PHYSICAL REVIEW A **91**, 012335 (2015)

Construction and properties of a class of private states in arbitrary dimensions

Adam Rutkowski,[*] Michał Studziński, Piotr Ćwikliński, and Michał Horodecki
Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
and National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland

(Received 1 October 2014; revised manuscript received 28 November 2014; published 27 January 2015)

We present a construction of quantum states in dimension d that has at least 1 dit of ideal key, called private dits (pdits), which covers most of the known examples of private bits (pbits) $d = 2$. We examine properties of this class of states, focusing mostly on its distance to the set of separable states $\mathcal{S}$, showing that for a fixed dimension of key part d_k, the distance increases with d_s. We provide explicit examples of positive partial transpose states (in d dimensions) which are nearly as far from separable ones as possible. Precisely, the distance from the set of $\mathcal{S}$ is $2-\epsilon$, where d scales with ϵ as $d \propto 1/\epsilon^3$, as opposed to $d \propto 2^{[\log(4/\epsilon)]^2}$ obtained by Badziąg *et al.* [Phys. Rev. A **90**, 012301 (2014)]. We do not use boosting (taking many copies of pdits to boost the distance) as in the Badziąg *et al.* paper.

DOI: 10.1103/PhysRevA.91.012335 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum cryptography allows perfect secret sharing among honest parties and is currently the most successful and commercial branch of quantum information science. In 2007, quantum cryptography was used to secure part of the vote counting in a referendum in the canton of Geneva and, in 2010, in collaboration with the University of Kwazulu-Natal, South Africa, to encrypt a connection in the Durban stadium during the football World Cup. But what is the source of its power? Briefly speaking, the fundamental property which guarantees security of the quantum cryptography is that if one does not know the state of a qubit, then with a high probability one disturbs the state while trying to get to know it.

This implies that there is a clear relation between quantum security and correlations in the form of quantum entanglement. If such correlations are maximal, between two qubits, they can be changed via measurement into one bit of a secret key (also called "classical" key). The first protocols of quantum key distribution were based only on pure entangled states [1–3] and were security proof [4], which led to natural expectations that pure entangled quantum states are the only source of quantum security [5,6]. However, we know that entanglement can be manifested not only in a pure form, but also in a mixed one. What is more, there are some mixed entangled quantum states from which no pure entangled states can be obtained using local operations and classical communication (LOCC), called bound entangled states [7,8]. It was hoped that bound states would be useless for quantum cryptography—no key would be distillable from the classical distribution. But, quite surprising at that time was the discovery of private bound entangled states, which has tempered those hopes and demonstrated a clear distinction between secrecy and bound entanglement [9].

The key ingredient in showing that distinction was the notion of private states (introduced in [9]), quantum states that contain a directly accessible, ideally secure classical key, and private bits (pbit) or, more generally, a private dit (pdit), which is a delocalized maximally entangled state that still retains some entanglement monogamy result. A quantum pdit is composed from a $d \otimes d$ AB part called the "key," and a $A'B'$ part called the "shield," shared between Alice (subsystems AA') and Bob (subsystems BB') in such a way that the results of the local von Neumann measurements on the key part in a particular basis are completely statistically uncorrelated from the results of any measurement of an eavesdropper Eve on her subsystem E, which is a part of the purification $|\Psi\rangle_{ABA'B'E}$ of the pdit state $\rho_{ABA'B'}$. Pdits (especially pbits) have been studied extensively for some time [10–15].

Quite recently, an important discovery has been made in studies between security and correlations. In [16], a clean classical analog of bound entanglement and private bound entanglement has been provided, where the authors have constructed private bound entangled states based on unambiguous classical probability distribution to a quantum state that is not based on a "standard" key or shield scheme, opening a new direction in the study of private states.

Our paper is organized in the following way. In Sec. II, we present a general construction of an alternate class of pdits and show that for specific choices of parameters, we can reduce this class to the cases previously known in the literature. In Sec. III, we investigate properties of this set of pdits. Namely, we calculate the trace distance of arbitrary pdits from this class from the pdit in maximally entangled form (Lemma 1). We also show that for the specific subclass, this distance scales inversely with the dimension of the shield part d_s (Lemma 2). At the end of this section, we give the lower bound for the trace distance from the set of separable states $\mathcal{S}$ and our subclass (Lemma 3), which gives a better estimation than the previous one [17]. Most importantly, we are able to show that for a particular subclass of pdits, we do not need to take many copies of pdits to boost the distance from the set of separable set $\mathcal{S}$ (like in [17]) using our construction. We also show that our family of states approximates the set of separable states obtaining the distance equal to $2-\epsilon$ and improving the scaling of ϵ with the distance. Additionally, we present two appendices in which we describe a special method which allows us to prove one of the crucial statements in our paper, i.e., Lemma 2 (see Appendix A). In Appendix B, we recall the special construction of the set of operators which is one of the possible realizations of operators with desired spectra needed in Sec. III.

