

Generalized Smolin states and their properties

Remigiusz Augusiak* and Paweł Horodecki†

Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gdańsk, Poland

(Received 5 September 2005; published 12 January 2006)

Four-qubit bound entangled Smolin states are generalized with help of the Hilbert-Schmidt formalism to any even number of qubits. They are shown to maximally violate simple correlation Bell inequalities and, as such, to reduce communication complexity, although they do not admit quantum security. They are also shown to serve for remote quantum information concentration, as in the case of the original four-qubit states. It is proven that the latter effect allows us to unlock some entanglement measures and classical correlations. Also the possibility of quantum secret sharing by the considered state is pointed out.

DOI: [10.1103/PhysRevA.73.012318](https://doi.org/10.1103/PhysRevA.73.012318)

PACS number(s): 03.67.Mn

I. INTRODUCTION

Quantum entanglement [1,2] is a very important resource in quantum-information theory (QIT) [3]. It contributes to fundamental quantum-information phenomena [4–7] and itself represents a quality that is not present in classical world. Entanglement of pure states has been shown to be incompatible with any local hidden models since it violates well-known Bell inequalities [8]. It has also been proven to be an optimal resource for quantum information. The case of mixed state is more complicated. Though mixed states in many cases can serve as a QIT resource it is difficult to characterize useful mixed state entanglement in general. In addition the fundamental question initiated in [9], namely, which entangled mixed states admit local hidden variable theories, remains open still. The very interesting type of entanglement that serves as an ideal probe for the above analysis is bound entanglement (BE) [10] that cannot be distilled to pure entangled form, nevertheless turns out to be useful in some quantum QIT tasks [11–16]. On the other hand, recently, following pioneering and surprising result [17], a few multipartite bound entangled states [18,19] including especially the case of six qubits [20] have been shown to violate Bell inequalities. Note that this means that BE can serve for reduction of communication complexity in a wide class of schemes provided in [21,22]. The scenario with minimal number of particles $N=6$ required continuous setting Bell inequalities that cannot be implemented experimentally. Also no maximal violation of Bell inequalities has been reported for analyzed states.

Quite recently, however, a Smolin bound entangled state [23] representing a qubit density matrix have been reported [24] to violate Bell inequalities *maximally* in a very simple setting (similar to the CHSH [25] scenario). At the same time the states do not admit a multiparty cryptography scenario. This means that one should be careful in interpreting the Bell inequality violation in the context of quantum security.

In the present work we generalize Smolin states to any even number of particles, calling these states generalized

Smolin states (GSSs). We show that they maximally violate Bell inequalities as was the case of four qubits. As such they can optimally reduce communication complexity in some well-defined scenarios [21,22]. Still it can be shown, as in the four-qubit case, that in spite of maximal Bell violation, the states are not useful for quantum security. On the other hand we show that GSSs like the original Smolin state (see [12]) allow for remote quantum-information concentration. Quantum networks realizing the noisy GSSs are designed. Finally we discuss the relation of Bell inequality violation and quantum security. We find a possibility of interesting application of the result of information concentration as an unlocking of large amount of classical information or quantum entanglement.

This paper is organized as follows. In Sec. II it is presented the method leading to construction of the generalized Smolin states. Here, we show that these states violate certain Bell inequalities. Finally we consider a one-parameter class of states, namely, the noisy Smolin states. In particular we compare the states with a one-parameter family of states unitarily equivalent to that known as the Werner or isotropic state. In Sec. III we show that despite being bound and entangled, GSSs may be used to perform some QIC tasks. In Sec. IV there are presented networks generating noisy Werner as well as noisy generalized Smolin states. The interesting effect unlocking entanglement measures with GSSs is described in Sec. V. The paper ends with discussion in Sec. VI, which summarizes the results obtained.

II. GENERALIZED SMOLIN STATES

A. Construction

In this section we extend the last considerations concerning bound entanglement in the context of Bell inequalities [24] to the case of an arbitrary even number of particles.

At the beginning let us define the following class of unitary operations:

$$U_n^{(m)} = I^{\otimes n-1} \otimes \sigma_m \quad (m = 0, 1, 2, 3, \quad n = 1, 2, 3, \dots), \quad (2.1)$$

where $\sigma_0 = I$ is the identity acting on \mathbb{C}^2 and σ_i ($i = 1, 2, 3$) are the standard Pauli matrices. Then, let us introduce the so-

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

†Electronic address: pawel@mif.pg.gda.pl

called Bell basis defined on a Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$ as

$$\begin{aligned}
 |\psi_0^B\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), & |\psi_1^B\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
 |\psi_2^B\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\psi_3^B\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \quad (2.2)
 \end{aligned}$$

From Eqs. (2.1) and (2.2) one can immediately infer that $U_2^{(m)} P_0^B U_2^{(m)} = P_m^B$ ($m=0, \dots, 3$), where P_m^B denotes a projector onto $|\psi_m^B\rangle$. For the purposes of further analyses it is convenient to rewrite the above states using the Hilbert-Schmidt formalism (see [26]). Let us recall that every state ρ acting on the space $\mathbb{C}^2 \otimes \mathbb{C}^2$ may be written in the form

$$\rho = \frac{1}{4} \left(I \otimes I + \mathbf{r} \cdot \boldsymbol{\sigma} \otimes I + I \otimes \mathbf{s} \cdot \boldsymbol{\sigma} + \sum_{i,j=1}^3 t_{ij} \sigma_i^{\otimes 2} \right), \quad (2.3)$$

where I is defined as previously, \mathbf{r} and \mathbf{s} are vectors from \mathbb{R}^3 given, respectively, by $\mathbf{r} = \text{Tr}[\rho(\boldsymbol{\sigma} \otimes I)]$ and $\mathbf{s} = \text{Tr}[\rho(I \otimes \boldsymbol{\sigma})]$, and $\boldsymbol{\sigma}$ is a vector constructed from the Pauli matrices, i.e., $\boldsymbol{\sigma} = [\sigma_1, \sigma_2, \sigma_3]$. Coefficients $t_{ij} = \text{Tr}[\rho \sigma_i \otimes \sigma_j]$ form a real-valued matrix \mathcal{T}_2 (the subscript refers to the number of particles). For the Bell states (2.2) we have the nice geometrical structure [26] that results in particular in

$$\begin{aligned}
 |\psi_m^B\rangle\langle\psi_m^B| &= \frac{1}{4} \left(I^{\otimes 2} + \sum_{i=1}^3 t_{ii}^{(m)} \sigma_i^{\otimes 2} \right) \quad (m=0, \dots, 3), \\
 \mathcal{T}_2^{(0)} &= -\text{diag}[1, 1, 1], & \mathcal{T}_2^{(1)} &= \text{diag}[-1, 1, 1], \\
 \mathcal{T}_2^{(2)} &= \text{diag}[1, -1, 1], & \mathcal{T}_2^{(3)} &= \text{diag}[1, 1, -1]. \quad (2.4)
 \end{aligned}$$

Note that for all the Bell states vectors \mathbf{r} and \mathbf{s} equal zero and matrices $\mathcal{T}_2^{(m)}$ ($m=0, \dots, 3$) are diagonal. Moreover, all these states maximally violate the CHSH-Bell inequality for the correlation function [25], i.e., the degree of violation is $\sqrt{2}$ and it is the maximal value achievable within the quantum theory.

