Multipartite Entanglement Verification Resistant against Dishonest Parties

Anna Pappa,[1,2] André Chailloux,[3] Stephanie Wehner,[4] Eleni Diamanti,[1] and Iordanis Kerenidis[2,4]

[1]*LTCI, CNRS—Télécom ParisTech, Paris 75013, France*
[2]*LIAFA, CNRS—Université Paris 7, Paris 75013, France*
[3]*Computer Science Department, University of California, Berkeley, California 94720-1776, USA*
[4]*Center for Quantum Technologies, National University of Singapore, Singapore 117543*

(Received 6 February 2012; published 26 June 2012; corrected 2 July 2012)

Future quantum information networks will consist of quantum and classical agents, who have the ability to communicate in a variety of ways with trusted and untrusted parties and securely delegate computational tasks to untrusted large-scale quantum computing servers. Multipartite quantum entanglement is a fundamental resource for such a network and, hence, it is imperative to study the possibility of verifying a multipartite entanglement source in a way that is efficient and provides strong guarantees even in the presence of multiple dishonest parties. In this Letter, we show how an agent of a quantum network can perform a distributed verification of a source creating multipartite Greenberger-Horne-Zeilinger (GHZ) states with minimal resources, which is, nevertheless, resistant against any number of dishonest parties. Moreover, we provide a tight tradeoff between the level of security and the distance between the state produced by the source and the ideal GHZ state. Last, by adding the resource of a trusted common random source, we can further provide security guarantees for all honest parties in the quantum network simultaneously.

DOI: 10.1103/PhysRevLett.108.260502 PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Bg, 03.67.Hk

Entanglement plays a key role in the study and development of quantum information theory. It has been widely used in all aspects of quantum information and has been essential to show the advantages obtained compared to the classical setting. Initially defined for bipartite states, the notion of entanglement has been generalized to multipartite systems, and despite the complexity this notion acquires in this case, many interesting properties of multipartite entangled states are known. If we consider, for example, the quantum correlations of the Greenberger-Horne-Zeilinger (GHZ) state [1] and its n-party generalization, we can find a nonlocal game that can be won with probability 1 in the quantum setting, while any classical local theory can win the game with probability at most $3/4$ [2].

Multipartite entangled states are a fundamental resource when quantum networks are considered. Indeed, they allow network agents to create strong correlations in order to perform distributed tasks, to delegate computation to untrusted servers [3], or to compute, for example, through the measurement-based quantum computation model [4]. A natural and fundamental question that arises then is whether the network agents should be required to trust the source that provides them with such multipartite entangled states or whether they are able to verify the entanglement.

In this Letter, we show that a quantum agent can verify efficiently, with respect to the necessary resources, that an untrusted source creates entanglement, even in the presence of dishonest parties.

The model.—We start our analysis by first describing in detail our model and its relation to previous work.

Source.—The source is untrusted. It is supposed to create the n-party GHZ state $\frac{1}{\sqrt{2^n}}(|0^n\rangle + |1^n\rangle)$ and distribute it to n parties. By applying a Hadamard and a phase shift ($\sqrt{Z}$) gate to each qubit, the GHZ state can be expressed by the locally equivalent state

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2^{n-1}}}\left[\sum_{\Delta(y)\equiv 04(\mathrm{mod}4)} |y\rangle - \sum_{\Delta(y)\equiv 24(\mathrm{mod}4)} |y\rangle\right],$$

where y is a classical n-bit string $y_1 \ldots y_n$ and $\Delta(y) = \sum_i y_i$ denotes the Hamming weight of y. We will use the latter state for our proofs. Such states have a wide range of applications, for example in nonlocal games, quantum game theory and quantum computation.

Parties.—A party can be honest or dishonest. An honest party does not know which parties are honest and which are dishonest. The dishonest parties can collaborate with each other and control the source. Their goal is to convince the honest parties that the source can create the n-party GHZ state, while in reality this may not be true. They are allowed to create a different state every time or entangle the state with any auxiliary space.

Local resources.—A party has a trusted single-qubit measurement device with two measurement settings and a trusted classical random source.

Network resources.—Every pair of parties shares a private classical channel, in other words, the communication between two honest parties remains secret. This is the standard setup for classical networks with dishonest parties, since in the absence of private channels we cannot guarantee security for more than a single honest party.