---

[*] fizar@ug.edu.pl

II. GENERAL CONSTRUCTION OF PDITS

As we have mentioned in Sec. I, we want to construct a four-partite state $\rho_{ABA'B'}$ (pdit) which has a positive partial transpose (PPT) property and is close to pdits in the so-called maximally entangled form (see Sec. III). Let us consider the following state:

$$\rho_{ABA'B'} = \sum_{l=0}^{d} \omega_l \in \mathcal{B}\big(\mathcal{H}_{d_k} \otimes \mathcal{H}_{d_k} \otimes \mathcal{H}_{d_s} \otimes \mathcal{H}_{d_s}\big), \qquad (1)$$

where $\mathcal{B}(\mathcal{H})$ is the algebra of all bounded linear operators on Hilbert space $\mathcal{H}$, $d = \frac{1}{2}d_k(d_k-1)$, and by d_k we denote the dimension of the key part acting on AB and by d_s the dimension of the shield part acting on $A'B'$. Now we describe each of the components from Eq. (1). First of all, we define the term ω_0 as

$$\omega_0 = \sum_{i,j=0}^{d_k-1} |i\rangle\langle j| \otimes |i\rangle\langle j| \otimes a_{ij}^{(0,0)}, \qquad (2)$$

where every $a_{ij}^{(0,0)} \in \mathcal{B}(\mathcal{H}_{d_s} \otimes \mathcal{H}_{d_s})$. From now on, every matrix of the form (2) we will call the matrix in the maximally entangled form. The rest of the elements ω_l, for $1 \leqslant l \leqslant \frac{1}{2}d_k(d_k-1)$ from Eq. (1), are given by the following formula:

$$\begin{aligned}\omega_l = {} & |i\rangle\langle i| \otimes |j\rangle\langle j| \otimes a_{00}^{(i,j)} + |i\rangle\langle j| \otimes |j\rangle\langle i| \otimes a_{01}^{(i,j)} \\ & + |j\rangle\langle i| \otimes |i\rangle\langle j| \otimes a_{10}^{(i,j)} + |j\rangle\langle j| \otimes |i\rangle\langle i| \otimes a_{11}^{(i,j)},\end{aligned} \qquad (3)$$

where $i,j = 1,\dots,d_k-1$ and $i < j$. In the above, we also implicitly assume a bijection function between indices l and i,j.

Let us introduce the following notation:

$$A^{(i,j)} = \begin{pmatrix} a_{00}^{(i,j)} & a_{01}^{(i,j)} \\ a_{10}^{(i,j)} & a_{11}^{(i,j)} \end{pmatrix}, \qquad (4)$$

where $i,j = 0,\dots,d_k-1$ for $i < j$. Separately, for the term $A^{(0,0)}$, we have

$$A^{(0,0)} = \begin{pmatrix} a_{00}^{(0,0)} & \cdots & a_{0,d_k-1}^{(0,0)} \\ \vdots & \ddots & \vdots \\ a_{d_k-1,0}^{(0,0)} & \cdots & a_{d_k-1,d_k-1}^{(0,0)} \end{pmatrix}. \qquad (5)$$

Then, there is an explicit connection between positivity of the state $\rho_{ABA'B'}$ and each submatrix $A^{(i,j)}$ and positivity of $\rho_{ABA'B'}^{T_{A'}T_{B'}}$ and each block $A^{(i,j)}$ after partial transposition on the system B'. This can be summarized as follows:

Observation 1. We have the following relations between positivity of the state $\rho_{ABA'B'}$ before and after partial transposition and positivity properties of every block $A^{(i,j)}$:

(i) Positivity of the state $\rho_{ABA'B'}$,

$$\rho_{ABA'B'} \geqslant 0 \Leftrightarrow A^{(i,j)} \geqslant 0, \qquad (6)$$

(ii) Positivity of the state $\rho_{ABA'B'}$ with respect to partial transposition in the cut $AB : A'B'$,

$$(\mathbb{1}_A \otimes T_B \otimes \mathbb{1}_{A'} \otimes T_{B'})\rho_{ABA'B'} \geqslant 0 \Leftrightarrow \widetilde{A}^{(i,j)} \geqslant 0, \qquad (7)$$

where $\widetilde{A}^{(i,j)}$ is given by

$$\widetilde{A}^{(i,j)} = \begin{pmatrix} \widetilde{a}_{00}^{(i,j)} & \widetilde{a}_{ij}^{(0,0)} \\ \widetilde{a}_{ji}^{(0,0)} & \widetilde{a}_{11}^{(i,j)} \end{pmatrix}, \quad i,j = 0,\dots,d_k-1 \text{ with } i < j,$$

and

$$\widetilde{A}_{ij}^{(0,0)} = \begin{cases} \widetilde{a}_{ij}^{(0,0)}, & i = j \\ \widetilde{a}_{01}^{(i,j)}, & i < j \\ \widetilde{a}_{10}^{(i,j)}, & i > j \end{cases}, \quad i,j = 0,\dots,d_k-1.$$

In the above, we have $\widetilde{a}_{00}^{(i,j)} = (\mathbb{1}_B \otimes T_{B'})a_{00}{}^{(i,j)}$, and so on.

Proof. The proof of the above statement is based on straightforward observation. Namely, one can notice that every component of the state from Eq. (1) is defined on different subspaces which are orthogonal to each other, thus every block can be treated separately—we can consider positivity and PPT conditions on each of the components independently. This fact implies all claimed properties of states $\rho_{ABA'B'}$ from (1). ■

At the end of this section, we show for which choices of matrices ω_0 and ω_l we can reduce our general construction, given by formulas (1)–(3), to the previously known cases. First let us write general matrix expressions for state $\rho_{ABA'B'}$ from the formula (1) when the dimension of the key part is $d_k = 2,3$. Namely, for $d_k = 2$, we have

$$\rho_{ABA'B'} = \omega_0 + \omega_1, \qquad (8)$$

where

$$\omega_0 = \left(\begin{array}{cc|cc} a_{00}^{(0,0)} & \cdot & \cdot & a_{01}^{(0,0)} \\ \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot \\ a_{10}^{(0,0)} & \cdot & \cdot & a_{11}^{(0,0)} \end{array}\right),$$

$$\omega_1 = \left(\begin{array}{cc|cc} \cdot & \cdot & \cdot & \cdot \\ \cdot & a_{00}^{(0,1)} & a_{01}^{(0,1)} & \cdot \\ \hline \cdot & a_{10}^{(0,1)} & a_{11}^{(0,1)} & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{array}\right). \qquad (9)$$

For $d_k = 3$, state $\rho_{ABA'B'}$ is represented as

$$\rho_{ABA'B'} = \omega_0 + \omega_1 + \omega_2 + \omega_3 \in \mathcal{B}(\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s}), \qquad (10)$$

where

$$\rho_0 = \left(\begin{array}{ccc|ccc|ccc} a_{00}^{(0,0)} & \cdot & \cdot & \cdot & a_{01}^{(0,0)} & \cdot & \cdot & \cdot & a_{02}^{(0,0)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{10}^{(0,0)} & \cdot & \cdot & \cdot & a_{11}^{(0,0)} & \cdot & \cdot & \cdot & a_{12}^{(0,0)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{20}^{(0,0)} & \cdot & \cdot & \cdot & a_{21}^{(0,0)} & \cdot & \cdot & \cdot & a_{22}^{(0,0)} \end{array}\right),$$

$$\rho_1 = \left(\begin{array}{ccc|ccc|ccc} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & a_{00}^{(0,1)} & \cdot & a_{01}^{(0,1)} & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & a_{10}^{(0,1)} & \cdot & a_{11}^{(0,1)} & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}\right),$$

$$\rho_2 = \left(\begin{array}{ccc|ccc|ccc} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & a_{00}^{(0,2)} & \cdot & \cdot & \cdot & a_{01}^{(0,2)} & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & a_{10}^{(0,2)} & \cdot & \cdot & \cdot & a_{11}^{(0,2)} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}\right),$$

$$\rho_3 = \left(\begin{array}{ccc|ccc|ccc} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & a_{00}^{(1,2)} & \cdot & a_{01}^{(1,2)} & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & a_{10}^{(1,2)} & \cdot & a_{11}^{(1,2)} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}\right). \tag{11}$$

