Perfect Quantum Privacy Implies Nonlocality

Remigiusz Augusiak,[1] Daniel Cavalcanti,[1] Giuseppe Prettico,[1] and Antonio Acín[1,2]

[1]*ICFO-Institut de Ciències Fotòniques, E-08860 Castelldefels, Barcelona, Spain*
[2]*ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*

Private states are those quantum states from which a perfectly secure cryptographic key can be extracted. They represent the basic unit of quantum privacy. In this work we show that all states belonging to this class violate a Bell inequality. This result establishes a connection between perfect privacy and nonlocality in the quantum domain.

PACS numbers: 03.65.Ud, 03.67.Dd

Classical and quantum information theory (QIT) are mainly theories about resources [1]. Quantum features however make the quantum theory richer and more powerful than its classical counterpart. This richness is reflected by the variety of different resources appearing in the quantum formalism. These are for instance entanglement [2], i.e., the existence of compound states that do not admit a description in terms of probabilistic combinations of products of states representing individual subsystems, secret correlations [3], that is, correlations that cannot be created by public communication, and nonlocal correlations (see below) [4]. While some of these resources, e.g., secret correlations, are also found in the classical formalism, most of them do not have a classical analogue. This allows performing tasks that are not achievable in the classical world such as quantum teleportation [5] or secure key distribution [6,7]. The two general questions the theory addresses are (i) understanding those quantum resources necessary to accomplish an information task and (ii) establishing interconversion laws between all the different resources.

A key step when comparing and quantifying resources consists of the identification of the basic unit for each of them. It is well established that a Bell state, that is, a two-qubit maximally entangled state, represents the basic unit of entanglement, known as *e*-bit [8]. Moving to secret correlations, Horodecki *et al.* showed that private states are the basic unit of privacy in the quantum domain [9,10]. Clearly, all these states are entangled, as entanglement is a necessary condition for secure key distribution [11,12]. However, a Bell state is just the simplest state belonging to the larger class of private states. This implies that the distillation of privacy from quantum states is not equivalent to entanglement distillation, as it was commonly believed. Indeed, key (entanglement) distillation from a quantum state ρ can be understood as the process of extracting copies of private (Bell) states out of many copies of ρ. This nonequivalence is behind the existence of bound entangled states that, though not allowing for distillation of the Bell states [13], are a resource for secure key distillation [9,10].

Beyond these results, however, the principles allowing for secure key distillation from quantum resources, a crucial question in QIT, are hardly understood. In order to achieve this, it is essential to identify the quantum properties common to all private states. It is well known that Bell states are nonlocal since they violate the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [14]. Moved by this fact, one could ask whether all private states violate a Bell inequality. This is *a priori* unclear, as private states may exhibit radically different entanglement properties [10].

In this work we address the above question and show that all private states are indeed nonlocal. This result is general, as our proof works for any dimension and any number of parties. Private states, then, not only represent the unit of quantum privacy, but also allow two distant parties to establish a different quantum resource, namely, nonlocal correlations. These states contain the strongest form of entanglement as they can give rise to correlations with no classical analogue. More generally, our findings point out an intriguing connection between two of the most intrinsic quantum properties: privacy and nonlocality.

Preliminaries.—Before proceeding with the proof of our results, we recall in what follows the notions of nonlocality and private states.

Consider first a Bell-type experiment in which party i can measure one of the k_i observables $\{A_i^{(j_i)}\}$ ($j_i = 1, \ldots, k_i$), each with $r_i^{(j_i)}$ outcomes denoted by $a_i^{(j_i)} \in \{1, \ldots, r_i^{(j_i)}\}$. We say that there exists a local model for this experiment if the conditional probabilities $P(a_1^{(j_1)}, \ldots, a_N^{(j_N)} | A_1^{(j_1)}, \ldots, A_N^{(j_N)})$ of obtaining result $a_i^{(j_i)}$ upon the measurement of $A_i^{(j_i)}$, can be written in the following form

$$P(a_1^{(j_1)}, \ldots, a_N^{(j_N)} | A_1^{(j_1)}, \ldots, A_N^{(j_N)})$$
$$= \int d\lambda P(\lambda) P(a_1^{(j_1)} | A_1^{(j_1)}, \lambda) \ldots P(a_N^{(j_N)} | A_N^{(j_N)}, \lambda). \quad (1)$$

