PHYSICAL REVIEW A **74**, 010305(R) (2006)

Bound entanglement maximally violating Bell inequalities: Quantum entanglement is not fully equivalent to cryptographic security

Remigiusz Augusiak* and Pawel Horodecki
Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gdańsk, Poland
(Received 27 July 2005; published 28 July 2006)

It is shown that Smolin four-qubit bound entangled states [J. A. Smolin, Phys. Rev. A **63**, 032306 (2001)] can maximally violate the simple two-setting Bell inequality similar to the standard Clauser-Horne-Shimony-Holt (CHSH) inequality. The simplicity of the setting and the robustness of the entanglement make it promising for current experimental technology. On the other hand, the entanglement does not allow for secure key distillation, so neither entanglement nor maximal violation of Bell inequalities implies directly the presence of a quantum secure key. As a result, one concludes that two tasks—reducing of communication complexity and cryptography—are not (even qualitatively) equivalent in a quantum multipartite scenario.

DOI: 10.1103/PhysRevA.74.010305 PACS number(s): 03.67.Mn, 03.67.Hk

Quantum entanglement is one of the most intriguing phenomena within quantum physics. The pure state of a composite quantum system is considered entangled if it is impossible to describe its subsystems by pure states. Historically, the importance of quantum entanglement has been recognized by Einstein, Podolsky, and Rosen (EPR) [1] and Schrödinger [2]. The so-called EPR paradox began a long debate over whether local realistic theories can simulate quantum mechanics. The well-known Bell theorem [3] says that such a simulation is, in general, impossible. On the other hand, entanglement has been found to be an important resource in quantum information theory [4] involving, in particular, an entanglement-based cryptographic scheme [5].

To overcome the problem of noisy entanglement [6], the idea of entanglement distillation has been invented [7], which is useful in quantum privacy amplification [8]. While any entangled two-qubit (or qubit-qutrit) state can be distilled to a singlet form [9], this is not true in general, a fact that reflects the existence of the so-called bound entanglement phenomenon [10]. This is a very weak type of entanglement that cannot serve in dense coding or teleportation. However, in the multipartite case (see [11]) it can be useful for remote quantum information concentration [12] (bipartite) activation [13] and (multipartite) superactivation [14], classical cryptographic key distillation [15], or nonadditivity of quantum channels with multiple receivers [16]. Remarkably, bipartite bound entangled (BE) states have not been reported to violate any Bell inequalities so far (see [17,18]). For the multipartite case, the seminal result has been obtained by Dür [19], who showed that some multiqubit BE states violate two-settings Bell inequalities. The following question has arisen: what is the minimal size of a quantum system (in terms of subsystems) that admits bound entanglement to violate Bell inequalities?

It is an important question since violation of Bell inequalities by entangled states seems to imply that the entanglement is useful for some classical tasks. In particular, it has been shown that violation of a wide class of Bell inequalities is equivalent to the possibility of reduction of communication complexity by the corresponding states [20,21]. There is even a conjecture following cryptography analysis [22] that violation of Bell inequalities is an indicator of the usefulness of entanglement in general [23].

The minimal number of BE qubits violating the inequalities in the Dür scheme was $N=8$. This limit has been lowered by Kaszlikowski *et al.* [24] to $N\geqslant 7$ with the help of three apparatus settings per site, and then by Sen *et al.* [25] to $N\geqslant 6$ with the help of so-called functional Bell inequalities [26]. The relation of the results to bipartite distillability has been analyzed in detail in [18].

In the present paper, we show that there are BE states that violate *maximally* very simple Bell inequalities, i.e., with two settings per site [17] for $N=4$, in a way similar to standard CHSH inequality for two qubits [27]. Moreover, the robustness of the considered bound entanglement is comparable to that of entangled two-qubit Werner states. Both the simplicity of the scenario and the robustness make the result very promising from an experimental point of view. Note that, although maximal violation of Bell inequalities by some mixed states has already been shown [28], to our knowledge this is the first time such a violation has been reported for bound entangled states.