From the above examples, we see that operators ω_k are supported on orthogonal subspaces. Now, we are ready to present five examples of private states which belong to our class:

(i) Suppose that $\gamma^V \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s})$ such that

$$\gamma^V = \frac{1}{2}\begin{pmatrix} \mathbb{1}/d_s^2 & \cdot & \cdot & V/d_s^2 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ V/d_s^2 & \cdot & \cdot & \mathbb{1}/d_s^2 \end{pmatrix}, \tag{12}$$

where $V = \sum_{i=0}^{d_s-1} |ij\rangle\langle ji|$ is known as the swap operator, $\mathbb{1}$ is the identity matrix of dimension $d_s^2 \times d_s^2$, and by dots we denote matrices of dimension $d_s^2 \times d_s^2$ filled with zeros [18].

(ii) Suppose that $\rho_{\text{flower}} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s})$ such that

$$\rho_{\text{flower}} = \frac{1}{2}\begin{pmatrix} \sigma & \cdot & \cdot & U^T/d_s \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ U^*/d_s & \cdot & \cdot & \sigma \end{pmatrix}, \tag{13}$$

where $\sigma = (1/d_s)\sum_{i=0}^{d_s-1} |ii\rangle\langle ii|$ is the classical maximally correlated state and U is an embedding of unitary transformation $W = \sum_{i,j=0}^{d_s-1} w_{ij}|i\rangle\langle j|$ in the form $U = \sum_{i,j=0}^{d_s-1} w_{ij}|ii\rangle\langle jj|$. The state (13) is known as the flower state [13].

(iii) Suppose that $\rho \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{ld_s} \otimes \mathbb{C}^{ld_s})$ such that

$$\rho_{ABA'B'} = \frac{1}{2}\begin{pmatrix} p(\tau_0+\tau_1) & \cdot & \cdot & p(\tau_1-\tau_0) \\ \cdot & (1-2p)\tau_0 & \cdot & \cdot \\ \cdot & \cdot & (1-2p)\tau_0 & \cdot \\ p(\tau_1-\tau_0) & \cdot & \cdot & p(\tau_0+\tau_1) \end{pmatrix}. \tag{14}$$

In the above, $\tau_0 = \rho_s^{\otimes l}, \tau_1 = [(\rho_a+\rho_s)/2]^{\otimes l}$, l is a positive integer number, $\mathcal{B}(\mathbb{C}^{d_s}) \ni \rho_s = \frac{2}{d_s^2+d_s} P_{\text{sym}}, \mathcal{B}(\mathbb{C}^{d_s}) \ni \rho_a = \frac{2}{d_s^2-d_s} P_{\text{as}}$, where $P_{\text{sym}}, P_{\text{as}}$ are, respectively, symmetric and antisymmetric projectors for the bipartite case. It has been shown that a class of states (14) is bound entangled with a private key, $K_D > 0$ [13].

(iv) Finally, let us take $\rho_{ABA'B'} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s})$ in the most general form of pbit, the so-called X form of pbit [13],

$$\rho_{ABA'B'} = \frac{1}{2}\begin{pmatrix} \sqrt{XX^\dagger} & \cdot & \cdot & X \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ X^\dagger & \cdot & \cdot & \sqrt{X^\dagger X} \end{pmatrix}, \tag{15}$$

where X is an arbitrary operator with $||X||_1 = 1$, and dots represent zero matrices.

(v) For a larger dimension of the key part, for example $d_k = 3$, we can take $\rho_{ABA'B'} \in \mathcal{B}(\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s})$ in the following way:

$$\rho_{ABA'B'} = \frac{1}{3}\begin{pmatrix} \sqrt{XX^\dagger} & \cdot & \cdot & \cdot & X & \cdot & \cdot & \cdot & XY \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ X^\dagger & \cdot & \cdot & \cdot & \sqrt{X^\dagger X} & \cdot & \cdot & \cdot & Y \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ (XY)^\dagger & \cdot & \cdot & \cdot & Y^\dagger & \cdot & \cdot & \cdot & \sqrt{Y^\dagger Y} \end{pmatrix}, \tag{16}$$

where matrices X, Y satisfy $||X||_1 = ||Y||_1 = 1$ and $X = WY^\dagger$ for an arbitrary unitary transformation W [18].