Then let us introduce the so-called Smolin state [23], acting on a space $(\mathbb{C}^2)^{\otimes 4}$:

$$\rho^S = \frac{1}{4} \sum_{m=0}^3 |\psi_m^B\rangle\langle\psi_m^B| \otimes |\psi_m^B\rangle\langle\psi_m^B| = \frac{1}{4} \sum_{m=0}^3 (U_2^{(m)} |\psi_0^B\rangle\langle\psi_0^B| U_2^{(m)})^{\otimes 2}. \quad (2.5)$$

This state is bound entangled since we cannot distill a singlet between any pair of particles. However, the distillation of entanglement between any two parties is possible when the two others are in the same laboratory. As shown in [24] the Smolin state posses the intriguing feature, namely despite being bound entangled it violates maximally the CHSH-type Bell inequality for four particles.

Now, we are in position to present our construction. First, let us define certain states in the following recursive way:

$$\begin{aligned}
 \rho_2 &\equiv |\psi_0^B\rangle\langle\psi_0^B|, \\
 \rho_4 &= \frac{1}{4} \sum_{m=0}^3 U_2^{(m)} \rho_2 U_2^{(m)} \otimes U_2^{(m)} \rho_2 U_2^{(m)} \equiv \rho^S, \\
 \rho_6 &= \frac{1}{4} \sum_{m=0}^3 U_4^{(m)} \rho_4 U_4^{(m)} \otimes U_2^{(m)} \rho_2 U_2^{(m)}, \\
 &\vdots \\
 \rho_{2(n+1)} &= \frac{1}{4} \sum_{m=0}^3 U_{2n}^{(m)} \rho_{2n} U_{2n}^{(m)} \otimes U_2^{(m)} \rho_2 U_2^{(m)}. \quad (2.6)
 \end{aligned}$$

This construction starts from one of the Bell states (2.2), namely, the singlet. Obviously this state is a *free* entangled state and, as previously mentioned, violates maximally Bell inequalities. This property is crucial for our purposes since, as we shall see below, our construction is ‘‘smuggling’’ it to the arbitrary even number of particles. Furthermore, $\rho_4 \equiv \rho^S$ is bound entangled and therefore, again because of this specific type of construction, all states from this class with $n \geq 2$ are bound entangled. It is interesting that from all these states it is possible to distill only one singlet whenever any subset of $2n-2$ particles are in the same laboratory. Hereafter states ρ_{2n} for $n > 2$ we shall call *generalized Smolin states*.

It is worth noticing that all these states, including ρ_2 are permutationally invariant since we have the following observation.

Observation 1. Any state ρ_{2n} may be written in the form

$$\rho_{2n} = \frac{1}{2^{2n}} \left(I^{\otimes 2n} + (-1)^n \sum_{i=1}^3 \sigma_i^{\otimes 2n} \right) \quad (n=1, 2, 3, \dots). \quad (2.7)$$

Proof. The proof will be established using mathematical induction. For $n=1$ this observation is obvious, since Eq. (2.7) represents the Hilbert-Schmidt expression for singlet (2.4). Therefore for further clarity we investigate the case with $n=2$, i.e., the case of a Smolin state. So our task is to prove that

$$\rho_4 \equiv \rho^S = \frac{1}{16} \left(I^{\otimes 4} + \sum_{i=1}^3 \sigma_i^{\otimes 4} \right). \quad (2.8)$$

with this aim it suffices to substitute the Hilbert-Schmidt expansions for all the Bell states (2.4) to Eq. (2.5) and to utilize the facts that $\sum_{m=0}^3 \mathcal{T}_2^{(m)} = \text{diag}[0, 0, 0]$ and

$$\sum_{m=0}^3 \mathcal{T}_2^{(m)} \otimes \mathcal{T}_2^{(m)} = 4 \text{diag}[1, 0, 0, 0, 1, 0, 0, 0, 1]. \quad (2.9)$$

Now we assume that for arbitrary natural number n the thesis (2.7) is satisfied. Below we prove that the expression

$$\rho_{2(n+1)} = \frac{1}{2^{2(n+1)}} \left(I^{\otimes 2(n+1)} + (-1)^{n+1} \sum_{i=1}^3 \sigma_i^{\otimes 2(n+1)} \right) \quad (2.10)$$

is satisfied. First, let us recall that by the definition (2.6) the state $\rho_{2(n+1)}$ may be constructed as follows:

$$\rho_{2(n+1)} = \frac{1}{4} \sum_{m=0}^3 U_m^{(2n)} \rho_{2n} U_m^{(2n)} \otimes U_m^{(2)} \rho_2 U_m^{(2)}. \quad (2.11)$$

Second, let us note that arbitrary density matrix ξ describing N spin-1/2 particles may be written as

$$\xi = \frac{1}{2^N} \sum_{m_1, \dots, m_N=0}^3 \lambda_{m_1, \dots, m_N} \sigma_{m_1} \otimes \dots \otimes \sigma_{m_N}. \quad (2.12)$$

Here, the coefficients $\lambda_{m_1, \dots, m_N}$ ($m_1, \dots, m_N=0, \dots, 3$) form a tensor that we shall denote by Λ_N and its part responsible for $m_1, \dots, m_N=1, 2, 3$ by \mathcal{T}_N . Immediate observation is that for states $U_{2n}^{(m)} \rho_{2n} U_{2n}^{(m)}$ ($m=0, \dots, 3$) all coefficients $\lambda_{m_1, \dots, m_{2n}}$ equal zero except the cases where $m_1=m_2=\dots=m_{2n}$. Moreover, it is clear from Eq. (2.7) and by virtue of the equality $\sigma_i \sigma_j \sigma_i = 2\delta_{ij} \sigma_i - \sigma_j$, that tensors $\mathcal{T}_{2n}^{(m)}$ for states $U_{2n}^{(m)} \rho_{2n} U_{2n}^{(m)}$ ($m=0, \dots, 3$) may be written in vector form as

$$\begin{aligned} \mathcal{T}_{2n}^{(0)} &= (-1)^n [1, \dots, 1, \dots, 1], \\ \mathcal{T}_{2n}^{(1)} &= (-1)^n [1, \dots, -1, \dots, -1], \\ \mathcal{T}_{2n}^{(2)} &= (-1)^n [-1, \dots, 1, \dots, -1], \\ \mathcal{T}_{2n}^{(3)} &= (-1)^n [-1, \dots, -1, \dots, 1], \end{aligned} \quad (2.13)$$

with only nonzero elements being explicitly written, i.e., those for $m_1=\dots=m_{2n}$ ($m_1, \dots, m_{2n}=1, 2, 3$).

