which the quantum switch—or other causally indefinite processes—may yield interesting advantages. For example, one could look at the uses of the quantum switch for secure distributed computation [27–30]. Indeed, imagine that Alice and Bob both want to learn about the value of EE_n, in such a way that the other party does not learn about their inputs. They could achieve this goal by enlisting a third party and using the quantum switch with the EE_n protocol.

We thank Ashley Montanaro for pointing out Ref. [15] to us, used to establish the bounded-error advantage. We acknowledge support from the European Commission project RAQUEL (No. 323970); the Austrian Science Fund (FWF) through the Special Research Programme FoQuS, the Doctoral Programme CoQuS and Individual Project (No. 2462), and the John Templeton Foundation. P. A. G. is also supported by FQRNT (Quebec).

*Corresponding author.
philippe.guerin@univie.ac.at

[1] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1979), pp. 209–213.
[2] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, 1997).
[3] A. C.-C. Yao, in *Proceedings of the 34th Annual Symposium on the Foundations of Computer Science* (IEEE, New York, 1993), pp. 352–361.
[4] H. Buhrman, R. Cleve, S. Massar, and R. De Wolf, Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010).
[5] H. R. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1999), pp. 63–68.
[6] R. Raz, in *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, STOC '99 (ACM, New York, 1999), pp. 358–367.
[7] O. Oreshkov, F. Costa, and Č. Brukner, Quantum correlations with no causal order, Nat. Commun. **3**, 1092 (2012).
[8] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, and Č. Brukner, Witnessing causal nonseparability, New J. Phys. **17**, 102001 (2015).
[9] O. Oreshkov and C. Giarmatzi, Causal and causally separable processes, arXiv:1506.05449.
[10] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Quantum computations without definite causal structure, Phys. Rev. A **88**, 022318 (2013).
[11] L. M. Procopio, A. Moqanaki, M. Araújo, F. Costa, I. Alonso Calafell, E. G. Dowd, D. R. Hamel, L. A. Rozema, Č. Brukner, and P. Walther, Experimental superposition of orders of quantum gates, Nat. Commun. **6**, 7913 (2015).
[12] M. Araújo, F. Costa, and Č. Brukner, Computational Advantage from Quantum-Controlled Ordering of Gates, Phys. Rev. Lett. **113**, 250402 (2014).
[13] A. Feix, M. Araújo, and Č. Brukner, Quantum superposition of the order of parties as a communication resource, Phys. Rev. A **92**, 052326 (2015).
[14] G. Chiribella, Perfect discrimination of no-signalling channels via quantum superposition of causal structures, Phys. Rev. A **86**, 040301 (2012).
[15] H. Klauck, in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (ACM, New York, 2000), pp. 644–651.
[16] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Classical information capacity of a quantum channel, Phys. Rev. A **54**, 1869 (1996).
[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, Cambridge, England, 2011).
[18] C. H. Bennett and S. J. Wiesner, Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States, Phys. Rev. Lett. **69**, 2881 (1992).
[19] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, Quantum entanglement and the communication complexity of the inner product function, Lect. Notes Comput. Sci. **1509**, 61 (1998).
[20] A. Nayak and J. Salzman, in *Proceedings of 34th ACM STOC* (ACM, New York, 2002), pp. 698–704.
[21] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, in *Proceedings of the Thirty-sixth Annual ACM Symposium on Theory of Computing*, STOC '04 (ACM, New York, 2004), pp. 128–137.
[22] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, in *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, STOC '99 (ACM, New York, 1999), pp. 376–383.
[23] A. Nayak, *FOCS '99 Proceedings of the 40th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, 1998), pp. 369–376.
[24] B. Klartag and O. Regev, in *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11 (ACM, New York, 2011), pp. 31–40.
[25] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.100502 for a proof of the exponential communication complexity advantage with bounded error probability.
[26] V. N. Vapnik and A. Y. Chervonenkis, On the uniform convergence of relative frequencies of events to their probabilities, Theory Probab. Appl. **16**, 264 (1971).
[27] A. C. Yao, *FOCS 23rd Annual Symposium on Foundations of Computer Science* (1982), pp 160–164, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4568388.
[28] H.-K. Lo, Insecurity of quantum secure computations, Phys. Rev. A **56**, 1154 (1997).
[29] H. Buhrman, M. Christandl, and C. Schaffner, Complete Insecurity of Quantum Protocols for Classical Two-Party Computation, Phys. Rev. Lett. **109**, 160501 (2012).
[30] W. Liu, C. Liu, H. Wang, and T. Jia, Quantum private comparison: A review, IETE Tech Rev **30**, 439 (2013).