Note that we want to use the least possible resources for our protocol. Indeed, we only need each party to be able to produce randomness, to perform single-qubit measurements, and to securely communicate classical information with the other parties. Since our goal is to construct protocols that can be widely available in the near future, it is imperative to minimize the resources available to the agents, especially the quantum resources that are considered more expensive than the classical ones, hence bringing such tasks closer to reality.

Related work.—Most of the work on entanglement verification has considered the case where all parties are honest. For two parties, three models have been studied.

First, the standard model, where both parties trust their devices but they do not trust the source. This model corresponds to the setting of nonseparability tests, where the two parties can perform together quantum tomography on the state distributed by the source and thus verify the existence of entanglement. In a cryptographic language, this corresponds to a setting where all parties are guaranteed to be honest. A related question concerning untrusted sources in quantum key distribution protocols is discussed in [5].

Second, the device-independent model, where the parties trust neither their quantum devices nor the source. This model is related to the well-known setting of the Bell nonlocality tests as well as to self-testing [6].

Third, the one-sided device-independent model [7], where the security is asymmetric: one party trusts his devices but the second party's devices and the source are untrusted. This model corresponds to the setting of generalized quantum steering [8,9], where one party is also given control of the source and tries to convince the other party, who trusts his devices, that she can create entanglement. In a cryptographic language, an honest party tries to verify entanglement in the presence of a dishonest party who controls the source. Recently, there have been experimental demonstrations in this model [10–12].

For the multipartite case, much less is known. In the standard model, pseudotelepathy [13] extends Mermin's game [2] to many parties; a maximally entangled state is used to play the game and wins with probability 1, which is strictly better than in the classical case. In the device independent model, it was shown that honest parties who do not trust their devices can verify genuine multipartite entanglement by using appropriate entanglement witnesses [14]. Finally, in [15] the authors present a unified framework for n-party entanglement verification and provide inequalities with different bounds for the different nonlocality classes that are considered.

Our work.—In our model, there are, in general, k honest parties and n-k dishonest parties who control the source, which is supposed to create an n-party GHZ state. Each honest party does not know which other parties are honest. Our goal is to provide an efficient test for an honest party, such that the test passes only if the state produced by the source creates entanglement between all k honest parties and the n-k dishonest parties.

First, if all players are honest, we prove that any n-party state that is ϵ-away from the n-party GHZ state passes the test with probability at most $1 - \epsilon^2/2$. Second, in the presence of any number of dishonest parties, we prove the same quantitative statement, this time for any n-party state that is ϵ-away from the n-party GHZ state up to a local unitary operation on the space of the dishonest parties.

For the special case of $n = 2$, our model significantly extends the results in the generalized quantum steering setting by providing a tight analysis of the tradeoff between the distance of the shared state to the n-party GHZ and the probability of success of the test. For the case of $n = k$, i.e., the standard model, our results again provide a tight analysis of the tradeoff between the distance and the probability the test passes. For general n parties and k honest ones, this is the first rigorous analysis of an entanglement verification test.

The protocol V.—Consider a source that is supposed to create and distribute the state $|\Phi_0^n\rangle$ to n parties. We present a verification protocol V that one party, called the Verifier, can run with the other $n - 1$ parties, in order to verify that the state $|\Psi\rangle$ created by the source is in fact the correct one. (1) The Verifier selects for each $i \in [n]$ a random input $X_i \in \{0, 1\}$, such that $\sum_{i=1}^n X_i \equiv 0 \pmod 2$ and sends it to the corresponding party via a private classical channel. (2) If $X_i = 0$, party i performs a Z operation. If $X_i = 1$, party i performs a Hadamard operation. (3) Party i measures in the $\{|0\rangle, |1\rangle\}$ basis and sends the corresponding outcome $Y_i \in \{0, 1\}$ to the Verifier via the private channel. (4) The Verifier accepts the result if and only if

$$\sum_{i=1}^n Y_i \equiv \frac{1}{2}\sum_{i=1}^n X_i \qquad (\text{mod}2).$$

The above protocol assumes that a specific party plays the role of the Verifier. We will later address the question of how to pick such a Verifier among all honest parties. Note that this test has been used before [13]; however, our analysis is entirely different. We denote by $T(|\Psi\rangle)$ the event that the Verifier accepts the result of the Test, when the joint state is $|\Psi\rangle$.