Fine [15] showed that the existence of this model for the experiment is equivalent to the existence of a joint probability distribution $P(a_1^{(1)}, \ldots, a_1^{(k_1)}, \ldots, a_N^{(1)}, \ldots, a_N^{(k_N)})$ in-

volving all local measurements, such that the marginal probabilities reproduce the observed measured outcomes. The observed correlations are said to be non-local if the conditional probability distributions $P(a_1^{(j_1)}, \ldots, a_N^{(j_N)} | A_1^{(j_1)}, \ldots, A_N^{(j_N)})$ do not admit a local model. An N-partite quantum state ρ_N is then nonlocal whenever it is possible to find local measurements leading to nonlocal correlations when applied to ρ_N.

Now, let us pass to the definition of private states [9,10,16,17]. In general, these are N-partite states that can be written as

$$\Gamma_{\mathsf{AA}'}^{(d)} = \frac{1}{d} \sum_{i,j=0}^{d-1} (|i\rangle\langle j|)_{\mathsf{A}}^{\otimes N} \otimes U_i \rho_{\mathsf{A}'} U_j^{\dagger}, \qquad (2)$$

where $\rho_{\mathsf{A}'}$ is some density matrix, $\{U_i\}$ a set of unitary operations, and $\mathsf{A} = A_1 \ldots A_N$ and $\mathsf{A}' = A_1' \ldots A_N'$ are multi-indices referring to subsystems. The subsystem marked with the subscript A consists of N qudits and is called the key part. The remaining subsystem is the shield part and is defined on some arbitrary finite-dimensional product Hilbert space $\mathcal{H}' = \mathcal{H}_1' \otimes \ldots \otimes \mathcal{H}_N'$. Party i holds one particle from the key part A_i and one from the shield part A_i'. The key point behind the private states is that $\log_2 d$ bits of perfectly secure bits of cryptographic key can be extracted from $\Gamma_{\mathsf{AA}'}^{(d)}$ [9,18].

All private states are nonlocal.—We are in position to prove our main result. We divide the proof into two parts. First, following the ideas of Ref. [16], we show that using local quantum operations (represented by appropriately chosen quantum channels) *without* any use of classical communication, the key part of any private state (subsystem A), can be brought to the form

$$\varrho_N^{(d)} = \sum_{k,l=0}^{d-1} \alpha_{kl} (|k\rangle\langle l|)^{\otimes N} \qquad (3)$$

with $\alpha_{kk} = 1/d$ and at least one off-diagonal element nonzero; i.e., there exists a pair of indices $k < l$ such that $\alpha_{kl} \neq 0$. Note that the shield part is discarded during this process. Second, we show that any state of the form (3) with $\alpha_{kl} \neq 0$ is nonlocal. Finally, the fact that local operations without classical communication cannot produce a nonlocal state from a local one implies that all private states are nonlocal.

Let us now proceed with the first part of the proof. For this aim we assume that the ith party performs, on its subsystems A_i and A_i', the quantum operation represented by the following quantum channel

$$\Lambda^{(i)}(\cdot) = V^{(i)}(\cdot)V^{(i)\dagger} + W^{(i)}(\cdot)W^{(i)\dagger}, \qquad (4)$$

where the Kraus operators $V^{(i)}$ and $W^{(i)}$ are given by

$$V^{(i)} = \sum_k |k\rangle\langle k|_{A_i} \otimes \tilde{V}_k^{(i)}, \qquad W^{(i)} = \sum_k |k\rangle\langle k|_{A_i} \otimes \tilde{W}_k^{(i)}.$$