Treating $\mathcal{T}_{2n}^{(m)}$ ($m=0, \dots, 3$) as vectors from \mathbb{R}^9 and using Eqs. (2.4) and (2.13) one can immediately infer that

$$\sum_{m=0}^3 \mathcal{T}_{2n}^{(m)} = \mathbf{0},$$

$$\sum_{m=0}^3 \mathcal{T}_{2n}^{(m)} \otimes \mathcal{T}_2^{(m)} = 4(-1)^{n+1} [1, \underbrace{\dots}_0, 1, \underbrace{\dots}_0, 1]. \quad (2.14)$$

Here $\mathbf{0}$ denotes a zero vector from \mathbb{R}^{9n} . Finally, substitution of the states $U_{2n}^{(m)} \rho_{2n} U_{2n}^{(m)}$ and the Bell states (2.2) into Eq. (2.11) with the aid of Eqs. (2.13) and (2.14) completes the proof. ■

B. Violation of Bell inequalities

Now, we show that GSSs for arbitrary $n \geq 2$ can violate certain Bell inequalities. This will be done in an analogous way to that presented in [24]. With this aim consider a standard scenario in which the j th party ($j=1, 2, \dots, N$) can choose between two dichotomic observables $\hat{O}_{k_j}^{(j)}$ ($k_j=1, 2$). For our purposes it suffices to consider an N -particle CHSH-type Bell inequality of the form

$$|E_{1, \dots, 1, 1} + E_{1, \dots, 1, 2} + E_{2, \dots, 2, 1} - E_{2, \dots, 2, 2}| \leq 2, \quad (2.15)$$

which may be derived from the more general set of Bell inequalities [27,28] or using the same technique as for the two-particle CHSH Bell inequality [25]. The function E appearing in Eq. (2.15) is the so-called correlation function classically defined as an average of the measurement outputs taken over many runs of experiment:

$$E_{k_1, \dots, k_N} = \left\langle \prod_{j=1}^N O_{k_j}^{(j)} \right\rangle_{\text{av}}. \quad (2.16)$$

In quantum regime the definition is

$$E_{k_1, \dots, k_N}^{QM}(\varrho) = \text{Tr}(\varrho \hat{O}_{k_1}^{(1)} \otimes \dots \otimes \hat{O}_{k_N}^{(N)}), \quad (2.17)$$

where in the case of spin- $\frac{1}{2}$ particles the dichotomic observables are of the form

$$\hat{O}_{k_j}^{(j)} = \hat{n}_{k_j}^{(j)} \cdot \boldsymbol{\sigma} \quad (k_j=1, 2, \quad j=1, 2, \dots, N), \quad (2.18)$$

with $\hat{n}_{k_j}^{(j)}$ denoting vectors from \mathbb{R}^3 , obeying $|\hat{n}_{k_j}^{(j)}|=1$. Here we deal with an even number of particles and therefore we put $N=2n$ ($n=2, 3, \dots$). To achieve violation of the Bell inequalities (2.15) it suffices to choose

$$\begin{aligned} \hat{n}_1^{(j)} &= \hat{x}, \quad \hat{n}_2^{(j)} = \hat{y} \quad (j=1, 2, \dots, 2n-1), \\ \hat{n}_1^{(2n)} &= \frac{1}{\sqrt{2}}(\hat{x} + \hat{y}), \quad \hat{n}_2^{(2n)} = \frac{1}{\sqrt{2}}(\hat{x} - \hat{y}), \end{aligned} \quad (2.19)$$

where \hat{x} and \hat{y} stand for unit vectors directed along, respectively, the OX and OY axes. The above vectors give

$$\begin{aligned} E_{1, \dots, 1, 1}^{QM}(\rho_{2n}) + E_{1, \dots, 1, 2}^{QM}(\rho_{2n}) + E_{2, \dots, 2, 1}^{QM}(\rho_{2n}) \\ - E_{2, \dots, 2, 2}^{QM}(\rho_{2n}) = (-)^n 2\sqrt{2}, \end{aligned} \quad (2.20)$$

which obviously violates the Bell inequality (2.15) for arbitrary $n \geq 2$. Moreover, this violation is maximal which can be easily shown by the Cirel'son bound [29] since for this purpose in each term of (2.20) one can combine all $2n-1$ local operators into one dichotomic operator.

Concluding, we have just shown that any of states (2.6) violates the Bell inequality (2.15) *maximally* in the sense that no other quantum state can violate that in a stronger way. For $n=1$ it is obvious since for this value of n we have one of the Bell states; however for $n \geq 2$ this violation is surprising in the light of the fact that all these states are bound entangled. One could partially resolve that paradox observing that the above inequality has a nonsymmetric structure: the last particle is distinguished, while all the previous ones are treated on the same footing. This however does not mean automatically that it is only bipartite inequality, i.e., that it measures only absence of bipartite hidden local variables model, since all the remaining $2n-1$ observables are *local*.

C. Noisy states

Trying to generalize the above considerations, we investigate some of the properties of the GSS in presence of noise. In other words below we characterize states

$$\varrho_{2n}(p) = (1-p) \frac{I^{\otimes 2n}}{2^{2n}} + p\rho_{2n} \quad (0 \leq p \leq 1), \quad (2.21)$$

where I as previous is identity acting on one-qubit space and bound entangled states ρ_{2n} are defined by Eq. (2.6). Below we show that this family of states has similar separability properties and violate Bell inequality in the same regime with respect to p as two-qubit Werner states [9].

In the first step let us observe that by virtue of Eq. (2.7) we may rewrite Eq. (2.21) as follows:

$$\varrho_{2n}(p) = \frac{1}{2^{2n}} \left(I^{\otimes 2n} + (-1)^n p \sum_{i=1}^3 \sigma_i^{\otimes 2n} \right). \quad (2.22)$$

To investigate separability properties of the noisy GSS (2.21) let us introduce projectors

$$P_k^{(\pm)} = \frac{1}{2} (I \pm \sigma_k) \quad (k = 1, 2, 3) \quad (2.23)$$

as corresponding to eigenvectors of σ_k with eigenvalues ± 1 . Then let us consider two-qubit mixed separable states introduced in [26]:

$$\varrho_k^{(\pm)} = \frac{1}{2} (P_k^{(+)} \otimes P_k^{(\pm)} + P_k^{(-)} \otimes P_k^{(\mp)}). \quad (2.24)$$

Please notice that these states may be easily generalized to arbitrary amount of particles. To this aim let us introduce the following notations:

$$\begin{aligned} \eta_{k,1}^{(\pm)} &\equiv P_k^{(\pm)}, \\ \eta_{k,2}^{(\pm)} &= \frac{1}{2} [\eta_{k,1}^{(+)} \otimes P_k^{(\pm)} + \eta_{k,1}^{(-)} \otimes P_k^{(\mp)}] \equiv \varrho_k^{(\pm)}, \\ \eta_{k,3}^{(\pm)} &= \frac{1}{2} [\eta_{k,2}^{(+)} \otimes P_k^{(\pm)} + \eta_{k,2}^{(-)} \otimes P_k^{(\mp)}], \\ &\vdots \\ \eta_{k,n}^{(\pm)} &= \frac{1}{2} [\eta_{k,n-1}^{(+)} \otimes P_k^{(\pm)} + \eta_{k,n-1}^{(-)} \otimes P_k^{(\mp)}]. \end{aligned} \quad (2.25)$$

From that construction it is obvious that all states $\eta_{k,n}^{(\pm)}$ ($k=1, 2, 3$, $n=2, 3, \dots$) are fully separable. Moreover, taking into account expression (2.23) we may constitute the following observation.