Somewhat surprisingly, despite maximal violation, the considered states do not allow for secure key distillation, as was the case for bipartite BE states from Ref. [15]. This is a striking feature: the existence of the Ekert protocol [5] might suggest that violation of Bell inequalities is always an indicator of secure key distillation. For the bipartite case this intuition has been to some extent formalized in Ref. [29] where the authors stated that violation of some Bell inequalities is sufficient for cryptographic security even if an eavesdropper uses some post-quantum theories and is limited only by no signaling condition. The correlations considered in [29] are the same as those coming from the singlet state in quantum mechanics.

Quite remarkably, in the present paper the considered Bell test on quantum state reveals singlet-like correlations between any arbitrarily chosen party and the three remaining parties *considered locally rather than jointly*. Despite this fact, it is impossible to distill quantum key in this scenario. An implication of the result is the conclusion that being a

*Electronic address: remik@mif.pg.gda.pl

precondition for quantum cryptography [30] entanglement is not always sufficient for the latter, even if apparently convincing evidences occur.

The BE states that we will show to violate Bell inequalities are Smolin states [32]. They have a special property: if the four particles are far apart, no entanglement between any subsystems can be distilled. If, however, two particles are in the same location, it is possible to create maximal entanglement between the remaining two particles by means of local operations and classical communication (LOCC). Detailed analysis has shown additional interesting aspects: the entanglement cost of such states corresponds just to a singlet state [33].

Using the result we also show, via the results of Refs. [20,21], that the considered bound entanglement can serve to reduce communication complexity. In fact, somewhat surprisingly, it reduces it optimally, i.e., there is no quantum state with better performance than the considered bound entangled one.

Noisy Smolin states. Let us consider the following four-qubit mixed state defined on a product Hilbert space $(\mathbb{C}^2)^{\otimes 4}$:

$$\varrho^S_{ABCD}(p) \equiv \varrho^S(p) = (1-p)\frac{I^{\otimes 4}}{16} + p\rho^S, \tag{1}$$

where I stands for identity acting on one-qubit space, while ρ^S is the four-qubit bound entangled state introduced by Smolin [32] and is defined through the relation

$$\rho^S_{ABCD} = \rho^S = \frac{1}{4}\sum_{i=1}^{4} |\psi_i^B\rangle\langle\psi_i^B| \otimes |\psi_i^B\rangle\langle\psi_i^B|, \tag{2}$$

where the two-qubit states $|\psi^B_{1(2)}\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$, $|\psi^B_{3(4)}\rangle = (1/\sqrt{2})(|01\rangle \pm |10\rangle)$ form the so-called Bell basis in a Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. It is worth noticing that the states (1) are fully permutationally invariant, since they can be written in the form

$$\varrho^S(p) = \frac{1}{16}\left(I^{\otimes 4} + p\sum_{i=1}^{3} \sigma_i^{\otimes 4}\right) \tag{3}$$

with σ_i (i= 1, 2, 3) denoting the standard Pauli matrices. One can see that for $p=1/3$, the state $\varrho^S(p)$ is separable. Indeed, for such a value of p we can rewrite Eq. (1) as

$$\varrho^S\left(\frac{1}{3}\right) = \frac{1}{6}\sum_{i=1}^{3}\sum_{s=-}^{+} \varrho_i^{(s)} \otimes \varrho_i^{(s)}, \tag{4}$$

where $\varrho_k^{(\pm)}$ are two-qubit separable states (see [34]):

$$\varrho_k^{(\pm)} = \frac{1}{2}(P_k^{(+)} \otimes P_k^{(\pm)} + P_k^{(-)} \otimes P_k^{(\mp)}) \quad (k = 1,2,3), \tag{5}$$

$P_k^{(\pm)}$ denotes projectors onto eigenvectors of σ_k (k= 1, 2, 3) corresponding to eigenvalues ±1. Since by LOCC we can add some noise to the state, the above fact implies that for all $p \leqslant 1/3$ the state ϱ is separable. On the other hand, for $p > 1/3$ the state is BE. Indeed, it is easy to see that for this region the state violates PPT separability criterion [35] if we transpose indices corresponding to a single qubit, i.e., against any of the cuts: $A|BCD$, $B|ACD$, etc. Thus the state is entangled. It is BE since the state maintains the property of original ρ^S: it is separable against bipartite symmetric cuts like $AB|CD$, $BC|AD$, etc., which makes sure that no maximal entanglement between any subsystems can be distilled.