From the above examples, we can easily figure out the explicit form of the operators ω_k in every case.

III. PROPERTIES

In this section, we formulate a theorem, which determines the distance in the trace norm between our set of states and the set of pdits in the maximally entangled form. Next, we show (Lemma 2) that this distance depends on the shield dimension d_s for a special, but quite general, subclass of pdits. Namely, we show that this distance scales inversely with the shield dimension d_s. At the end, we also calculate the trace distance from the set of separable states using a special representation of the pdit (Lemma 3). In this and the next sections, without loss of generality, we assume the state $\rho_{ABA'B'}$ to be

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i, \tag{17}$$

where $p+q=1$, $d=\frac{1}{2}d_k(d_k-1)$ and

$$\gamma_0 = \frac{1}{\mathrm{Tr}\omega_0}\omega_0,\ \ \gamma_i = \frac{1}{\mathrm{Tr}\,\omega_i}\omega_i, \tag{18}$$

so such a state indeed belongs to the class defined in Sec. II, and state γ_0 we will call pdit in the maximally entangled form. Now, we are ready to formulate the main results of this section.

Lemma 1. Let us assume that we are given $\rho_{ABA'B'}$ as in Eq. (1) and the pdit γ_0 in its maximally entangled form. Then the following statement holds:

$$||\rho_{ABA'B'} - \gamma_0||_1 = 2q. \tag{19}$$

Proof. The proof is based on straightforward calculations. Let us compute the desired trace distance between $\rho_{ABA'B'}$ and γ_0,

$$\begin{aligned} &||\rho_{ABA'B'} - \gamma_0||_1 \\ &= \left|\left| p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i - \gamma_0 \right|\right|_1 \\ &= \left|\left| \frac{q}{d}\sum_{i=1}^{d}\gamma_i - q\gamma_0 \right|\right|_1 = \frac{q}{d}\left|\left| \sum_{i=1}^{d}\gamma_i - d\gamma_0 \right|\right|_1 . \end{aligned} \tag{20}$$

Now, using the definition of trace norm, we rewrite the last term from the above calculations in a more explicit way,

$$\begin{aligned} &||\rho_{ABA'B'} - \gamma_0||_1 \\ &= \frac{q}{d}\mathrm{Tr}\left[\left(\sum_{i=1}^{d}\gamma_i - d\gamma_0\right)\left(\sum_{i=1}^{d}\gamma_i - d\gamma_0\right)^{\dagger}\right]^{1/2}. \end{aligned} \tag{21}$$

Because we deal with Hermitian matrices, we have

$$||\rho_{ABA'B'} - \gamma_0||_1 = \frac{q}{d}\mathrm{Tr}\left[\left(\sum_{i=1}^{d}\gamma_i + d\gamma_0\right)^2\right]^{1/2}, \tag{22}$$

and finally

$$||\rho_{ABA'B'} - \gamma_0||_1 = \frac{q}{d}\mathrm{Tr}\left[\sum_{i=1}^{d}\gamma_i + d\gamma_0\right] = 2q. \tag{23}$$

We obtain the statement of our theorem, so the proof is finished. ■

Next, we formulate and prove the next lemma, which states that the distance between our class of states given in Sec. II and pdit in its maximally entangled form decreases with the dimension of the shield part d_s. We do it for a specific choice of operators ω_0,ω_k given by Eqs. (2) and (3), which gives a wide class of pdits. Let us choose all matrices $a_{ij}^{(0,0)} = a$, where $0 \leqslant i,j \leqslant d_k$ in such a way that

$$\mathrm{spec}(a) = \left\{\frac{1}{d_s^2},\ldots,\frac{1}{d_s^2}\right\}, \tag{24}$$

and all matrices $a_{mn}^{(i,j)} = b$, where $0 \leqslant m,n \leqslant 1$ and $0 \leqslant i,j \leqslant \frac{1}{2}d_k(d_k-1)$ with $i<j$ as

$$\mathrm{spec}(b) = \left\{\frac{1}{d_s},\ldots,\frac{1}{d_s}\right\}. \tag{25}$$

We also assume that operators which have such spectra are invariant under partial transposition with respect to the system B'. At this point, we refer the reader to Appendix B in which we show the explicit form of operators satisfying all requirements. Using the above definitions, we are ready to show the following.

