Multipartite maximally entangled states in symmetric scenarios

Carlos E. González-Guillén
Departamento de Matemáticas, E.T.S.I. Industriales, Universidad Politécnica de Madrid, 28006 Madrid, Spain and IMI, Universidad Complutense de Madrid, 28040 Madrid, Spain
(Received 17 April 2012; published 2 August 2012)

We consider the class of $(N+1)$-partite states suitable for protocols where there is a *powerful* party, the authority, and the other N parties *play the same role*, namely, the state of their system lies in the symmetric Hilbert space. We show that, within this scenario, there is a "maximally entangled state" that can be transform by a local operations and classical communication protocol into any other state. In addition, we show how to use the protocol efficiently, including the construction of the state, and discuss security issues for possible applications to cryptographic protocols. As an immediate consequence we recover a sequential protocol that implements the 1-to-N symmetric cloning.

DOI: 10.1103/PhysRevA.86.022304 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Ac

I. INTRODUCTION

The understanding, classification, quantification, and use of multipartite entanglement has been one of the most challenging issues in the theory of quantum information during the last decade. Even in the tripartite case, strange phenomena start to occur, like the nonequivalence of W and Greenberger-Horne-Zeilinger states [1], the possibility of distributing entanglement with separable states [2], or the existence of unbounded violations for some correlation Bell inequalities [3]. Going into the N-partite situation only increases the number of interesting phenomena: universal states for quantum computation [4], topological entanglement [5], relations with complexity theory [6], and so on.

Associated with the different points of view in the theory of multipartite entanglement, different entanglement measures have been defined, focusing on the different aspects of entanglement: the topological entropy [7] measures the amount of topological entanglement in a state and is hence appropriate in the context of topological quantum computation and error correction; the localizable entanglement [8] measures the amount of bipartite entanglement that can be created between two sites in a collaborative scenario and is hence appropriate in the context of quantum networks and quantum repeaters; there are also measures which intend to be more general, and usually measure the distance (in some sense) to the set of separable states, like the relative entropy of entanglement, the global robustness of entanglement, or the geometric measure of entanglement [9]. As is pointed out repeatedly in the literature [10,11], the variety of multipartite entanglement measures has its roots in the impossibility of defining the concept of "maximally entangled state" in the multipartite setting.

We will show here that if one imposes some symmetry restrictions on the state, motivated by the class of multipartite protocols one wants to implement with it, there is still hope of defining properly the concept of a maximally entangled state. Here we will concentrate on protocols in which there is an authority A and a set of participants $p_1, \ldots, p_N$ which *have to play the same role in the protocol*. This is the desired situation in a wide variety of multipartite protocols, like secret sharing or voting, and leads to the following assumptions.

Assumption 1. We will work with $(N+1)$-partite states which are permutation-symmetric with respect to N of the parties.

Assumption 2. To make things simpler we will assume that the Hilbert space dimension of the participants is 2, while that of the authority is $N+1$, which is the smallest possible dimension to purify any mixed state among the participants.

The permutational symmetry of the state is the quantum resource, with no classical analog, which enures that all participants are treated equally and are indistinguishable from the authority's point of view. This kind of requirements are gaining importance nowadays as *privacy* is becoming a serious issue in the new electronic society. In fact, permutational symmetry also appears as a natural condition in quantum de Finetti theorems [12].

Within assumptions 1 and 2, we will show that there is a maximally entangled state $|\Phi\rangle$ and a local operations and classical communication (LOCC) protocol that transforms this to any other state with the same symmetry. Moreover, we will show how all the elements of the protocol, including the construction of the state, can be performed efficiently and discuss some security issues concerning possible applications to cryptographic protocols. Along the way we will prove again the main result in [13] from a more general point of view. We will mix basic tools from several areas: representation theory, convex analysis, matrix product states (MPSs), and quantum channels. For the nonspecialized reader we introduce here the mathematical definitions that will be used later.

Definition (irrep). A representation of a group G over the vector space V is a homomorphism $\pi : G \to GL(V)$. It is an irreducible representation (irrep) if the only invariant subspaces of π are the trivial ones. That is, if for all $x \in X \subset V$ and $g \in G$, $\pi(g)x \in X$, then X is V or $\{0\}$.