The operators $\tilde{V}_k^{(i)}$ and $\tilde{W}_k^{(i)}$ act on the shield part belonging to the ith party (the A_i' subsystem) and are chosen so that

they define a proper quantum measurement. Precisely, given $\tilde{V}_k^{(i)}$ we define the second Kraus operator to be $\tilde{W}_k^{(i)} = (\mathbb{1} - \tilde{V}_k^{(i)\dagger} \tilde{V}_k^{(i)})^{1/2}$, with $\mathbb{1}$ being the identity matrix acting on the A_i' subsystem. Application of all the channels $\Lambda^{(i)}$ to $\Gamma_{\mathsf{AA}'}^{(d)}$ results in the following state

$$\bigotimes_{i=1}^{N} \Lambda^{(i)}(\Gamma_{\mathsf{AA}'}^{(d)}) = \frac{1}{d} \sum_{k,l=0}^{d-1} |k\rangle\langle l|^{\otimes N} \otimes \sum_{n=1}^{2^N} X_k^{(n)} U_k \varrho_{\mathsf{A}'} U_l^{\dagger} X_l^{(n)\dagger},$$

where matrices $X_k^{(n)}$ are defined as members of the 2^N-element set $\{\tilde{V}_k^{(i)}, \tilde{W}_k^{(i)}\}^{\otimes N}$. Explicitly, one has $X_k^{(1)} = \tilde{V}_k^{(1)} \otimes \ldots \otimes \tilde{V}_k^{(N)}$, $X_k^{(2)} = \tilde{V}_k^{(1)} \otimes \ldots \otimes \tilde{V}_k^{(N-1)} \otimes \tilde{W}_k^{(N)}$, and so on. Tracing now the shield part we get the promised state (3) with α_{kl} given by

$$\alpha_{kl} = \mathrm{Tr}\left[\bigotimes_{i=1}^{N} (\tilde{V}_l^{(i)\dagger} \tilde{V}_k^{(i)} + \tilde{W}_l^{(i)\dagger} \tilde{W}_k^{(i)}) U_k \varrho U_l^{\dagger} \right]. \qquad (5)$$

One also finds that, since by construction $\tilde{V}_k^{(i)\dagger} \tilde{V}_k^{(i)} + \tilde{W}_k^{(i)\dagger} \tilde{W}_k^{(i)} = \mathbb{1}$ for any i, the diagonal elements α_{kk} of this state are equal to $1/d$.

Now we need to show that at least one of the above coefficients is nonzero. In other words, for some fixed pair of k and l ($k < l$) we need to choose the operators $\tilde{V}_k^{(i)}$ and $\tilde{V}_l^{(i)}$ in such a way that α_{kl} is nonzero. To this aim we simplify a little our considerations by assuming that the operators $\tilde{V}_k^{(i)}$ and $\tilde{V}_l^{(i)}$ corresponding to ith party are positive and diagonal in the same basis. Thus, we can write these particular operators in the form

$$\tilde{V}_k^{(i)} = \sum_m v_m^{(i)} |e_m^{(i)}\rangle\langle e_m^{(i)}|, \qquad \tilde{V}_l^{(i)} = \sum_m \bar{v}_m^{(i)} |e_m^{(i)}\rangle\langle e_m^{(i)}|,$$

where we assume that the eigenvalues satisfy $v_m^{(i)}, \bar{v}_m^{(i)} \in [0, 1]$ and the eigenvectors $|e_m^{(i)}\rangle$ are orthonormal, i.e., $\langle e_m^{(i)}|e_n^{(i)}\rangle = \delta_{mn}$ (note that the fixed indices k, l we are interested in are omitted in the right-hand side of the previous expression). This, in turn means that the operators $\tilde{W}_k^{(i)}$ and $\tilde{W}_l^{(i)}$ are also diagonal in the basis $\{|e_m^{(i)}\rangle\}$, and have eigenvalues $(1 - v_m^{(i)2})^{1/2}$ and $(1 - \bar{v}_m^{(i)2})^{1/2}$, respectively. As a consequence the operator appearing in parenthesis in Eq. (5) simplifies to