Violation of Bell inequalities. Below we shall prove that for $p > 1/\sqrt{2}$ the state violates Bell inequalities introduced in Ref. [17]. In the corresponding scenario, each of the N parties corresponding to index j (j=1,2,…,N) can choose between two dichotomic observables $O^{(j)}_{k_j}$ (k_j=1,2). The set of 2^{2^N} Bell inequalities is [17]

$$\left| \sum_{s_1,\ldots,s_N=-1}^{1} S(s_1,\ldots,s_N) \sum_{k_1,\ldots,k_N=1}^{2} s_1^{k_1-1}\cdots s_N^{k_N-1} E_{k_1,\ldots,k_N} \right| \leqslant 2^N, \tag{6}$$

where S is an arbitrary sign function, and the correlation function E is defined through the relation (average over many runs of experiment) $E_{k_1,\ldots,k_N} = \langle \Pi_{j=1}^N O^{(j)}_{k_j}\rangle_{\text{av}}$. Trying to predict the above (experimental) average, local hidden variable (LHV) theories offer its calculation as an integral over probabilistic measure on the space of "hidden parameters." The measure corresponds to classical states. In a quantum-mechanical regime, the observables depend on vector parameters, i.e., are of the form $\hat{O}^{(j)}_{k_j} = \hat{n}^{(j)}_{k_j}\cdot\vec{\sigma}$ and the corresponding average for a given quantum state ϱ is calculated as follows:

$$E^{QM}_{k_1,\ldots,k_N}(\varrho) = \text{Tr}[\varrho \hat{O}^{(1)}_{k_1} \otimes \cdots \otimes \hat{O}^{(N)}_{k_N}]. \tag{7}$$

One can see that for the following nontrivial sign function: $S(+,+,-,-) = S(+,-,+,-) = S(-,+,+,-) = S(-,-,-,-) = -1$, where $\pm$ stands for ±1 (for other cases, the sign function is equal to unity), and for N=4 we can derive the following Bell inequality:

$$|E_{1,1,1,1} + E_{1,1,1,2} + E_{2,2,2,1} - E_{2,2,2,2}| \leqslant 2. \tag{8}$$

This inequality can be also derived very easily using the same technique as in the standard CHSH inequality [27]. We keep the above derivation for the purpose of further analysis.

Subsequently, for the state given by Eq. (2), we choose the following observables: $\hat{n}^{(i)}_{1(2)} = \hat{x}(\hat{y})$ (i=1, 2, 3) and $\hat{n}^{(4)}_1 = (\hat{x}+\hat{y})/\sqrt{2}$ or $\hat{n}^{(4)}_2 = (\hat{x}-\hat{y})/\sqrt{2}$. This gives the violation of inequality (8) for any $p \in (1/\sqrt{2}, 1]$. One can easily show that for p=1, i.e., for original Smolin states $\varrho^S(p)$ [32], the above violation is maximal, i.e., there is no other quantum state that can make the right-hand side of Eq. (8) greater than $2\sqrt{2}$. To this end, it suffices to apply the co-called Cirel'son bound [36].