Lemma 2. Let us consider the class of states given by

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i, \tag{26}$$

where $q=1-p$, $d=\frac{1}{2}d_k(d_k-1)$, and states γ_0,γ_i are given by Eqs. (2) and (3), together with (24) and (25). Then the trace distance from the set of private dits in maximally entangled form is equal to

$$\frac{1}{2}||\rho_{ABA'B'} - \gamma_0||_1 = \frac{1}{1+\frac{d_s}{d_k-1}}, \tag{27}$$

where d_s is the dimension of the shield part and d_k is the dimension of the key part.

Proof. We need to show that in our scheme, the parameter q which is equal to the trace distance between states $\rho_{ABA'B'}$ and pdits γ_0 in their maximally entangled form is equal to $1/(1+\frac{d_s}{d_k-1})$, where d_s,d_k are dimensions of the shield and the key part, respectively. To prove this property, we use the construction described in detail in Appendix A. Because we have assumed that our matrices a and b are invariant under partial transposition with respect to the system B', we can directly use the equality from Eq. (A8) putting, instead of $\widetilde{a}$, a matrix a and, instead of $\widetilde{b}$, a matrix b. Then we have

$$\frac{q}{d_k-1}\lambda(b) - p\lambda(a) = 0, \tag{28}$$

where by $\lambda(a),\lambda(b)$ we denote nonzero eigenvalues of operators a and b, respectively. Now using formulas (24) and (25), we get

$$\frac{q}{d_k-1}\frac{1}{d_s} - p\frac{1}{d_s^2} = 0. \tag{29}$$

Solving the above equality with $p=1-q$, we obtain the statement of our lemma. This finishes the proof. ■

Before we formulate the next result, we introduce the following notation.

Notation 1. Suppose that we are given a quantum state ρ and the set of separable states $\mathcal{S}$. Then, by $\mathrm{dist}(\rho,\mathcal{S})$, we understand the following quantity:

$$\mathrm{dist}(\rho,\mathcal{S}) = \min_{\sigma\in\mathcal{S}}||\rho-\sigma||_1, \tag{30}$$

which is, of course, double minimal trace distance. In the remainder of this manuscript, whenever we talk about distance, we mean the above notation.

Now we are ready to calculate the lower bound on distance between the set of separable states denoted by $\mathcal{S}$ and our subclass of pdits given in the argument before Lemma 2.

Lemma 3. The distance between the set of separable states $\mathcal{S}$ and the class of states of the form

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i, \tag{31}$$

where $q = 1 - p$ and $d = \frac{1}{2}d_k(d_k - 1)$, is bounded from below:

$$\mathrm{dist}(\rho_{ABA'B'},\mathcal{S}) \geqslant 2 - \frac{2}{d_k} - \frac{2}{1 + \frac{d_s}{d_k - 1}}, \tag{32}$$

where d_s denotes the dimension of the shield part and d_k denotes the dimension of the key part.

Proof. In our proof, we use the fact that the distance between an arbitrary private state $\bar{\gamma}$ and the set of separable states $\mathcal{S}$ is bounded from below [17] by

$$\mathrm{dist}(\bar{\gamma},\mathcal{S}) \geqslant 2 - \frac{2}{d_k}, \tag{33}$$

where d_k is the dimension of the key part. Because the above bound holds for an arbitrary private state, it also holds for a pdit in its maximally entangled form γ_0. Now let us take the closest separable state ω to $\rho_{ABA'B'}$ given by Eq. (31). Using the triangle inequality, we can write

$$\begin{aligned} &||\rho_{ABA'B'} - \omega||_1 + ||\rho_{ABA'B'} - \gamma_0||_1 \\ &\quad \geqslant ||\omega - \gamma_0||_1 \geqslant \mathrm{dist}(\gamma_0,\mathcal{S}) \geqslant 2 - \frac{2}{d_k}, \end{aligned} \tag{34}$$

but from Lemma 2 we know that $||\rho_{ABA'B'} - \gamma_0||_1 = \frac{2}{1+\frac{d_s}{d_k-1}}$, so

$$||\rho_{ABA'B'} - \omega||_1 + \frac{2}{1 + \frac{d_s}{d_k-1}} \geqslant 2 - \frac{2}{d_k}. \tag{35}$$

The above inequality directly implies that

$$\mathrm{dist}(\rho_{ABA'B'},\mathcal{S}) \geqslant 2 - \frac{2}{d_k} - \frac{2}{1 + \frac{d_s}{d_k-1}}. \tag{36}$$

■

Let us notice that for our special case $d_k = 2$, when Alice and Bob share qubit states, the bound obviously improves with dimension of the shield part and has minimum for $d_s = 2$, i.e., when Alice and Bob share a four-qubit state.