We will also make use of the following lemma.

Schur's lemma. Let π be an irrep of G over V and let $\rho : V \to V$ be a linear function such that $\pi(g)V = V\pi(g)$ for all $g \in G$; then $A = c\mathbb{1}$ for some consant c.

A proof of this lemma together with many other important results in representation theory can be found in [14].

Definition (MPS). A MPS representation of a system $|\phi\rangle$ of N parties is a description of the state in the following way:

$$|\phi\rangle = \sum_{i_1,\ldots,i_N} A^{[N]}_{i_N} \cdots A^{[1]}_{i_1} |i_N \cdots i_1\rangle,$$

where $A_{i_k}^{[k]}$ are $D_k \times D_{k+1}$ matrices $D_1 = D_{N+1} = 1$, $\sum_{i_j} A_{i_j}^{[j]} A_{i_j}^{[j]\dagger} = \mathbb{1}$, and D_k is bounded by the maximum of the ranks of any reduced density matrix.

MPSs have been shown to be a useful tool for simulating one-dimensional quantum spin chains, both numerically and analytically. For these and other results on MPSs, see the recent works [15–17].

Definition (quantum channel). A quantum channel is a completely positive trace-preserving map $T : S(H) \to S(H)$ between the set of density operators of a Hilbert space. That is, $T(\rho) = E_k \rho E_k^\dagger$, where $\{E_k\}$ are operators satisfying $\sum_k E_k^\dagger E_k = \mathbb{1}_H$.

A quantum channel describes the evolution in time of a quantum system and, thus, it is a key concept in quantum information theory. For a review see [18,19].

II. THE MAXIMALLY ENTANGLED STATE

The unnormalized maximally entangled state can be described in a valence bond picture in the following way (see Fig. 1). Assume that we have singlets shared between any participant and the authority. Then we project the virtual space of the authority in the permutationally symmetric subspace, which is $N+1$ dimensional. That is, we project onto the space of total spin $N/2$. This can be seen as a star-shaped version of the famous Affleck-Kennedy-Lieb-Tasaki state [20]. Expressed as a formula, our state will be

$$|\Psi\rangle = (P_{\text{sym}} \otimes \mathbb{1}_P)(|01\rangle - |10\rangle)^{\otimes N}.$$

Since we can transform the singlet to any other maximally entangled state using a local unitary in any participant qubit, we can assume the same construction starting with $|00\rangle + |11\rangle$, and we will call the resulting state $|\Phi\rangle$. In most parts of this paper we will use the latter state. In this particular case, by considering the usual basis in the space of the authority, that is, $|\alpha\rangle = \sum_{\substack{i_1,\ldots,i_N \\ i_1+\cdots+i_N=\alpha}} \frac{1}{\sqrt{\binom{N}{\alpha}}} |i_1,\ldots,i_N\rangle$, as below we get the following explicit formula for $|\Phi\rangle$:

$$|\Phi\rangle = \sum_{\alpha=0}^{N} \sum_{\substack{i_1,\ldots,i_N \\ i_1+\cdots+i_N=\alpha}} \frac{1}{\sqrt{(N+1)\binom{N}{\alpha}}} |\alpha\rangle_A |i_1,\ldots,i_N\rangle_P. \quad (1)$$

Of course, this implies that $|\Phi\rangle = \frac{1}{\sqrt{N+1}} \sum_\alpha |\alpha\rangle_A |\alpha\rangle_P$ and therefore $|\Phi\rangle$ is the maximally entangled state along the bipartite cut AP. The problem now is that the set of participants P is delocalized and therefore one cannot use general quantum operations $\mathbb{E}$ in P, but only those that are of the form $\mathbb{E}_1 \otimes \cdots \otimes \mathbb{E}_N$. However, in many situations, since $V \mapsto V^{\otimes N}|_{H_{\text{sym}}}$ is an irrep of SU(2), Schur's lemma enables us to reduce to this situation. As we will see below, the price is the need for general positive-operator-valued measures (POVMs), since projective measurements are no longer sufficient. In any case, the state $|\Phi\rangle$ is also maximally entangled in this more restrictive scenario, since one can construct from it any state with the same symmetry using only LOCC. This is the content of the following theorem.