Observation 2. All states $\eta_{k,n}^{(\pm)}$ have the form

$$\eta_{k,n}^{(\pm)} = \frac{1}{2^n} (I^{\otimes n} \pm \sigma_k^{\otimes n}) \quad (k = 1, 2, 3, n = 1, 2, \dots). \quad (2.26)$$

Proof. Since the above observation is rather obvious, we decided to present below proof for $n=2$. Generalization to arbitrary $n > 2$ is straightforward. From the definition (2.25) we infer

$$\eta_{k,2}^{(\pm)} \equiv \varrho_k^{(\pm)} = \frac{1}{2} (P_k^{(+)} \otimes P_k^{(\pm)} + P_k^{(-)} \otimes P_k^{(\mp)}), \quad (2.27)$$

and then application of Eqs. (2.23) to the above yields

$$\begin{aligned} \eta_{k,2}^{(\pm)} &= \frac{1}{8} [(I + \sigma_k) \otimes (I \pm \sigma_k) + (I - \sigma_k) \otimes (I \mp \sigma_k)] \\ &= \frac{1}{2^2} (I^{\otimes 2} \pm \sigma_k^{\otimes 2}). \end{aligned} \quad (2.28)$$

Now we are in a position to finish considerations respecting separability properties of the states (2.21). Since the Werner states $\varrho^W(p)$ and the Smolin states $\varrho^S(p)$ are separable for $p=1/3$ [24], we may conjecture that all GSSs for $n \geq 2$ also possess this property. Indeed, we have the following observation.

Observation 3. For $p=1/3$ states $\varrho_{2n}(1/3)$ are separable and are of the form

$$\varrho_{2n}\left(\frac{1}{3}\right) = \frac{1}{6} \sum_{k=1}^3 \begin{cases} \eta_{k,n}^{(+)} \otimes \eta_{k,n}^{(-)} + \eta_{k,n}^{(-)} \otimes \eta_{k,n}^{(+)} & n = 1, 3, 5, \dots, \\ \eta_{k,n}^{(-)} \otimes \eta_{k,n}^{(-)} + \eta_{k,n}^{(+)} \otimes \eta_{k,n}^{(+)} & n = 2, 4, 6, \dots. \end{cases} \quad (2.29)$$

Proof. The proof is rather technical, so we restrict our consideration to the case of odd number of particles. After application of Eq. (2.26) to Eq. (2.29) we obtain

$$\begin{aligned} \varrho_{2n}\left(\frac{1}{3}\right) &= \frac{1}{6} \frac{1}{2^{2n}} \sum_{k=1}^3 [(I^{\otimes n} + \sigma_k^{\otimes n}) \otimes (I^{\otimes n} - \sigma_k^{\otimes n}) + (I^{\otimes n} - \sigma_k^{\otimes n}) \\ &\quad \otimes (I^{\otimes n} + \sigma_k^{\otimes n})] = \frac{1}{2^{2n}} \left(I^{\otimes 2n} - \frac{1}{3} \sum_{k=1}^3 \sigma_k^{\otimes 2n} \right) \\ &\quad (n = 1, 3, 5, \dots). \end{aligned} \quad (2.30)$$

The same procedure for the even number of particles gives expression with plus before the last term. Therefore, we may rewrite these two relations as

$$\varrho_{2n}\left(\frac{1}{3}\right) = \frac{1}{2^{2n}} \left(I^{\otimes 2n} + (-1)^n \frac{1}{3} \sum_{k=1}^3 \sigma_k^{\otimes 2n} \right), \quad (2.31)$$

which completes the proof. \blacksquare

We remark that using LOCC we may always add some noise and therefore the noisy GSSs become separable for all $p \in [0, 1/3]$. Subsequently, using observables defined by Eq. (2.19), we can see that violation of (2.15) by (2.21) is for $p \in (1/\sqrt{2}, 1]$.

III. APPLICATIONS

A. Communication complexity

Quite recently Brukner *et al.* [21] showed that aside from being one of the most important tools in detection of nonlocality, Bell inequalities constitute criterion of usefulness of

the quantum states in reducing communication complexity. The prove is constructive since for every Bell inequality and for broad class of quantum protocols they propose a multi-party communication complexity problem. Quantum protocols for this problem are more efficient when one uses quantum state violating that inequality.

In [24] we showed that despite being bound entangled, Smolin state may be considered as a useful tool in reducing communication complexity. Moreover, since it is possible to the Smolin state to violate certain Bell inequality maximally, its efficiency is the same as for free entangled states. In the light of the previous section it is clear that the rest of the GSSs are also useful in reducing communication complexity. Note that for the communication complexity problems related to these Bell inequalities the corresponding states work optimally, i.e., there are no other states that can work better.

B. Remote information concentration

Before we consider the GSS in context of remote information concentration we outline the basic ideas of telecloning scheme proposed by Murao *et al.* [30]. This scheme, comprising quantum teleportation and cloning, allow a sender to teleport an unknown one-qubit state to spatially separated receivers. Of course, by virtue of the no-cloning theorem received qubits are no longer perfect clones of teleported one.

Suppose that Alice wishes to teleport the one-qubit state

$$|\phi\rangle = a|0\rangle + b|1\rangle \quad (3.1)$$

to her spatially separated friends B_1, \dots, B_M . With this aim she needs $M-1$ ancilla qubits A_1, \dots, A_{M-1} , which may be also spatially separated. After the whole procedure (for more details see [30]) all of them share the so-called *optimal cloning state*:

$$|\Psi_c\rangle = a|\phi_0\rangle_{AB} + b|\phi_1\rangle_{AB}, \quad (3.2)$$

where

$$\begin{aligned} |\phi_0\rangle_{AB} &= \sum_{j=0}^{M-1} \alpha_j |A_j\rangle_A \otimes |\{0, M-j\}, \{1, j\}\rangle_B, \\ |\phi_1\rangle_{AB} &= \sum_{j=0}^{M-1} \alpha_j |A_{M-1-j}\rangle_A \otimes |\{0, j\}, \{1, M-j\}\rangle_B \\ \alpha_j &= \sqrt{\frac{2(M-j)}{M(M+1)}}, \end{aligned} \quad (3.3)$$

and

$$|A_j\rangle_A = |\{0, M-1-j\}, \{1, j\}\rangle_A. \quad (3.4)$$

The kets $|A_j\rangle_A$ represent M normalized and orthogonal states of ancilla involving $M-1$ qubits. The subscript B refers to M

qubits holding the clones and finally ket $|\{0, M-j\}, \{1, j\}\rangle$ stands for normalized and symmetric state of M qubits with $M-j$ zeros. Let us notice that

$$\begin{aligned} \underbrace{\sigma_1 \otimes \dots \otimes \sigma_1}_{2M-1} |\phi_l\rangle_{AB} &= |\phi_{l \oplus 1}\rangle_{AB}, \\ \underbrace{\sigma_2 \otimes \dots \otimes \sigma_2}_{2M-1} |\phi_l\rangle_{AB} &= (-1)^{M+l+1} i |\phi_{l \oplus 1}\rangle_{AB}, \\ \underbrace{\sigma_3 \otimes \dots \otimes \sigma_3}_{2M-1} |\phi_l\rangle_{AB} &= (-1)^l |\phi_l\rangle_{AC} \quad (l=0,1), \end{aligned} \quad (3.5)$$

with \oplus denoting addition modulo 2.