Let us recall that the state from Lemma 2 can be considered as a PPT state acting on $\mathbb{C}^d \otimes \mathbb{C}^d$, where $d = d_s d_k$. We can formulate the following, recovering the result from [17] and [19].

Theorem 1. For an arbitrary $\epsilon > 0$, there exists a PPT state ρ acting on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ with $d \leqslant \frac{c}{\epsilon^3}$ such that

$$\mathrm{dist}(\rho,\mathcal{S}) \geqslant 2 - \epsilon, \tag{37}$$

where c is constant. The state is given by (26).

The proof is straightforward and based on simple calculations, so it is not reported here. We have found analytically that constant $c < 64$. This result considerably improves the bound obtained in [17].

IV. SUMMARY

In this paper, we present the construction of the set of pdits, which contains many known examples of private states from the literature (Sec. II). We also present the result specifying the trace distance between our set of pdits and the pdit in the maximally entangled form. Next, we connect this result with a dimension of the shield part d_s, and we prove that this distance is inversely proportional to d_s, at least for a particular subclass of pdits. We also calculate the trace distance from the set of separable states $\mathcal{S}$ and show that for a fixed dimension of key part d_k, this distance decreases with d_s. The most interesting property of our alternate class of states, which differentiates it from the known results, is that we do not need many copies of them (see [17]) to boost the distance from the set of separable states $\mathcal{S}$ (Sec. III). We also provide explicit calculations of a family of states such that we recover the $2 - \epsilon$ distance from $\mathcal{S}$ [17,19] in a natural and basic way. Finally, we show that the scaling of ϵ with the distance is $d \propto 1/\epsilon^3$, and it is considerably better than $d \propto 2^{[\log(4/\epsilon)]^2}$ from [17].

ACKNOWLEDGMENTS

M.H. thanks S. Szarek for valuable discussions. Part of this work was done at the National Quantum Information Center of Gdansk. M.S. and P.Ć. are thankful for the hospitality of the IBM TJ Watson Research Center, where (another) part of this work was done, and acknowledge helpful discussions with Graeme Smith and John Smolin about private states and private bits. M.S. is supported by the International PhD Project “Physics of future quantum-based information technologies,” Grant No. MPD/2009-3/4 from the Foundation for Polish Sciences. M.S. and P.Ć. acknowledge the support from the National Science Centre project Maestro, Grant No. DEC-2011/02/A/ST2/00305. A.R. is supported by a postdoctoral internship, Decision No. DEC-2012/04/S/ST2/00002, from the (Polish) National Science Center. M.H. is supported by Polish Ministry of Science and Higher Education Grant No. IdP2011 000361.

APPENDIX A: CONSTRUCTION OF SPECIAL PDITS SUBCLASS

In this section, we describe the method which we have used to obtain explicit positivity conditions in the proof of Lemma 2 for an arbitrary dimension of the key part d_k. Our argument is made for the specific subclass of states given at the beginning of Sec. II. Suppose that the above-mentioned subclass is in the following form:

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i \in \mathcal{B}(\mathcal{H}_{d_k} \otimes \mathcal{H}_{d_k} \otimes \mathcal{H}_{d_s} \otimes \mathcal{H}_{d_s}), \tag{A1}$$

where $d = \frac{1}{2}d_k(d_k - 1)$ and matrices γ_0, γ_i are defined on orthogonal subspaces in a similar way as in (2) and (3). Of course, to satisfy $\rho_{ABA'B'} \geqslant 0$, we need $\gamma_0 \geqslant 0$ and $\gamma_i \geqslant 0$. In our construction operator, γ_0 corresponds with (2), but all $a_{ij}^{(0,0)} = a$ together with $||a||_1 = 1$. Similarly, we proceed for the matrices γ_i by putting all submatrices $a_{mn}^{(i,j)}$ equal to b with $||b||_1 = 1$. Thanks to this, we have an explicit connection between states γ_0,γ_i and ω_0,ω_i from (2) and (3) by the following formulas:

$$\gamma_0 = \frac{1}{d_k}\omega_0, \quad \gamma_i = \frac{1}{2}\omega_i, \quad \text{where} \quad d = \frac{1}{2}d_k(d_k-1). \tag{A2}$$