Correctness of the protocol.—We want to show that the state $|\Phi_0^n\rangle$ passes the test with probability 1. We need to define the following state:

$$|\Phi_1^n\rangle = \frac{1}{\sqrt{2^{n-1}}}\left[\sum_{\Delta(y)\equiv 1 \pmod 4} |y\rangle - \sum_{\Delta(y)\equiv 3 \pmod 4} |y\rangle\right].$$

It is easily verifiable (from the definition of the states) that for any k and n,

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2}}[|\Phi_0^k\rangle|\Phi_0^{n-k}\rangle - |\Phi_1^k\rangle|\Phi_1^{n-k}\rangle]. \qquad (1)$$

From condition $\sum_{i=1}^n X_i \equiv 0 \pmod 2$ we have two cases: (1) $(\frac{1}{2}\sum_{i=1}^n X_i) \equiv 0 \pmod 2$: This means that the sum of

the inputs is a multiple of 4. Using Eq. (1), it can be proven that the state $|\Phi_0^n\rangle$ goes to $\pm|\Phi_0^n\rangle$ when we apply to it an operator consisting of a 0 (mod 4) number of single-qubit Hadamards and Z gates on the remaining qubits. Hence, we always have $\sum_{i=1}^n Y_i \equiv 0 \pmod 2$.

(2) $(\frac{1}{2}\sum_{i=1}^n X_i) \equiv 1 \pmod 2$: This means that the sum of the inputs is even but not a multiple of 4. Again, it can be proven that the state $|\Phi_0^n\rangle$ goes to $\pm|\Phi_1^n\rangle$ when we apply to it an operator consisting of a 2 (mod 4) number of single-qubit Hadamards and Z gates on the remaining qubits. Hence, we always have $\sum_{i=1}^n Y_i \equiv 1 \pmod 2$.

Security in the honest model.—We now look at the model where all n parties are honest and analyze the probability that our test accepts a state as a function of the distance of this state to $|\Phi_0^n\rangle$. We first analyze the case of a pure state. Denoting by $D(|\psi\rangle, |\phi\rangle)$ the trace distance between two states $|\psi\rangle$ and $|\phi\rangle$, we have

Theorem 1.—If $D(|\Psi\rangle, |\Phi_0^n\rangle) = \epsilon$, $\Pr[T(|\Psi\rangle)] \leq 1 - \frac{\epsilon^2}{2}$.

The main idea of the proof is to show that our test is equivalent to performing a POVM $\{P_n, I - P_n\}$, (where the first outcome corresponds to acceptance) with

$$P_n = |\Phi_0^n\rangle\langle\Phi_0^n| + \tfrac{1}{2}I_{S_n},$$

where S_n denotes the subspace of n-qubit states that are orthogonal to both $|\Phi_0^n\rangle$ and $|\Phi_1^n\rangle$, and I_{S_n} denotes the projection on this subspace. In other words, we show that the state $|\Phi_0^n\rangle$ passes the test with probability 1, the state $|\Phi_1^n\rangle$ passes the test with probability 0, and all other states in the orthogonal subspace pass the test with probability exactly 1/2. The proof of this statement is in fact quite involved and is done by induction on the dimension of the state (see [16] for details). With this characterization for our test, we express any state $|\Psi\rangle$ such that $D(|\Psi\rangle, |\Phi_0^n\rangle) = \epsilon$ as $|\Psi\rangle = \sqrt{1-\epsilon^2}|\Phi_0^n\rangle + \sum_{i=1}^{2^n-1}\epsilon_i|\Phi_i^n\rangle$, where for $i \geq 2$, $|\Phi_i^n\rangle \in S_n$ and $\sum_{i=1}^{2^n-1}\epsilon_i^2 = \epsilon^2$, and hence we have $\Pr[T(|\Psi\rangle)] = \mathrm{tr}(P_n|\Psi\rangle) \leq 1 - \frac{\epsilon^2}{2}$.

Note that for a mixed state $\rho = \{p_i, |\Psi_i\rangle\}$, $\Pr[T(\rho)] = \sum_i p_i \Pr[T(|\Psi_i\rangle)]$. Then, by convexity we have

Corollary 1: If $D(\rho, |\Phi_0^n\rangle) = \epsilon$, $\Pr[T(\rho)] \leq 1 - \frac{\epsilon^2}{2}$.