$$\tilde{V}_l^{(i)\dagger} \tilde{V}_k^{(i)} + \tilde{W}_l^{(i)\dagger} \tilde{W}_k^{(i)} = \sum_m \beta_m^{(i)} |e_m^{(i)}\rangle\langle e_m^{(i)}|, \qquad (6)$$

where its eigenvalues are given by $\beta_m^{(i)} = v_m^{(i)} \bar{v}_m^{(i)} + (1 - v_m^{(i)2})^{1/2} (1 - \bar{v}_m^{(i)2})^{1/2}$ and obviously satisfy $0 \leq \beta_m^{(i)} \leq 1$. Now, putting Eq. (6) to Eq. (5), we get

$$\alpha_{kl} = \sum_{m_1, \ldots, m_N} \beta_{m_1}^{(1)} \ldots \beta_{m_N}^{(N)} \langle e_{m_1}^{(1)}| \ldots \langle e_{m_N}^{(N)}| U_k \rho U_l^{\dagger} |e_{m_1}^{(1)}\rangle \ldots |e_{m_N}^{(N)}\rangle. \qquad (7)$$

Finally, to prove that $\alpha_{kl} \neq 0$ it suffices to notice that for any nonzero matrix X (and in particular $U_k \rho U_l^{\dagger}$) there

always exists at least one N partite product vector $|\psi\rangle = |\psi_1\rangle \ldots |\psi_N\rangle$ such that $\langle\psi|X|\psi\rangle$ is nonzero. Otherwise, if for all such vectors $\langle\psi|X|\psi\rangle = 0$, the matrix X has to be the zero matrix (see Lemma 2 of Ref. [19]).

As just discussed, there exists a product vector $|\psi\rangle$ such that $\langle\psi|U_k\rho U_l^\dagger|\psi\rangle \neq 0$ for a pair of indices $k < l$. Therefore we can always chose $\tilde{V}_k^{(i)}$ and $\tilde{V}_l^{(i)}$ for each party in such way that $|\psi\rangle$ is one of the product vectors appearing in Eq. (7) (more precisely, $|\psi_i\rangle$ can be set as one of eigenvectors of $\tilde{V}_k^{(i)}$ and $\tilde{V}_l^{(i)}$). Now, we can use the freedom in the numbers $\beta_m^{(i)}$ in such a way that $\alpha_{kl} \neq 0$, which is exactly what we wanted to prove. Actually, we can always choose $\tilde{V}_{k(l)}^{(i)}$ so that at least one of the coefficients α's in each row and column of $\varrho_N^{(d)}$ is nonzero.

Let us move to the second part of the proof. In what follows we show that any state of the form (3) is nonlocal. First we will consider the bipartite case and then we will move to the multipartite scenario.

Bipartite case ($d = 2$).—A generic form of the simplest example of bipartite private states (two-qubit key part) reads (zeros denote null matrices of adequate dimension)

$$\Gamma_{AA'}^{(2)} = \frac{1}{2}\begin{pmatrix} U_0\rho_{A'}U_0^\dagger & 0 & 0 & U_0\rho_{A'}U_1^\dagger \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ U_1\rho_{A'}U_0^\dagger & 0 & 0 & U_1\rho_{A'}U_1^\dagger \end{pmatrix}. \quad (8)$$

After applying the previous local quantum operations to this state the parties are left with a two-qubit state:

$$\varrho_2^{(2)} = \begin{pmatrix} 1/2 & 0 & 0 & \alpha_{01} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha_{01}^* & 0 & 0 & 1/2 \end{pmatrix}. \quad (9)$$

Since we already know that $\alpha_{01} \neq 0$, it follows from the criterion proposed in Ref. [20] that the above state violates the CHSH-Bell inequality [14] (here written in the equivalent Clauser-Horne form [21])

$$P(A_1B_1) + P(A_2B_1) + P(A_1B_2)$$
$$- P(A_2B_2) - P(A_1) - P(B_1) \leq 0. \quad (10)$$

Here $P(A_iB_j)$ denotes the probability that Alice and Bob obtain the first result upon the measurement of observables A_i and B_j ($i, j = 1, 2$). Recall that the CHSH test involves the measurement of two dichotomic observables per site.