Remarkably, both separability and violation of Bell inequalities (8) are in the same regime as in two-qubit Werner states [6] we write them in the form $\varrho^W(p) = (1-p)\frac{1}{4}I\otimes I + p|\psi_4^B\rangle\langle\psi_4^B|$ and consider CHSH inequality. Indeed, $\varrho^W(p)$ is known (i) to be entangled for $p \in (1/3, 1]$ [6,37] and (ii) to violate Bell-CHSH inequality for $p \in (1/\sqrt{2}, 1]$ [38]. Note that, though the present violation of Bell inequalities can be interpreted as a violation by singlet-like correlations between system A and the composite system

BCD, there is one striking feature: all dychotomic observables are local, i.e., the scheme lies within the so-called *four-partite LOCC* paradigm rather than within the bipartite one.

Communication complexity. Here we analyze the Smolin state in the context of the general class of communication complexity problems, proposed by Brukner *et al.* [20] (see also [21]), in which the main goal of each party is to find the correct value of the function $f=y_1\cdots y_N S[g(x_1,\ldots,x_N)]$, where $S[g]=g/|g|=\pm 1$ is the sign function of g and $f\in\{-1,1\}$. Each party receives a two-bit input string (x_i,y_i) according to specially defined probability. The success is achieved when all parties get the correct value of f. Their joint task is to maximize the probability of success. Following the broad class of quantum protocols, it is proven in [20] that the probability of success in the quantum case is higher than in the classical one if and only if for a given entangled state one of the following Bell inequalities for the correlation function

$$\sum_{x_1,\ldots,x_N=1}^{2} g(x_1,\ldots,x_N)E_{x_1,\ldots,x_N}\leqslant B(N) \tag{9}$$

is violated. In particular, the above class contains Bell inequalities given by Eq. (6) with $B(N)=2^N$ and

$$g(x_1,\ldots,x_N)=\sum_{s_1,\ldots,s_N=\pm 1} S(s_1,\ldots,s_N)s_1^{x_1-1}\cdots s_N^{x_N-1}. \tag{10}$$

The probability P of success in the case of classical protocols is estimated as follows (for proof, see [20]):

$$P\leqslant\frac{1}{2}\left(1+\frac{B(N)}{\sum_{x_1,\ldots,x_N=1}^{2}|g(x_1,\ldots,x_N)|}\right). \tag{11}$$

On the other hand, the above inequalities are equivalent to Bell inequalities (9), i.e., are violated if the inequalities (9) are violated. Therefore, one can see that violation of the Bell inequality implies violation of the respective inequality (11) and can result in a higher probability of success in the case of quantum entanglement. To show the usefulness of the Smolin state in this context, it suffices to consider the function

$$\begin{aligned}g(x_1,\ldots,x_4)=&\,4\sqrt{2}\cos\left[(x_1-x_2)\tfrac{\pi}{2}\right]\sin\left\{\left[\tfrac{3}{2}(-1)^{x_4}-x_3\right]\tfrac{\pi}{2}\right\}\\&+4\sqrt{2}\cos\left[(x_1+x_2)\tfrac{\pi}{2}\right]\sin\left\{\left[\tfrac{3}{2}(-1)^{x_4}+x_3\right]\tfrac{\pi}{2}\right\}\end{aligned}$$

and to put $B(4)=16$. By virtue of Eq. (11), we infer that the maximal probability achievable in any classical protocol is $P^C_{\max}=0.75$, whereas the optimal value for the quantum protocol is $P^Q_{\max}=(1/2)(1+1/\sqrt{2})\approx 0.85$. It is remarkable that this optimal value can be achieved by the BE state.

First maximal violation of Bell inequalities by bound entanglement. Bound entanglement is quite a unique type of entanglement that does not possess the property of distillability. Being useful for some quantum tasks, it is located in a sense in between usual free "strong" entanglement and separability. As such, it represents the region of quantumness where natural limits of local hidden variable theories can be tested. So far it has been known that they are excluded for BE states with a number of qubits not lower that six. We show that violation of the hidden variable model test is possible in the four-qubit system. In particular, the four-qubit Smolin state can violate CHSH-like Bell inequalities *maximally*, i.e., in a way, no other quantum state can succeed better. To the best of our knowledge, this is the first time such maximal violation has been proven for BE states. This result lowers the number of qubits needed for BE to violate Bell inequalities from six to four. If we consider the family of *two settings inequalities* (which are most easy to implement) Bell inequalities, the present offers significant progress from $N=8$ [19] to $N=4$.