Security in the dishonest model.—We look now at the model where the honest Verifier runs the test in the presence of dishonest parties. The Verifier is considered to be known to all parties. We prove in this case a theorem similar to the case of all honest parties. It should be clear here that there is no way for the honest parties to determine whether the dishonest parties act as n-k independent parties each holding one qubit or whether they have colluded to one party. For example, the state $|\Phi_0^{k+1}\rangle = \frac{1}{\sqrt{2}}[\Phi_0^k\rangle 0\rangle - \Phi_1^k\rangle 1\rangle]$, where the n-k dishonest parties hold a single qubit, passes the test with probability 1, since the dishonest parties can locally map this state to $|\Phi_0^n\rangle$. Hence, the correct security statement must take into account the fact that the dishonest parties may apply some operator on their space.

Theorem 2. Let $|\Psi\rangle$ be the state of all n parties. If $\min_U D(U|\Psi\rangle, |\Phi_0^n\rangle) = \epsilon$, where U is an operator on the space of the dishonest parties, then $\Pr[T(|\Psi\rangle] \leq 1 - \frac{\epsilon^2}{2}$.

Let us assume, without loss of generality, that the n parties share a state of the form $|\Psi\rangle = |\Phi_0^k\rangle|\Psi_0\rangle + |\Phi_1^k\rangle|\Psi_1\rangle + |\mathcal{X}\rangle$, where in $|\mathcal{X}\rangle$ the component of the honest parties is orthogonal to $|\Phi_0^k\rangle$ and $|\Phi_1^k\rangle$. For the dishonest parties, making the Verifier accept the test is equivalent to guessing the honest output $Y_H := \sum_H Y_i \pmod 2$, where H is the set of the honest parties, before announcing their measurement outcomes. The optimal probability of guessing Y_H given $X_H := \sum_H X_i \pmod 2$ is given by the Helstrom measurement. Let $p = \| |\Psi_0\rangle \|^2$, $1 - p = \| |\Psi_1\rangle \|^2$ and $\langle\Psi_0|\Psi_1\rangle^2 = p(1-p)\cos^2\theta$. Then, we calculate that

$$\Pr[\text{guess}Y_H] \leq 1 - \frac{1}{2}\left(p(1-p)\cos^2\theta + \frac{(2p-1)^2}{4}\right).$$

Note that the probability of guessing Y_H is independent of the state $|\mathcal{X}\rangle$. Now, consider the operation R acting on the space of the dishonest parties:

$$R|\Psi_b\rangle = \| |\Psi_b\rangle \| \left(\cos\left(\frac{\pi}{4} - \frac{\theta}{2}\right)|\Phi_b^{n-k}\rangle + \sin\left(\frac{\pi}{4} - \frac{\theta}{2}\right)|\Phi_{1-b}^{n-k}\rangle\right)$$

for $b \in \{0, 1\}$. For the new shared state $|\Xi\rangle = I_k \otimes R|\Psi\rangle$, we have $\langle\Xi|\Phi_0^n\rangle^2 = \frac{1}{4}(1 + \sin\theta)(1 + 2\sqrt{p(1-p)})$. Since by assumption $\langle\Xi|\Phi_0^n\rangle^2 \leq 1 - \epsilon^2$, this concludes the proof (see [16] for more details).

Security for all honest parties.—We have presented a protocol that a Verifier can use to verify the state of an untrusted source in the presence of dishonest parties with minimal resources. Our protocol can be useful in the scenario where some party wants to perform a complex quantum computation and needs to delegate parts of the computation to other parties, who, of course, would need some source of multipartite entanglement in order to perform the joint computation. Note that the Verifier can repeat the protocol sequentially in order to increase the probability of detecting an erroneous state.

In a more general scenario, however, where parties need to perform securely some distributed multipartite computation using the multipartite entangled state as an initial shared resource, we need to guarantee security for all honest parties at the same time. In other words, we would like a protocol that guarantees to all honest parties that they will only accept to use a state for the computation that comes from a source that produces states that are very close to an n-party GHZ state. *A priori*, such a task is impossible, since any such protocol could be used to produce unbiased strong coins [17] (the parties could just measure the entangled state to produce coins). Hence, we need to provide some additional resource.

Trusted common random source (CRS).—We assume that all parties have access to a trusted classical random source that provides them with the same randomness.

This is, of course, a powerful, but necessary, resource. One way to achieve it would be to assume that at least a third of all parties are honest, since this implies the ability to securely produce random bits only with authenticated classical communication [18]. Note that in order to achieve quantum secure multiparty computation, at least a majority of honest parties is required [19], in which case it is possible to construct a CRS.