Bipartite case ($d > 2$).—For higher dimensional bipartite private states we use the fact that the inequality (10) only involves one measurement outcome for each of the observables. For this purpose, let us first assume that some α_{kl} is nonzero and rewrite $\varrho_2^{(d)}$ [cf. Eq. (3)] as

$$\varrho_2^{(d)} = \begin{pmatrix} \ddots & \vdots & & \vdots & \\ \cdots & 1/d & \cdots & \alpha_{kl} & \cdots \\ & \vdots & \ddots & \vdots & \\ \cdots & \alpha_{kl}^* & \cdots & 1/d & \cdots \\ & \vdots & & \vdots & \ddots \end{pmatrix}. \quad (11)$$

The marked 2×2 submatrix can be seen, up to a normalization factor $2/d$, as a two-qubit state like the one given in Eq. (9). As we have just shown, any such two-qubit state with nonzero off-diagonal element is nonlocal. Therefore, to prove nonlocality of $\varrho_2^{(d)}$ we can design the observables A_i and B_i ($i = 1, 2$) so that their first outcomes correspond to one-qubit projectors (embedded in $\mathbb{C}^d$) leading to the violation of (10) by the corresponding two-qubit state. Precisely, we take the projectors $\mathcal{P}_A^{(i)} = |\psi_i\rangle\langle\psi_i|$ and $\mathcal{P}_B^{(i)} = |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ ($i = 1, 2$), where the pure states $|\psi_i\rangle$ and $|\tilde{\psi}_i\rangle$ are of the general one-qubit form $a|k\rangle + b|l\rangle$. The remaining outcomes (which are irrelevant from the point of view of the inequality (10) of the involved observables $A_i(B_i)$ can just correspond to projectors $\mathbb{1} - \mathcal{P}_{A(B)}^{(i)}$ ($i = 1, 2$).

Now, by using these settings in the CHSH test (10), one sees that the state (11) leads to almost the same violation as for the two-qubit state in Eq. (9) with the only difference being the normalization factor $2/d$. Clearly, this does not cause any problem since the same factor appears in all the terms of the inequality. Therefore it *does not* change the sign of the CHSH parameter (10). As a conclusion the CHSH-Bell inequality for any bipartite state $\varrho_2^{(d)}$ is also violated.

Multipartite case.—We now move to the multipartite case. In order to prove the nonlocality of the states (3) we exploit the fact that, given a generic N-partite state, ρ_N, if there exist local projections of $N - m$ particles onto a product state leaving the remaining m particles in a nonlocal state, ρ_m, the initial state ρ_N is nonlocal. This follows from the fact that one cannot produce in this way a nonlocal state from a local one. The same reasoning was used, e.g., in Ref. [22] in the context of proving the nonlocality of general multipartite pure entangled states.

Indeed, denote by A_i ($i = m + 1, \ldots, N$) the local measurements (with outcomes a_i) by the previous $N - m$ parties such that for one of the outcomes, say 0, the state ρ_m shared by the remaining m parties is nonlocal. For the sake of simplicity we assume that the nonlocality of this m-partite state can be proven with only two measurements per site, A_i and A_i' with outcomes a_i and a_i' ($i = 1, \ldots, m$) (our reasoning can be trivially adapted to Bell tests involving more measurements). According to Fine's result (see above), there cannot exist a joint probability distribution $P(a_1, a_1', \ldots, a_m, a_m'|a_{m+1} = 0, \ldots, a_N = 0)$ reproducing the observed outcomes for the m parties conditioned on the fact that the measurement result for the remaining $N - m$ parties was equal to 0. Now, consider a Bell test

for the initial N-partite state ρ_N where the parties apply all the previously introduced measurements. Assume that the obtained statistics can be described by a local model. Then, there exists a joint probability distribution $P(a_1, a'_1, \ldots, a_m, a'_m, a_{m+1}, \ldots, a_N)$. But this would immediately imply the existence of the joint probability distribution $P(a_1, a'_1, \ldots, a_m, a'_m | a_{m+1} = 0, \ldots, a_N = 0)$, which is in contradiction with the fact that ϱ_m is nonlocal. Thus, the initial state ρ_N has to be nonlocal.