Violation of Bell inequalities not always equivalent to quantum cryptography. The intriguing feature of the present inequality is that it shows that the BE state here simulates maximal (singlet) correlations between *any* single party, say *A*, and the remaining three parties, say *BCD*, in a very strong way, i.e., *when each party is considered locally*. In spite of this, the state does *not* allow us to distill a singlet between *A* and the remaining parties within this four-parties paradigm: four partite LOCC operations can only produce a separable pure state from the Smolin state. In principle, this property does not automatically imply a lack of a quantum secure key (see [15]). So even more striking are the quantum cryptographic implications of the present result: one has an example showing that even very strong Bell inequalities violation or seemingly "strong" quantum entanglement does not imply cryptographic key distillation [31]. Indeed, the states are separable under any symmetric bipartite cut, which means (following the analysis of Ref. [30]) that no secure correlations can be distilled between any two groups of two people in the scheme, which, by full permutational symmetry of Eq. (2), implies that no secure key between four people can be distilled. Since the state violates multipartite Bell inequalities, this can be referred to Acin *et al.* [18], who showed that then one can distill singlets against some bipartite splitting (here $A|BCD$). It is, however, surprising that even maximal violation of Bell inequalities, with all four party observables measured *locally*, does not lead here to any better advantage of quantum security than the one observed in [18], i.e., it leads to no security within the considered (four-partite) scenario in which the violation is found.

Remarks on Smolin states and secret sharing. The interesting question is whether the correlations involved in the original Smolin state (2) represents quantum secret shared in all the parties *ABCD* (cf. [39]).

It happens that they do, at least as far as the external eavesdropper (Eve) is concerned. Due to symmetry of the state without loss of generality we can say that the bit shared by *ABCD* and secret to Eve is a result of measurement of Alice of any chosen Pauli matrix, say σ_1. Indeed, if all the other parties measure the same observable, then we have $r_A\oplus r_B\oplus r_C\oplus r_D=1$, where r_X is a binary result of the party X and we add the values modulo one. Thus if all *BCD* parties are together they can reconstruct the Alice bit r_A. Writing out the purification of the Smolin, it is easy to see that for eavesdropper E the bit r_A is completely random, so it truly represents a shared secret bit in the scheme. This is because the reduced state of Alice and Eve systems is a product state in such a representation. This proves secrecy of the bit against external party.

It would be interesting to analyze the quantum secret sharing properties concerning one or more of the parties potentially dishonest (see [39]). Further, both questions may be generalized qualitative analysis in case of noisy Smolin state (1). This, however, would require separate analysis which is not easy in general. In any case, one can raise a natural general question whether there are cases when violation of local realism is *necessary but not sufficient condition for quantum secret sharing*.

The results of the present paper are twofold. It has been shown that, quite surprisingly, multipartite bound entanglement can maximally violate Bell inequalities. Moreover, it has been provided in a much simpler case that all the previous results in the field—small (four) number of qubits and a simple (two-setting) regime—make the violation achievable within current experimental technology. The second aspect of the present paper concerns general quantum information: two important quantum information tasks within the four-parties scenario are shown to be (even qualitatively) *not* equivalent. Indeed, the possibility of generation of a quantum secure key between four locations *is not* equivalent to the possibility of reducing the communication complexity in this four-location scenario. A significant open question implied by our results (especially justified in the context of [29]) is as follows: which type of Bell inequalities already guarantees cryptographic security in quantum and post-quantum theory?

ACKNOWLEDGMENTS

R.A. thanks Maciej Demianowicz for stimulating discussions. P.H. thanks Ryszard, Michał, and Karol Horodecki for helpful discussions. The work is supported by the European Union under Grant RESQ No. IST-2001-37559 and Grant QUPRODIS No. IST-2001-38877, and by the Polish Ministry of Science under Grant No. PB2-MIN-008/P03/2003.