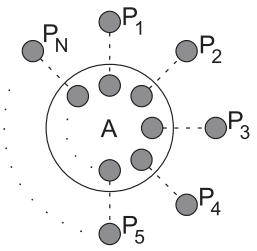

FIG. 1. Valence bond representation of the maximally entangled state Φ. Solid circles connected with dotted lines denote virtual Einstein-Podolsky-Rosen pairs; the big circle represents the projection in the Hilbert space $\mathcal{H}_{\text{sym}}$ of the authority.

Theorem 1. There is a LOCC protocol, given below, with one-way communication that allows the authority to transform $|\Phi\rangle$ to any known pure state $|\varphi\rangle$ that is permutationally symmetric in the Hilbert space of the participants.

Transformation protocol

(1) Let the Schmidt decomposition of the state $|\varphi\rangle = \sum_{i=0}^N \lambda_i |i\rangle_A |\varphi_i\rangle_P$. The authority A measures with measurement operators $\{F_U = \sqrt{N+1}\pi(U) \sum_{i=0}^N \lambda_i |\varphi_i^*\rangle\langle\varphi_i^*| \pi(U^\dagger)\}$ its part of the system (where $*$ means complex conjugation), the U's are distributed with respect to the Haar measure in SU(2), and π is the (unique) irrep of SU(2) in an $(N+1)$-dimensional space given by $V \mapsto V^{\otimes N}|_{\mathcal{H}_{\text{sym}}}$.

(2) A broadcasts the result of the measure U_0.

(3) Each participant applies to its system the unitary $Y U_0^\dagger Y$ to obtain the state $|\varphi\rangle$.

This theorem shows also that our state could be of use in situations (like secret sharing or key distribution) in which one authority is assumed to distribute some quantum state among the set of participants. One advantage now is that only permutationally symmetric states can be constructed and all the participants are then sure that they are treated on an equal footing.

Proof of Theorem 1. The result relies essentially on Schur's lemma, which guarantees that the measure in step 1 of the protocol is indeed a measure since

$$\frac{1}{N+1} \mathbb{1}_{H_A} = \int_{\text{U}(2)} \pi(U) \rho^* \pi(U^\dagger) dU, \quad (2)$$

where $\rho^* = \sum_{i=0}^N \lambda_i^2 |\varphi_i^*\rangle\langle\varphi_i^*|$.

It only remains to show that the state after the protocol is the one we want, which is a routine calculation. Suppose the result of the measure is α; then the state after the measure reads

$$\left(\pi(U_\alpha) \sum_{i=0}^N \lambda_i |\varphi_i^*\rangle\langle\varphi_i^*| \pi(U_\alpha^\dagger) \otimes \mathbb{1}_P \right) |\Phi\rangle. \quad (3)$$

Now, by the definition of π and the fact that $|00\rangle + |11\rangle$ is $U \otimes YUY$ invariant for any $U \in \text{U}(2)$, we get that $\pi(U) \otimes (YUY)^{\otimes N} |\Phi\rangle = |\Phi\rangle$ for every U. Using (1) it is now trivial to conclude that (3) is indeed equal to

$$[\pi(U_\alpha) \otimes (Y U_\alpha Y)^{\otimes N}] \sum_{i=0}^N \lambda_i |\varphi_i^*\rangle_A |\varphi_i\rangle_P. \quad (4)$$

Therefore, once the result α is known, each participant can apply $Y U_\alpha^\dagger Y$ to its system to obtain the joint state $|\varphi\rangle$ and A can apply the unitary that takes $\pi(U_\alpha)|\varphi_i^*\rangle$ to $|i\rangle$. ■

Considering $|\varphi\rangle$ to be a product state between the authority and the participants we have the following corollary.

Corollary 1 (state transfer). Given $|\Phi\rangle$, there is a LOCC protocol, given below, with one-way communication that allows the authority to create in the Hilbert space of the participants any permutationally symmetric pure state $|\varphi\rangle$.