Using this argument, in order to prove the nonlocality of multipartite states $\varrho_N^{(d)}$ it is enough to build local projections mapping these states into a nonlocal state of a fewer number of particles. Consider the local projections P_ϕ onto $|\phi\rangle = (1/\sqrt{d})(|0\rangle + \ldots + |d-1\rangle)$. Projecting an arbitrary subset of $N - m$ particles of $\varrho_N^{(d)}$ onto P_ϕ the remaining m parties are left with following m-partite state

$$\varrho_m^{(d)} = \sum_{k,l=0}^{d-1} \alpha_{kl}(|k\rangle\langle l|)^{\otimes m}. \tag{12}$$

Thus, if $N - 2$ parties apply the projector P_ϕ to the state (3), the remaining two parties are left with a bipartite private state $\varrho_2^{(d)}$. However, we have just shown that this state is nonlocal. Thus, $\varrho_N^{(d)}$ must also be nonlocal.

Discussion.—Private states play a relevant role in QIT because they represent perfectly secure bits of cryptographic key [9,10,17]. Knowing their entanglement properties is crucial to understand the mechanism allowing for secure key distribution from quantum states. In general, private states are thought to have a weaker form of entanglement than Bell states. However, we have shown here that all private states are nonlocal. They have, then, the strongest form of quantum correlations, since the results of local measurements on these states cannot be reproduced by classical means.

Finally, it would be interesting to study how our findings can be related to the Peres conjecture [23], a long-standing open question in quantum information theory. This conjecture states that bound entangled states do not violate any Bell inequality. The intuition is that these states have a very weak form of quantum correlations. Then, all the correlations obtained from these states should have a classical description. Note, however, that there exist bound entangled states with positive partial transposition which are arbitrarily close (in the trace norm) to private states [9,10,17,18,24]. This is indeed the reason why these examples of bound entangled states have nonzero distillable cryptographic key. But, as shown here, all private states are nonlocal. One would then be tempted to conclude that these bound entangled states are also nonlocal. Interestingly, the situation is subtler than initially thought. In fact, recall that the nonlocality of private states has been proven here by showing the violation of the CHSH-Bell inequality. Unfortunately, this inequality cannot be violated by bound entangled states with positive partial trans-

position [25]. This implies that the violation of this inequality by private states arbitrarily close to bound entangled states has to be very small. In view of all these findings it appears interesting to analyze the nonlocal properties of bound entangled states with positive distillable secret key.

[1] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991); M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] R. Horodecki *et al.*, Rev. Mod. Phys. **81**, 865 (2009).
[3] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[4] V. Scarani, arXiv:0910.4222.
[5] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[6] C. H. Bennett and G. Brassard, *Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[8] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).
[9] K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005).
[10] K. Horodecki *et al.*, IEEE Trans. Inf. Theory **55**, 1898 (2009).
[11] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004); M. Curty *et al.*, Phys. Rev. A **71**, 022306 (2005).
[12] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[14] J. F. Clauser *et al.*, Phys. Rev. Lett. **24**, 549 (1970).
[15] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).
[16] P. Horodecki and R. Augusiak, Phys. Rev. A **74**, 010302 (R) (2006).
[17] R. Augusiak and P. Horodecki, Phys. Rev. A **80**, 042307 (2009).
[18] K. Horodecki *et al.*, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[19] K. Życzkowski *et al.*, Phys. Rev. A **58**, 883 (1998).
[20] R. Horodecki *et al.*, Phys. Lett. A **200**, 340 (1995).
[21] J. F. Clauser and M. A. Horne, Phys. Rev. D **10**, 526 (1974).
[22] S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992).
[23] A. Peres, Found. Phys. **29**, 589 (1999).
[24] R. Augusiak and P. Horodecki, Europhys. Lett. **85**, 50 001 (2009).
[25] R. F. Werner and M. M. Wolf, Phys. Rev. A **61**, 062102 (2000).