Murao and Vedral proved [12] that even if local clones are not perfect replicas of teleported qubit, it is still possible to recover information included in optimal cloning state at one site using only LOCC plus bound entangled Smolin state. To show it explicitly they used the unlockable bound entangled Smolin state ρ^S . This result suggests that all GSSs are useful to perform such a task. Indeed, below we show that this is the case.

First, let us assume that the optimal cloning state is distributed among Alice and her friends B_1, \dots, B_M in such a way that the former posses $M-1$ ancilla qubits (generally these qubits may be also spatially separated) and the latter M qubits of clones. Subsequently, they wish to recreate the original qubit $|\phi\rangle$ to Charlie using as a quantum channel the noisy GSS state distributed previously among all actors. In this scenario $2M-1$ qubits of the noisy GSS are provided to Alice and Bobs, while the last M th one is given to Charlie. Now, to complete the goal Alice and B_1, \dots, B_M perform a Bell measurement between their qubits, one from optimal cloning state, and one from the noisy GSS. After that Charlie's qubit arrives at the state $\varrho_{k_1 \dots k_N}(p)$ ($k_1, \dots, k_N = 0, \dots, 3$) given by

$$\begin{aligned} \varrho_{k_1 \dots k_N}(p) &= \frac{1}{p_{k_1 \dots k_N}} \text{Tr}_{A_1 \dots A_{M-1} B_1 \dots B_M} \left(\bigotimes_{i=1}^N P_{k_i}^B \otimes U_{k_1 \dots k_N} |\Psi_c\rangle \right. \\ &\quad \left. \times \langle \Psi_c | \otimes \varrho_{2M}(p) \bigotimes_{i=1}^N P_{k_i}^B \otimes U_{k_1 \dots k_N}^\dagger \right), \end{aligned} \quad (3.6)$$

with probability $p_{k_1 \dots k_N} = \text{Tr}_C(\varrho_{k_1 \dots k_N})$. In the above $N=2M-1$, $P_{k_i}^B$ ($k_i=0, \dots, 3$, $i=1, \dots, N$) are projectors onto the corresponding Bell states (2.2). Finally, $U_{k_1 \dots k_N}$ denotes an operation that is supposed to be performed by Charlie to complete the task. To compute all traces appearing in Eq. (3.6) we shall utilize the same technique as presented in [31] (see also [32]). Therefore it is convenient to take the optimal cloning state $|\Psi_c\rangle$ in the form (2.12). Hence, after substitution of Eq. (2.7) in Eq. (3.6) we have

$$\begin{aligned} \varrho_{k_1 \dots k_N}(p) &= \frac{1}{p_{k_1 \dots k_N}} \frac{1}{2^{2M+N}} \sum_{m_1, \dots, m_N=0}^3 \lambda_{m_1 \dots m_N} \\ &\times \left(\prod_{i=1}^N \text{Tr}[P_{k_i}^B(\sigma_{m_i} \otimes I)] I \right. \\ &+ (-1)^M p \sum_{r=1}^3 \prod_{i=1}^N \text{Tr}[P_{k_i}^B(\sigma_{m_i} \\ &\otimes \sigma_r)] U_{k_1 k_2 \dots k_N} \sigma_r U_{k_1 k_2 \dots k_N}^\dagger \left. \right). \end{aligned} \quad (3.7)$$

Since

$$\text{Tr}[P_a^B(\sigma_b \otimes \sigma_c)] = \begin{cases} 1, & b=c=0, \\ 0, & (b=0, c \neq 0) \vee (b \neq 0, c=0), \\ t_{bc}^{(a)} \delta_{bc}, & b \neq 0, c \neq 0, \end{cases} \quad (3.8)$$

we may rewrite Eq. (3.7) as

$$\begin{aligned} \varrho_{k_1 \dots k_N}(p) &= \frac{1}{p_{k_1 \dots k_N}} \frac{1}{2^{2M+N}} [\lambda_{0..0} I + (-1)^M p U_{k_1 \dots k_N} \\ &\times [\mathcal{T}_2^{(k_1)} \dots \mathcal{T}_2^{(k_N)} \boldsymbol{\lambda}] \cdot \boldsymbol{\sigma} U_{k_1 \dots k_N}^\dagger], \end{aligned} \quad (3.9)$$

with $\boldsymbol{\lambda} = [\lambda_{1, \dots, 1}, \lambda_{2, \dots, 2}, \lambda_{3, \dots, 3}]$. As we shall see below it suffices for Charlie to perform an operation $U_{k_1 \dots k_N} = \sigma_2^{M \oplus 1} \sigma_{k_1} \dots \sigma_{k_N}$ in order to obtain an original qubit. Since we have

$$\sum_{k=0}^3 \sigma_k \dots \sigma_{k_N} [\mathcal{T}_2^{(k_1)} \dots \mathcal{T}_2^{(k_N)} \boldsymbol{\lambda}] \cdot \boldsymbol{\sigma} \sigma_{k_N} \dots \sigma_{k_1} = (-1)^N 4 \boldsymbol{\lambda} \cdot \boldsymbol{\sigma}, \quad (3.10)$$

utilizing Eq. (3.9), we arrive at

$$\begin{aligned} &\sum_{k_1, \dots, k_N=0}^3 p_{k_1 \dots k_N} \varrho_{k_1 \dots k_N}(p) \\ &= \frac{1}{2} [\lambda_{0..0} I + (-1)^{M+1} p \sigma_2^{M \oplus 1} \boldsymbol{\lambda} \cdot \boldsymbol{\sigma} \sigma_2^{M \oplus 1}]. \end{aligned} \quad (3.11)$$

In the last step we need to calculate coefficients $\lambda_{0..0}$ and $\boldsymbol{\lambda}$. Utilizing relations (3.5) we immediately infer that $\lambda_{0..0} = 1$ and $\boldsymbol{\lambda} = [2 \text{Re}(ab^*), 2(-1)^M \text{Im}(ab^*), |a|^2 - |b|^2]$ and therefore after some elementary operations

$$\sum_{k_1, \dots, k_N=0}^3 p_{k_1 \dots k_N} \varrho_{k_1 \dots k_N}(p) = p |\phi\rangle \langle \phi| + (1-p) \frac{I}{2}. \quad (3.12)$$

For $M=2$ and $p=1$ the above protocol reproduces the result obtained previously by Murao and Vedral [12].