The first thing to notice here is that the measurement required in step 1 of the state-transfer protocol has an infinite number of outcomes, which in turns implies that one needs an infinite-dimensional ancilla in order to implement it with orthogonal projectors. The way around this problem is by considering a set of unitaries $\{U_i\}_{i=1}^k \subset \mathrm{U}(2)$ and a set of scalars $\omega_i \geqslant 0$ such that $\sum_i \omega_i = 1$ and

$$\sum_{i=1}^{k} \omega_i \pi(U_i)\rho^*\pi(U_i^\dagger) = \int_{\mathrm{SU}(2)} \pi(U)\rho^*\pi(U^\dagger). \qquad (5)$$

This allows one to replace the measurement in step 1 of the protocol by the one with operators $\{F_i = \sqrt{\omega_i(N+1)}\pi(U_i)\sum_{j=0}^{N}\lambda_j|\varphi_j^*\rangle\langle\varphi_j^*|\pi(U_i^\dagger)\}$. Using Caratheodory's theorem it is not difficult to show that, in this case, k can indeed be taken $\leqslant (N+1)^2+1$ and hence polynomial in N (see the Appendix).

Since in step 2 the authority will broadcast the outcome of the measurement, it is interesting to note that, from (4), the probability of obtaining the output i is ω_i and hence independent of the state $|\varphi\rangle$ being transferred. This is crucial in cryptographic applications, like secret sharing, in which the public communication should give no information at all. The main problem with this state-transfer protocol is that the measurement in A, although it is local, depends on the state to transfer, and therefore it does not work in situations in which the authority wants to transfer an unknown state. However, thanks to Schur's lemma, it is possible to design a *teleportation-like* protocol that also works under our assumptions and allows A to teleport with LOCC any permutationally symmetric unknown state to P. The procedure is a particular case of the situation described in [21] and can be summed up in the following protocol.

Teleportation-like protocol

(1) The initial joint system is $|\varphi\rangle_{A_1} \otimes |\Phi\rangle_{A_2P}$, where $|\varphi\rangle$ is the state to be teleported.

(2) The authority A measures with measurement operators $\{F_U = (N+1)\pi(U)_{A_1} \otimes \mathbb{1}_{A_2}|\Phi\rangle\langle\Phi|\pi(U^\dagger)_{A_1} \otimes \mathbb{1}_{A_2}\}$ its part of the system, where the U's are distributed with respect to the Haar measure in U(2).

(3) A broadcasts the result of the measure U_0.

(4) Each participant applies to its system the unitary U_0 to obtain the state $|\varphi\rangle$.

Exactly as before, one can use a discrete set of unitaries to avoid the continuous parameter. In this case Eq. (5) should hold for any matrix $\rho \in \mathcal{M}_{N+1}$. By a similar reasoning one can show that the number of unitaries needed is upper bounded by $4(N+1)^4+1$. Nevertheless, weighted N-designs in U(2) already solve this problem and such a design exists with $\leqslant \binom{2N+3}{3}$ unitaries [22]. Likewise, not only is the output of the measurement completely independent of the state to be teleported, but also the set of unitaries itself. Finally, it is trivial to see that the same protocol allows one to teleport arbitrary unknown mixed states supported on the symmetric subspace.

In light of this result, it seems that if we restrict ourselves to our assumptions 1 and 2 everything works essentially as in the bipartite case, in which we start with the maximally entangled state $|\Phi\rangle = \sum_\alpha |\alpha\rangle_A|\alpha\rangle_P$. As we commented above, there is at least one important difference. In the protocols presented here we use POVMs instead of projective measurements. It is interesting to note that it is indeed *impossible* to reduce the protocol to projective measurements, as is shown in the following theorem.

Theorem 2. It is not possible to implement the *teleportation-like* protocol using projective measurements.