[1] A. Einstein *et al.*, Phys. Rev. **47**, 777 (1935).
[2] E. Schrödinger, Naturwiss. **23**, 807 (1935).
[3] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[4] *Introduction in Quantum Information and Computation*, edited by H.-K. Lo *et al.* (World Scientific, Singapore, 1998); J. Gruska, *Quantum Computing* (McGraw-Hill, London, 1999); *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, edited by D. Bouwmeester *et al.* (Springer, New York, 2000); M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000); G. Alber *et al.*, *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*, Vol. 173 of Springer Tracts in Modern Physics (Springer, Berlin, 2001).
[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[6] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[7] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[8] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).
[9] M. Horodecki *et al.*, Phys. Rev. Lett. **78**, 574 (1997).
[10] M. Horodecki *et al.*, Phys. Rev. Lett. **80**, 5239 (1998).
[11] C. H. Bennett *et al.*, Phys. Rev. Lett. **82**, 5385 (1999).
[12] M. Murao and V. Vedral, Phys. Rev. Lett. **86**, 352 (2001).
[13] P. Horodecki *et al.*, Phys. Rev. Lett. **82**, 1056 (1999).
[14] K. G. H. Vollbrecht and M. M. Wolf, Phys. Rev. Lett. **88**, 247901 (2002); P. W. Shor *et al.*, Phys. Rev. Lett. **90**, 107901 (2003); W. Dür and J. I. Cirac, Phys. Rev. A **62**, 022302 (2000).
[15] K. Horodecki *et al.*, Phys. Rev. Lett. **94**, 160502 (2005).
[16] W. Dür *et al.*, Phys. Rev. Lett. **93**, 020503 (2004).
[17] R. F. Werner and M. M. Wolf, Phys. Rev. A **64**, 032112 (2001); M. Żukowski and C. Brukner, Phys. Rev. Lett. **88**, 210401 (2002).
[18] A. Acin, Phys. Rev. Lett. **88**, 027901 (2002); A. Acin *et al.*, J. Phys. A **36**, L21 (2003); , Phys. Rev. A **66**, 042323 (2002).
[19] W. Dür, Phys. Rev. Lett. **87**, 230402 (2001).
[20] C. Brukner *et al.*, Phys. Rev. Lett. **92**, 127901 (2004).
[21] C. Brukner *et al.*, Phys. Rev. Lett. **89**, 197901 (2002).
[22] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001); Phys. Rev. A **65**, 012311 (2002); J. Phys. A **34**, 6043 (2001).
[23] A. Acin *et al.*, Int. J. Quantum Inf. **2**, 24 (2004).
[24] D. Kaszlikowski *et al.*, Phys. Rev. A **66**, 052309 (2002).
[25] A. Sen(De) *et al.*, Phys. Rev. A **66**, 062318 (2002).
[26] M. Żukowski, Phys. Lett. A **177**, 290 (1993); D. Kaszlikowski and M. Żukowski, Phys. Rev. A **61**, 022114 (2000).
[27] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).
[28] S. L. Braunstein *et al.*, Phys. Rev. Lett. **68**, 3259 (1992).
[29] J. Barrett *et al.*, Phys. Rev. Lett. **95**, 010503 (2005).
[30] M. Curty *et al.*, Phys. Rev. Lett. **92**, 217903 (2004).
[31] By cryptographic secure key distillation, one means creation (in a four distant labs scenario) of a random bit known to all parties and unknown to an eavesdropper (Eve).
[32] J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).
[33] T.-C. Wei *et al.*, Phys. Rev. A **70**, 022322 (2004).
[34] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996).
[35] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[36] B. S. Cirel'son, Lett. Math. Phys. **4**, 557 (1980).
[37] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1997).
[38] R. Horodecki *et al.*, Phys. Lett. A **200**, 350 (1995).
[39] M. Hillery *et al.*, Phys. Rev. A **59**, 1829 (1999).