C. Quantum secret sharing

Here we shall also prove that GSSs are useful for quantum secret sharing [33]. For original Smolin states this has

been pointed out in [24]. Note that this was the first example of secret sharing with the help of bound entangled states. A simple generalization of that fact to GSSs is possible. As in [24] the scenario here will be quite similar to that of pure states considered in [34]. Let us take the GSS state of $2n$ parties and let us denote them for a moment by A_1, \dots, A_{2n} . Let A_1 measure an arbitrary Pauli matrix, say σ_1 . It happens that the (counted in bits) result $r_1 \in \{0, 1\}$ of this measurement can represent a quantum secret bit that is shared by all other parties A_2, \dots, A_{2n} . Indeed, if all the other parties measure the same observable and get the results r_i then they satisfy:

$$\bigoplus_{i=1}^{2n} r_i = (n)_{\text{mod } 2} \quad (3.13)$$

(\oplus means here addition modulo 2). This is an immediate consequence of the fact that $\text{Tr}(\sigma_1^{\otimes 2n} \rho_{2n}) = (-1)^n$ which means that (if for a moment we count the results in values ± 1 one rather than in bits) if n is even, only even numbers of results equal to -1 can occur and whenever n takes an odd value, only odd numbers of negative results may be obtained. Here ρ_{2n} denotes a $2n$ -partite GSS defined by Eq. (2.6). From the above relation we see that if all the other parties A_2, \dots, A_{2n} meet and compare their results they can reveal the value of the secret bit r_1 . On the other and any purification of ρ_{2n} is of the form

$$\frac{1}{\sqrt{4^n}} \sum_{i=1}^{4^n} |\Psi_{A_1 \dots A_{2n}}^{(i)}\rangle |\phi_E^{(i)}\rangle \quad (3.14)$$

where each of the *orthonormal* states $|\Psi_{A_1 \dots A_{2n}}^{(i)}\rangle$ ($i=1, \dots, 4^n$) is the eigenstate of the $2n$ -partite generalized Smolin state. It is relatively easy to see that (3.14) means that, if after measurement of any binary observable, say σ_1 , on qubit A_1 we trace over all the other qubits, then the state of Eve does not depend on the result of the measurement r_i , i.e., Eve has no correlations with the qubit A_1 so she can get no knowledge about the secret bit that comes out as a result of measurement on that qubit. Note that because of the permutational symmetry of the Smolin states all the above reasoning applies to any other qubit A_i ($i=2, \dots, 2n$).

IV. NETWORKS

In the light of all what was said previously it seems the generalized Smolin states to be very promising in practical use. On the other hand there has not been devoted too much attention to problem of generating the bound entangled states experimentally [35]. Therefore below we present simple examples of networks generating GSSs. To this aim we need to make the following observation.

Observation 4. Noisy GSSs $\varrho_{2n}(p)$ obey the recursive formula

$$\varrho_{2(n+1)}(p) = \frac{1}{4} \sum_{m=0}^3 U_m^{(2n)} \varrho_{2n}(p) U_m^{(2n)} \otimes U_m^{(2)} \rho_2 U_m^{(2)}. \quad (4.1)$$

Proof. It suffice to substitute Eq. (2.21) and the first of Eqs. (2.6) in Eq. (4.1) and to utilize Eq. (2.1). ■

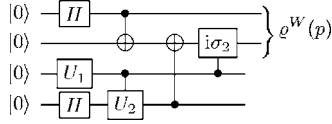


FIG. 1. Network generating the Werner state.

As a matter of fact substitution of $n=2$ in Eq. (2.21) leads to the well-known Werner state $\rho^W(p) = (1-p)\frac{1}{4}I \otimes I + p\rho_2$. Thus it is of particular interest to show the network generating this state. Such a network is presented in Fig. 1.

The unitary operations U_1 and U_2 appearing in Fig. 1 are of the form

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{1-p} & \sqrt{1+p} \\ \sqrt{1+p} & -\sqrt{1-p} \end{pmatrix}, \quad (4.2)$$

$$U_2 = \frac{1}{2\sqrt{1+p}} \begin{pmatrix} \sqrt{1+3p} - \sqrt{1-p} & \sqrt{1+3p} + \sqrt{1-p} \\ \sqrt{1+3p} + \sqrt{1-p} & \sqrt{1-p} - \sqrt{1+3p} \end{pmatrix}. \quad (4.3)$$

Moreover, H denotes the standard Hadamard gate and is given by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (4.4)$$

We shall denote the network presented on Fig. 1 by a black box with two outputs (see Fig. 2). Then, using Observation 4, it is easy to verify that the noisy Smolin states may be created by the network presented in Fig. 3.

It turns out that this network may be recursively generalized to arbitrary even number of particles. Indeed, using similar notation as for the noisy Werner states (see Fig. 2), we may denote the network generating $\rho_{2n}(p)$ by the black box as in Fig. 4. Hence, we may design the network for $\rho_{2(n+1)}(p)$ as presented in Fig. 5.

V. UNLOCKING QUANTUM ENTANGLEMENT WITH SMOLIN STATES

There is an interesting effect of locking quantum entanglement [36] which was inspired by previous result on locking classical correlations [37]. Here we shall show that Smolin states allow to unlock quantum entanglement that was deliberately locked by optimal cloning of locking qubit and distributing clones between many parties.

A. Undoing perfect locking

Consider the following initial state qubits:

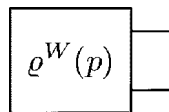


FIG. 2. Brief description of network generating the Werner state.

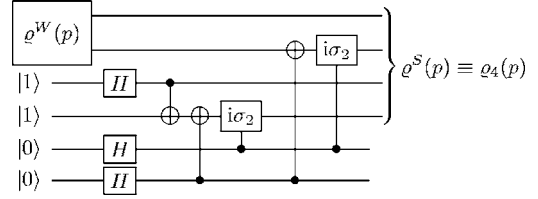


FIG. 3. Network generating the noisy Smolin states.

$$\Omega = \rho_{G_1, G_2, \dots, G_{2M}}^S \otimes (P_0^{\otimes 2M-2})_{A_1, \dots, A_{M-1}, B_1, \dots, B_{M-1}} \otimes \sigma_{C'D}^d, \quad (5.1)$$

where we have initially four parties, Alice, $M-1$ Bob, Charlie (possessing the $C'C$ system) and David, to whom the system D belongs. Here, P_0 denotes a projector onto $|0\rangle$. Suppose that a given entanglement measure E that estimates entanglement between Charlie and David is lockable on the $\sigma_{C'D}^d$ state and that C' represents the locking qubit, i.e., such that

$$E(\sigma_{C'D}^d) - E(\sigma_{CD}^d) \xrightarrow{d \rightarrow \infty} \infty. \quad (5.2)$$

In particular, the state $\sigma_{C'D}^d \in \mathbb{C}^{d+2} \otimes \mathbb{C}^{d+2}$ may be of the form (see [36])

$$\sigma_{C'D} = \frac{1}{2} \begin{bmatrix} \sigma & 0 & 0 & (1/d)U^T \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ (1/d)U^* & 0 & 0 & \sigma \end{bmatrix}, \quad (5.3)$$

where $U = \sum_{i,j=0}^{d-1} u_{ij} |ii\rangle\langle jj|$, $\sigma = (1/d) \sum_{i=0}^{d-1} |ii\rangle\langle ii|$, u_{ij} are elements of some unitary matrix, and the asterisk denotes complex conjugation. Suppose now that some external party performs nonlocal operation of locking of entanglement measure in two steps: (i) cloning the C' qubit according to the prescription between Alice and Bob; this produces state of $2M-1$ qubits $A_1, \dots, A_{M-1}, B_1, \dots, B_{M-1}, C'$ of the form (3.2); (ii) swapping the qubit C' with that of the G_M system; this completely depolarizes the qubit C' . Evidently after that operation the entanglement between Charlie and David is locked since it is in the final state $\sigma_{C'}^{dep} \otimes \sigma_{CD}^d$, where $\sigma_{C'}^{dep} = I/2$. This is just a locking effect we assumed [36]: (5.2) implies an arbitrary high loss of E because for any entanglement measure $E(\sigma_{CD}^d) = E(\sigma_{C'}^{dep} \otimes \sigma_{CD}^d)$.