Proof. Let us assume that it is possible to teleport from A to P the unknown permutationally symmetric state $|\varphi\rangle$ with projective measurements. It implies that there must exist a decomposition of the form

$$|\varphi\rangle_{A_1}|\Phi\rangle_{A_2P} = \sum_{r\in R}\sqrt{p_r}|r\rangle_A \otimes \pi(U_r)|\varphi\rangle,$$

where $|r\rangle$ is an orthonormal set in the joint system $A = A_1A_2$. On one hand, if we trace out system A we get $\mathbb{1}_{H_{\mathrm{sym}}} = \sum_r p_r\pi(U_r)|\varphi\rangle\langle\varphi|\pi(U_r)^\dagger$, which implies that $|R| \geqslant N+1$. On the other hand, if we trace out system P, we get $|\varphi\rangle\langle\varphi| \otimes \mathbb{1}_{\mathcal{H}_{\mathrm{sym}}} = \sum_{r,s\in R}\sqrt{p_r p_s}\langle\varphi|\pi(U_s^\dagger U_r)|\varphi\rangle|r\rangle\langle s|$, which implies that

$$\mathbb{1}_{\mathcal{H}_{\mathrm{sym}}\otimes\mathcal{H}_{\mathrm{sym}}} = \sum_{r,s}\sqrt{p_r p_s}\,\mathrm{tr}(U_s^\dagger U_r)^N|r\rangle\langle s|$$

and hence $\mathrm{tr}(U_s^\dagger U_r) = \delta_{rs}$. But this is not possible since $U_r, U_s \in \mathrm{U}(2)$. ■

III. PROPERTIES OF THE STATE

A. Characterization by symmetries

Just as the state $|00\rangle + |11\rangle$ can be characterized as the unique pure two-qubit state that is invariant under the action of $U \otimes U$ for any unitary U, one can show that our state $|\Phi\rangle$ is the unique pure state, within assumptions 1 and 2, that is invariant under the action of $U^{\otimes N} \otimes \pi(YUY)$ for any unitary $U \in \mathrm{U}(2)$, where π is the (unique) unitary irrep of SU(2) in an $(N+1)$-dimensional space given by $V \mapsto V^{\otimes N}|_{\mathcal{H}_{\mathrm{sym}}}$.

B. Creation of the state

Is there an efficient way, that is, polynomial in the parameters, to construct the maximally entangled state $|\Phi\rangle$? The answer is yes and comes from the following MPS representation:

$$|\Phi\rangle = \sum_{\alpha_0,i_1,\ldots,i_N} A^{[0]}_{\alpha_0}A^{[1]}_{i_1}\cdots A^{[N]}_{i_N}|\alpha_0 i_1\cdots i_N\rangle,$$

where

$$A^{[0]}_{\alpha_0} = (0,\ldots,0,\underset{\alpha_0}{1},0,\ldots,0),$$

$$A^{[j]}_{i_j} = \sum_{\alpha_j=0}^{N-j}\frac{\sqrt{(N-j+1)\binom{N-j}{\alpha_j}}}{\sqrt{(N-j+2)\binom{N-j+1}{\alpha_j+i_j}}}|\alpha_j+i_j\rangle\langle\alpha_j|, \quad j=1,\ldots,N.$$

Using the result in [17], this immediately gives an efficient way to create the state $|\Phi\rangle$ in the following sequential manner

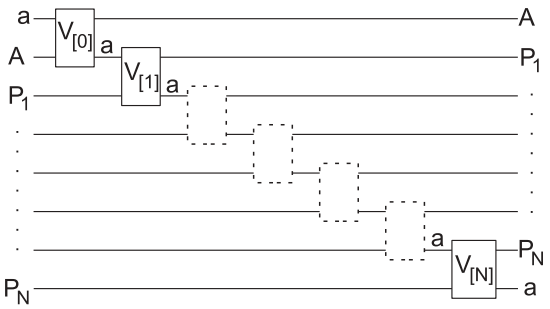

FIG. 2. Circuit for creating the state Φ in a sequential way, where each box implements a unitary $V_{[i]}$ between the ancilla a and participant i together with a SWAP operation between them.