We describe how to repeat our verification test in order to guarantee the following: when the parties decide to use the state for computation, then the probability that the state produced by the source is ϵ-away from the n-party GHZ state goes to zero exponentially fast with the number of repetitions. Note that our guarantee is on the state produced by the source. Of course, we cannot prevent the dishonest parties from destroying the entanglement with the honest parties just before using this state for further computation. However, we argue that our test is still useful for secure multiparty computation. First, as we noted before, if the goal of the dishonest parties is to convince the honest parties of the source's ability to create entanglement, destroying the entanglement after the source has produced it does not help them. Second, in general, in secure multiparty computation, one of the main goals is to guarantee that the inputs of the honest parties remain secret for the dishonest parties. Since in our model the parties will only perform local quantum operations (if the parties could send their qubits to other parties, then checking the source would be much easier by having all qubits sent to the Verifier), by destroying the entanglement, the dishonest parties cannot increase their information about the honest parties inputs. Third, we still have a strong guarantee on the honest player states from which they can, for example, extract correlated secret bits.

Let S be a security parameter.

The Symmetric protocol.—(1) The source distributes a state $|\Psi\rangle$ to the n parties (the honest source distributes the state $|\Phi_0^n\rangle$). (2) Parties receive $r \in \{0,1\}^S$ and $i \in [n]$ from CRS. (a) If $r = \mathbf{0}$, the state $|\Psi\rangle$ is used for computation. (b) If $r \neq \mathbf{0}$ Party i runs protocol V with $|\Psi\rangle$. If he rejects, then abort, otherwise go to Step 1.

Note that the source may create a different state at every repetition of the protocol. It is also important that the state is distributed before the parties receive the randomness from the CRS. Let C_ϵ be the event that the symmetric protocol has not aborted and that the state used for the computation, which we denote by $|\Psi\rangle$, is such that $\min_U D(U|\Psi\rangle, |\Phi_0^n\rangle) \geq \epsilon$, where U is an operator on the space of the dishonest parties. We will prove the following:.

Theorem 3.—For all $\epsilon > 0$, $\Pr[C_\epsilon] \leq 2^{-S\frac{2n}{k\epsilon^2}}$.

The proof is given in [16]. When the Verifier is dishonest, we suppose that the state always passes the test. By choosing $S = \log\frac{2n\delta}{\epsilon^2}$ for some constant $\delta > 0$, all honest parties have the guarantee that the probability the state used has distance at least ϵ from the correct one, is at most $1/\delta$. Note that the expected number of repetitions of the protocol is 2^S, which, with our choice of S, is polynomial in n and $1/\epsilon$ [and with probability exponentially close to 1, the number of repetitions is at most $O(2^S)$]. Moreover, this protocol provides guarantees to all honest parties, unlike the case of quantum steering and our multipartite generalization. To this end, it was necessary to make the assumption of a trusted classical random source.

Discussion.—It is important to note that our analysis does not take into account losses and noise that appear in a realistic setting. It will be interesting to study such conditions, as was recently done for bipartite quantum steering [10]. We also note that although our results provide a verification test for the GHZ state, the analysis should, in principle, be applicable to all states for which a Bell-type test is available, such as stabilizer states.

We acknowledge discussions with D. Markham, T. Lawson, and A. Leverrier and financial support from the ANR, Digiteo, the EU, and the Ministry of Education, Singapore.

[1] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), p. 69.
[2] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[3] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526.
[4] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[5] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).
[6] M. McKague, T. H. Yang, and V. Scarani, arXiv:1203.2976.
[7] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).
[8] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[9] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).
[10] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde, arXiv:1111.0739v1.
[11] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, arXiv:1111.0760v1.
[12] D. H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, and S.-W. Nam *et al.*, Nature Commun. **3**, 625 (2012).

[13] G. Brassard, A. Broadbent, and A. Tapp, in *Proceedings of the 8th International Workshop on Algorithms and Data Structures* (2003), vol. 2748, p. 1.

[14] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).

[15] E. G. Cavalcanti, Q. Y. He, M. D. Reid, and H. M. Wiseman, Phys. Rev. A **84**, 032115 (2011).

[16] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.108.260502 for the proofs of Theorems 1, 2, and 3.

[17] H.-K. Lo and H. F. Chau, Physica D (Amsterdam) **120**, 177 (1998).

[18] D. Chaum, C. Crépeau, and I. Damgård, in Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC 1988), New York, pp. 11–19.

[19] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith, in *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS, 2006)*, p. 249.