Now it is immediate to see that Alice and Bob can recover the system C' in its original form on the Charlie site with the help of quantum-information concentration. Because of the linearity of the transformation this is equivalent to reconstruction of the original state $\sigma_{C'D}$ and hence unlocking the entanglement between Charlie and David.

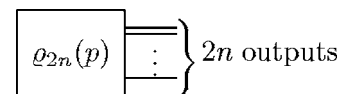


FIG. 4. Brief description of the network generating $\rho_{2n}(p)$.

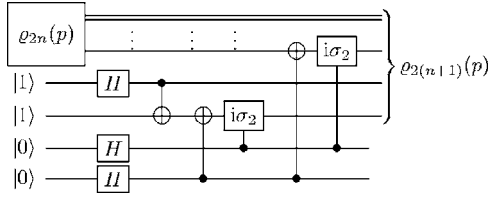


FIG. 5. Networks generating the GSS states.

B. The case of imperfect locking

Consider now the slightly modified initial state

$$\Omega_u = \varrho_{G_1, G_2, \dots, G_{2M}}^S \otimes (P_0^{\otimes 2M})_{A_1, \dots, A_{M-1}, B_1, \dots, B_{M-1}} \quad (5.4)$$

$$\otimes (P_0)_{C''} \otimes \sigma_{C'D}^d$$

again with $\sigma_{C'D}^d$ satisfying the condition (5.2). Suppose that here the external party performs the following global transformation (i) cloning the qubit C' as in the previous subsection (ii) swapping qubit G_M with the one C'' . Here Charlie has two qubits $C''C'$ instead of the one C' , but entanglement of the state shared by Charlie and David is the same as before since the C'' qubit is just added locally in pure state. It can be seen that the locking qubit C' is partially depolarized, i.e., the total state between Charlie and David $\sigma_{C''C'D}$ is turned into a new one:

$$\tilde{\sigma}_{C''C'D} \equiv \sigma_{C''}^{dep} \otimes \sigma_{C'D}^{\epsilon_M, d} = \sigma_{C''}^{dep} \otimes [\epsilon_M \sigma_{C'D}^d + (1 - \epsilon_M) \sigma_{C'}^{dep} \otimes \sigma_{CD}^d], \quad (5.5)$$

with $\sigma_{C'}^{dep}$ being defined as previously and $\epsilon_M = (1/3)(1 + 2/M)$ since we apply an optimal cloning machine (see [39]). Now consider the $\sigma_{C'D}$ to be one of two lockable states: either the state coming from the *flower state* or the one that leads to locking of logarithmic negativity [36]. In both cases σ_{CD}^d is just separable, i.e., $E(\sigma_{CD}^d) = 0$ while before depolarization $E(\sigma_{C'D}^d) \rightarrow \infty$ whenever $d \rightarrow \infty$. Let us stress that the measures considered there in place of E (entanglement cost or logarithmic negativity) are both *convex*. Now for any asymptotically continuous measure E measuring entanglement (or correlation) between $C'C$ and D one has

$$\begin{aligned} E(\sigma_{C''C'D}) - E(\tilde{\sigma}_{C''C'D}) &= E(\sigma_{C'D}^d) - E(\sigma_{C''C'D}^{\epsilon_M, d}) \geq E(\sigma_{C'D}^d) \\ &\quad - (1 - \epsilon_M)E(\sigma_{C'}^{dep} \otimes \sigma_{CD}^d) - \epsilon_M E(\sigma_{C'D}^d) \\ &= E(\sigma_{C'D}^d) - (1 - \epsilon_M)E(\sigma_{CD}^d) - \epsilon_M E(\sigma_{C'D}^d) \\ &= (1 - \epsilon_M)E(\sigma_{C'D}^d) \\ &= \frac{2}{3} \left(1 - \frac{1}{M}\right) E(\sigma_{C'D}^d) \xrightarrow{d \rightarrow \infty} \infty \end{aligned} \quad (5.6)$$

for any $M \geq 2$. We use here in particular the convexity of the considered measure E .

Thus we see that the operation performed by an external party locks either of the two measures. Now if we remotely concentrate the original qubit C' on the Charlie C'' site and finally Charlie swaps it with the qubit C' then the most important part of the state shared by Charlie and David, i.e., the state $\sigma_{C'D}^d$, is recovered, which completes the process of unlocking the measure E . Note that here it is important that because of the linearity of the concentration process the state $\sigma_{C'D}^d$ is product with qubit C'' as it was before the initial step. Otherwise the procedure of unlocking could fail because of possible locking with the qubit C'' .

Finally let us consider the analogous effect of locking of classical information. It is easy to see that the first version of the above protocol can be immediately extended to that case. Instead of entanglement measure one should use the measure I_c introduced in [37] while in place of $\sigma_{C'D}^d$ one should put the pure whole state from [37]. Note that the second of the above versions involving partially depolarized qubits does not generalize automatically since the quantity I_c measuring optimal classical bipartite correlations is not convex.

VI. DISCUSSION

Let us consider some of the properties of generalized Smolin states. It is interesting to understand why maximal Bell violation does not imply quantum security in this case. The first intuition would be that because there are some correlations that (i) are strictly nonlocal (since all the measurements in Bell measurement are performed locally) and (ii) are not accessible to Eve (since Bell inequalities are violated), one should expect quantum security. On the other hand, one could argue that any violation revealed here singles out one particle versus all the remaining ones taken together. Thus, one may say there are doubts whether the inequalities have any multipartite character. However, the remaining parties still perform measurements *locally*, which means that the correlations are stronger than just if they were interpreted in terms of entanglement of a single particle versus all the other parties taken together. On the other hand we have an obvious argument against security since the states are biseparable [separable against any $(2) - (2n - 2)$ particle cut] which means that no security can be distilled even if some parties can communicate in a quantum manner. Most probably the reason is that the present states, despite violating Bell inequalities, do not have any set of axes that provide perfect correlations between all the parties. Thus, in a sense, the quantum correlations even if nonlocal are completely useless for establishing correlated data.