(see Fig. 2):

$$|\Phi\rangle_{AP}|0\rangle_a = V_{[0]}\cdots V_{[N]}|0\cdots 0\rangle_{AP}|0\rangle_a,$$

where a is an ancillary system of dimension $N+1$ and $V_{[j]}$ is the unitary gate, involving only participant j (0 being the authority) and the ancilla a, given by

$$V_{[j]}|0\rangle_j|r\rangle_a = \sum_{s,i_j}\langle s|A^{[j]}_{i_j}|r\rangle|i_j\rangle_j|s\rangle_a.$$

The condition $\sum_{i_j} A^{[j]\dagger}_{i_j}A^{[j]}_{i_j} = \mathbb{1}$ makes $V_{[j]}$ unitary [17]. Of course, one may take the authority system as the ancilla and then obtain the state $|\Phi\rangle$ after one round of two-body interactions between the authority and each participant.

C. Sequential cloning

The fundamental no-cloning theorem [23] states that it is impossible to clone unknown quantum states. However, as one can infer from the excellent review [24], there are many situations in cryptography in which the optimal approximate cloning is important. In [13] (see [25] for a refinement), the authors use MPS theory to design a protocol which implements the $1\to N$ symmetric universal quantum cloning in the following sequential manner (see Fig. 3):

Step 1. An ancilla of dimension $O(N)$ interacts sequentially with each qubit.

Step 2. A final measurement is implemented in the ancilla.

Step 3. A local unitary correction is made in the qubits depending on the output of the measurement.

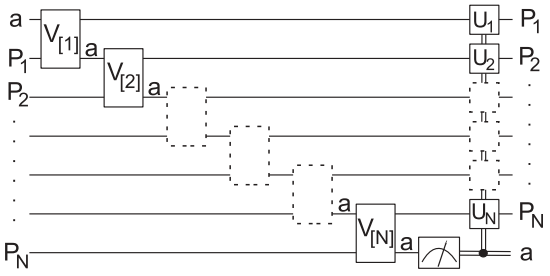

FIG. 3. Sequential circuit implementing cloning. First, the maximally entangled state is created sequentially between the ancilla and the participants. Second, the ancilla is measured. Finally, depending on the result of the measurement, local unitary corrections are applied to the participants.

Since in the symmetric universal cloning the final state is supported in the symmetric subspace, one can use step 1 to create our maximally entangled state and steps 2 and 3 to teleport the cloned state to all the qubits with our *teleportation-like* protocol. Of course, the same can be done for *any* protocol in which the final state lies in the symmetric subspace.

IV. CHECKING SYMMETRY

Since the participants want to keep their privacy, they must have a way to be sure that the state they receive from the authority is permutationally symmetric or, even more, is supported in the symmetric subspace. The latter is indeed equivalent to implementing the measure of the total spin in N spin-$\frac{1}{2}$ particles. A simple way to do so is the following protocol which requires very little computational power in the participants: a one-qubit channel from participant i to participant $i+1$ and the ability to implement two-qubit measures. The protocol aims to (i) do nothing if the original state was supported on the symmetric subspace, and (ii) end up with a state supported on the symmetric subspace.

The protocol consists of repeating the following round R times. With probability $1/N$, participant i sends its qubit to participant $i+1$, which checks if the $(i,i+1)$ qubits are supported in the symmetric or the antisymmetric subspace. If it is the latter, participant $i+1$ constructs the mixed state over the symmetric subspace and sends the ith qubit back to participant i.

The quantum channel implemented is $T = 1/N\sum_{i=1}^{N} T_{i,i+1}\otimes\mathbb{1}_{\text{all}\setminus i,i+1}$ where $T_{i,i+1}(\rho)=P_{\text{sym}}\rho_{i,i+1}P_{\text{sym}}+1/4\langle\Psi_-|\rho_{i,i+1}|\Psi_-\rangle\mathbb{1}$. It is clear that this channel verifies (i). (ii) is a consequence of the fact that all fixed points of Φ are supported in the symmetric subspace. To see this we rely on [26], in which the fixed points are characterized as those matrices ρ that are fixed points of $T_{i,i+1}$ for any $i=1,\ldots,N$; these are density matrices that are supported in the symmetric subspace of any pair of consecutive participants.