Such a set of axes with corresponding maximally correlated probabilities is possessed by a Greenberger-Horne-Zeilinger state, the Hilbert-Schmidt representation of which has nonvanishing coefficients not only at $\sigma_i^{\otimes 2n}$ ($i = 1, 2, 3$) operators (as GSSs have) but also at all permutations of operators $\sigma_3^{\otimes 2k} \otimes I^{\otimes 2(n-k)}$. This easily allows one to design an Ekert scheme [4] with any of observers choosing randomly one of the following four axes: \hat{x} , \hat{y} , $(1/\sqrt{2})(\hat{x} + \hat{y})$, $(1/\sqrt{2}) \times (\hat{x} - \hat{y})$. This is not the case in for a GSSs where only few correlation terms survive in the Hilbert-Schmidt representation.

In the presence of recent important results on security in postquantum theories [38], following the above discussion it is reasonable to conjecture that any physical system, even in postquantum theory, that maximally violate Bell inequalities leads to cryptographic security if only has one pair of axes with maximal correlations. It would be also interesting to consider the cases when the presence of maximal correlations is accompanied by nonmaximal Bell inequality violation.

Let us pass to another interesting issue—remote concentration of quantum information. We have shown that generalized Smolin states can serve as a resource to concentrate quantum information delocalized in the process of cloning. We pointed out that, because of linearity of the process, the states allow one to unlock entanglement measures as well as classical correlations measured with the help of the quantity defined in [37].

Finally it is interesting to note that the states allow for secret sharing. Although they are highly mixed they share this property with multipartite pure states considered in [34].

In the present paper we have performed construction of generalized Smolin states with the help of the Hilbert-Schmidt formalism. We have also shown that they can be

useful for various quantum tasks. It is very interesting to what extent that type of state can serve as a tool in quantum computing processes. A natural application would be remote quantum-information concentration, but it requires an explicitly nonlocal resource (delocalized information itself). It is interesting to ask what is a minimal additional resource that would make states of GSSs type useful for quantum computing, but this goes beyond the scope of the present paper [40,41].

After completing the first version of this work [e-print quant-ph/0411142], we became aware of the work of Bandyopadhyay *et al.* [42], where generalized Smolin states were introduced in explicitly correlated (Einstein-Podolsky-Rosen-like) form and their unlockability property was discussed.

ACKNOWLEDGMENTS

R.A. thanks Maciej Demianowicz for discussions. This work is supported by the European Union (project RESQ), the Polish Ministry of Scientific Research, Information Technology (Grant No. PB2-Min-008/P03/03), and the Fujitsu Laboratories (Europe).

-
- [1] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
 - [2] E. Schrödinger, *Naturwiss.* **23**, 807 (1935).
 - [3] *Introduction in Quantum Information and Computation*, edited by H.-K. Lo, S. Popescu, and T. Spiller (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, A. K. Ekert, and A. Zeilinger (Springer, New York, 2000); M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000); G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Röttler, H. Weinfurter, R. F. Werner, and A. Zeilinger, *Quantum Information: An Introduction To Basic Theoretical Concepts and Experiments*, Springer Tracts in Modern Physics Vol. 173 (Springer, Berlin, 2001).
 - [4] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [5] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
 - [6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
 - [7] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser, (IEEE Computer Society, Los Alamitos, California 1994).
 - [8] J. S. Bell, *Physics* (Long Island City, N.Y.) **1**, 195 (1964).
 - [9] R. F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
 - [10] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **80**, 5239 (1998).
 - [11] P. Horodecki, M. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **82**, 1056 (1999).
 - [12] M. Murao and V. Vedral, *Phys. Rev. Lett.* **86**, 352 (2001).
 - [13] K. G. H. Vollbrecht and M. M. Wolf, *Phys. Rev. Lett.* **88**, 247901 (2002); P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *ibid.* **90**, 107901 (2003); W. Dür and J. I. Cirac, *Phys. Rev. A* **62**, 022302 (2000).
 - [14] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Phys. Rev. Lett.* **94**, 160502 (2005).
 - [15] W. Dür, J. I. Cirac, and P. Horodecki, *Phys. Rev. Lett.* **93**, 020503 (2004).
 - [16] S. Ishizaka, *Phys. Rev. Lett.* **93**, 190501 (2004).
 - [17] W. Dür, *Phys. Rev. Lett.* **87**, 230402 (2001).
 - [18] A. Acin, *Phys. Rev. Lett.* **88**, 027901 (2002); A. Acin, V. Scarani, and M. M. Wolf, *J. Phys. A* **36**, L21 (2003); *Phys. Rev. A* **66**, 042323 (2002).
 - [19] D. Kaszlikowski, L. C. Kwek, J. Chen, and C. H. Oh, *Phys. Rev. A* **66**, 052309 (2002).
 - [20] A. Sen (De), U. Sen, and M. Żukowski, *Phys. Rev. A* **66**, 062318 (2002).
 - [21] C. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, *Phys. Rev. Lett.* **92**, 127901 (2004).
 - [22] C. Brukner, M. Żukowski, and A. Zeilinger, *Phys. Rev. Lett.* **89**, 197901 (2002).
 - [23] J. A. Smolin, *Phys. Rev. A* **63**, 032306 (2001).
 - [24] R. Augusiak and P. Horodecki, e-print quant-ph/0405187.
 - [25] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969); J. F. Clauser and M. A. Horne, *Phys. Rev. D* **10**, 526 (1974).
 - [26] R. Horodecki and M. Horodecki, *Phys. Rev. A* **54**, 1838 (1996).
 - [27] R. F. Werner and M. M. Wolf, *Phys. Rev. A* **64**, 032112 (2001).
 - [28] M. Żukowski and C. Brukner, *Phys. Rev. Lett.* **88**, 210401 (2002).

- [29] B. S. Cirel'son, *Lett. Math. Phys.* **4**, 557 (1980).
- [30] M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral, *Phys. Rev. A* **59**, 156 (1999).
- [31] R. Horodecki, M. Horodecki, and P. Horodecki, *Phys. Lett. A* **222**, 21 (1996).
- [32] N. Linden and S. Popescu, *Phys. Rev. A* **59**, 137 (1999).
- [33] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
- [34] A. Sen (De), U. Sen, and M. Żukowski, *Phys. Rev. A* **68**, 032309 (2003).
- [35] P. Hyllus, C. Moura Alves, D. Bruss, and C. Macchiavello, *Phys. Rev. A* **70**, 032316 (2004).
- [36] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Phys. Rev. Lett.* **94**, 200501 (2005).
- [37] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, *Phys. Rev. Lett.* **92**, 067902 (2004).
- [38] J. Barrett, L. Hardy, and A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005).
- [39] R. F. Werner, *Phys. Rev. A* **58**, 1827 (1998).
- [40] M. Christandl and A. Winter, *IEEE Trans. Inf. Theory*, **51**, 3159 (2005).
- [41] M. Horodecki, *Quantum Inf. Comput.* **1**, 3 (2001).
- [42] S. Bandyopadhyay, I. Chattopadhyay, V. P. Roychowdhury, and D. Sarkar, *Phys. Rev. A* **71**, 062317 (2005); see also e-print quant-ph/0411082.