The efficiency of the protocol, that is, how it approaches a fixed point with the number of iterations is governed by the modulus of the second largest eigenvalue of T. Numerically (see Fig. 4) the second eigenvalue of the protocol after $O(N^3)$

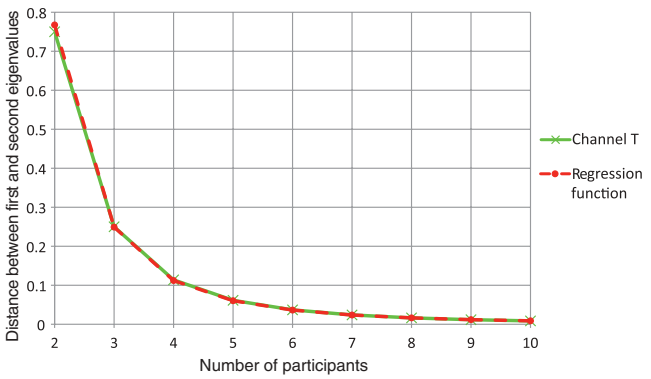

FIG. 4. (Color online) Distance between the first and second eigenvalues of the channel T as a function of the number of participants (green line) compared with the values of its regression function when considering a power regression model (red dashed line). The exponent of the function is -2.77.

rounds seems to behave as $(1 - cN^{-2.77})^{O(N^3)}$, where c is a constant, which is exponentially small in N.

Alternatively one can use the general procedures concerning secure multipartite quantum computation in [27].

V. CONCLUSION

We have considered the set of multipartite states in which the system of the participants lies in their symmetric subspace and whose state is purified by the authority. Among this set we find a maximally entangled state which, thanks to Schur's lemma, can be transformed into any other and allows teleportation from the authority to the participants. Nevertheless, POVMs are needed for both applications. We have shown how to create this maximally entangled state sequentially in an efficient way thanks to its MPS representation. Putting together the sequential generation and the teleportation result, we prove again that any protocol in which the final state lies in the symmetric subspace can be performed sequentially in an efficient way. This is illustrated with $1 \to N$ symmetric universal quantum cloning. Moreover, we have argued that the result of the measures in the protocols does not reveal information and that the participants can make sure that their state lies in the symmetric subspace.

ACKNOWLEDGMENTS

We thank Sofyan Iblisdir, Juanjo García-Ripoll, and David Pérez-García for their useful comments and discussions. This work has been partially funded by the Spanish Grants No. MTM2011-26912 and QUITEMAD and the European Project QUEVADIS.

APPENDIX

We show in this appendix that given a density matrix $\rho \in \mathrm{Herm}(\mathcal{H}_{\mathrm{sym}})$ there exists a set of unitaries $\{U_i\}_{i=0}^{(N+1)^2} \subset \mathrm{U}(2)$ and a set of scalars $\lambda_i \geqslant 0$ such that $\sum_i \lambda_i = 1$ and

$$\sum_{i=0}^{(N+1)^2} \lambda_i \pi(U_i)\rho\pi(U_i^\dagger) = \int_{\mathrm{SU}(2)} \pi(U)\rho\pi(U^\dagger).$$

Proof. Let $T : \mathbb{U}(2) \to \mathrm{Herm}(\mathcal{H}_{\mathrm{sym}})$ be defined by $U \to T_U$ where $T_U = U^{\otimes N}\rho U^{\otimes N\dagger}$. Let $S \in \mathrm{Herm}(\mathcal{H}_{\mathrm{sym}})$ be the result of applying the twirling operator to ρ, that is, $S := \int_{U\in\mathrm{U}(2)} U^{\otimes N}\rho U^{\otimes N\dagger} dU$. We have shown in (2) that $S = \frac{1}{N+1}\mathbb{I}_{\mathcal{H}_{\mathrm{sym}}}$. Let h be a linear functional of $\mathrm{Herm}(\mathcal{H}_{\mathrm{sym}})$ whose positive closed half space contains $\mathrm{Im}(T)$; then

$$h(S) = \int_{U\in\mathrm{U}(2)} h(T_U)dU \geqslant 0,$$

so $h(S) \in \overline{co}[\mathrm{Im}(T)]$. Moreover, if $\mathrm{Im}(T) \not\subseteq \ker(h)$ then there is an $\epsilon > 0$ such that $\mathrm{Im}(T)$ meets $h^{-1}[(\epsilon,\infty)]$. So the set $V = (h \circ T)^{-1}[(\epsilon,\infty)]$ of $\mathbb{U}(2)$ is nonvoid and, by the continuity of T, open. Therefore $h(S) > \epsilon\mu(V) > 0$. Hence

$$S \in \mathrm{relint}co[\mathrm{Im}(T)] \subseteq co[\mathrm{Im}(T)].$$

Then, applying Caratheodory's theorem [28], there exist functions $U_0, U_1, \ldots, U_{(N+1)^2} \in \mathrm{U}(2)$ such that $S \in co\{T_{U_0}, T_{U_1}, \ldots, T_{U_{(N+1)^2}}\}$. That is, there exist $\lambda_i \geqslant 0$, $U_i \in \mathrm{U}(2)$ for $i = 0, \ldots, (N+1)^2$ such that $\sum_i \lambda_i = 1$ and

$$\frac{\mathrm{tr}(A)}{N+1}\mathbb{I}_{\mathcal{H}_{\mathrm{sym}}} = \sum_{i=0}^{(N+1)^2} \lambda_i U_i^{\otimes N}\rho U_i^{\otimes N\dagger}.$$

■

[1] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[2] T. S. Cubitt, F. Verstraete, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **91**, 037902 (2003).
[3] D. Pérez-García, M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge, Commun. Math. Phys. **279**, 455 (2008); J. Briet and T. Vidick, arXiv:1108.5647v2.
[4] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[5] A. Kitaev, Ann. Phys. (NY) **321**, 2 (2006).
[6] A. W. Harrow and A. Montanaro, in *51st IEEE Annual Symposium on the Foundations of Computer Science, 2010* (IEEE Computer Society, Los Alamitos, CA, 2010), p. 633.
[7] A. Kitaev and J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006).
[8] M. Popp, F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac, Phys. Rev. A **71**, 042306 (2005).
[9] T.-C. Wei and P. M. Goldbart, Phys. Rev. A **68**, 042307 (2003).
[10] M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007).
[11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[12] R. Konig and R. Renner, J. Math. Phys. **46**, 122108 (2005).
[13] Y. Delgado, L. Lamata, J. León, D. Salgado, and E. Solano, Phys. Rev. Lett. **98**, 150502 (2007).
[14] B. Simon, *Representations of Finite and Compact Groups*, Graduate Studies in Mathematics, Vol. 10 (American Mathematical Society, Providence, RI, 1996).
[15] S. R. White, Phys. Rev. Lett. **69**, 2863 (1992).
[16] M. B. Hastings, J. Stat. Mech.: Theory Exp. (2007) P08024.
[17] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac, Quantum Inf. Comput. **7**, 1 (2006).
[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[19] M. Wolf, http://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf.
[20] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Phys. Rev. Lett. **59**, 799 (1987).
[21] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, Phys. Rev. Lett. **84**, 3486 (2000).
[22] A. Roy and A. Scott, Designs, Codes Cryptogr. **53**, 13 (2009).
[23] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[24] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005).

[25] L. Lamata, J. León, D. Pérez-García, D. Salgado, and E. Solano, Phys. Rev. Lett. **101**, 180506 (2008).

[26] F. Verstraete, M. M. Wolf, and J. Ignacio Cirac, Nat. Phys. **5**, 633 (2009).

[27] C. Crépeau, D. Gottesman, and A. Smith, in *Proceedings of the 34th Annual ACM Symposium on the Theory of Computing (STOC'02)*, edited by J. H. Reif (ACM, New York, 2002), pp. 643–652; M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, in *IEEE Annual Symposium on the Foundations of Computer Science*, *2006* (IEEE Computer Society, Los Alamitos, CA, 2066), p. 249.

[28] C. Carathéodory, Rend. Circ. Mat. Palermo **32**, 193 (1911).