It is easy to see that to ensure the PPT property with respect to partial transposition on BB', it is enough to satisfy the PPT condition for every component of (A1) separately after partial transposition. Thanks to this and the property of orthogonality, we can write

$$\begin{aligned}&(\mathbb{1}_A \otimes T_B \otimes \mathbb{1}_{A'} \otimes T_{B'})\rho_{ABA'B'}\\ &\quad\geqslant 0 \Leftrightarrow PT_{d_k} = \begin{pmatrix} p\widetilde{a} & \frac{q}{d_k-1}\widetilde{b} & \cdots & \frac{q}{d_k-1}\widetilde{b} \\ \frac{q}{d_k-1}\widetilde{b} & p\widetilde{a} & \cdots & \frac{q}{d_k-1}\widetilde{b} \\ \vdots & & \ddots & \vdots \\ \frac{q}{d_k-1}\widetilde{b} & \cdots & p\widetilde{b} & \frac{q}{d_k-1}\widetilde{a} \end{pmatrix} \geqslant 0,\end{aligned} \tag{A3}$$

and

$$\begin{aligned}&(\mathbb{1}_A \otimes T_B \otimes \mathbb{1}_{A'} \otimes T_{B'})\rho_{ABA'B'}\\ &\quad\geqslant 0 \Leftrightarrow PT = \begin{pmatrix} \frac{q}{d_k-1}\widetilde{b} & p\widetilde{a} \\ p\widetilde{a} & \frac{q}{d_k-1}\widetilde{b} \end{pmatrix} \geqslant 0,\end{aligned} \tag{A4}$$

where $\widetilde{a},\widetilde{b}$ are operators a,b after partial transposition with respect to subsystem B', and the second condition is taken d_k times.

In general, still it is hard to say whether constraints (A3) and (A4) are satisfied, but there is a nice mathematical trick which allows us to rewrite the above condition in a more operative way. Namely, matrices PT_{d_k} and PT can be written as

$$\begin{aligned} PT_{d_k} &= \mathbb{1}_{d_k} \otimes p\widetilde{a} - \mathbb{1}_{d_k} \otimes \frac{q}{d_k-1}\widetilde{b} + \mathbb{I}_{d_k} \otimes \frac{q}{d_k-1}\widetilde{b} \geqslant 0,\\ PT &= \mathbb{1}_2 \otimes \frac{q}{d_k-1}\widetilde{b} - \mathbb{1}_2 \otimes p\widetilde{a} + \mathbb{I}_2 \otimes p\widetilde{a} \geqslant 0,\end{aligned} \tag{A5}$$

where $\mathbb{1}_{d_k},\mathbb{1}_2$ are identity matrices of dimensions d_k and 2, respectively, and $\mathbb{I}_{d_k}$ and $\mathbb{I}_2$ are with all entries equal to 1 of dimensions d_k and 2, respectively. To say that PT_{d_k} and PT are positive is enough to say that they have all eigenvalues λ greater or equal to zero, so we can write

$$\begin{aligned} \lambda(PT_{d_k}) &= \lambda(\mathbb{1}_{d_k} \otimes p\widetilde{a}) - \lambda\left(\mathbb{1}_{d_k} \otimes \frac{q}{d_k-1}\widetilde{b}\right)\\ &\quad + \lambda\left(\mathbb{I}_{d_k} \otimes \frac{q}{d_k-1}\widetilde{b}\right) \geqslant 0,\\ \lambda(PT) &= \lambda\left(\mathbb{1}_2 \otimes \frac{q}{d_k-1}\widetilde{b}\right) - \lambda(\mathbb{1}_2 \otimes p\widetilde{a})\\ &\quad + \lambda(\mathbb{I}_2 \otimes p\widetilde{a}) \geqslant 0. \end{aligned} \tag{A6}$$

Because $\mathrm{spec}(\mathbb{I}_{d_k}) = \{0,\ldots,0,d_k\}$, where 0 is taken $d_k - 1$ times, we have the following set of constraints:

$$\begin{aligned} &p\lambda(\widetilde{a}) + q\lambda(\widetilde{b}) \geqslant 0, \quad p\lambda(\widetilde{a}) - \frac{q}{d_k-1}\lambda(\widetilde{b}) \geqslant 0,\\ &\frac{q}{d_k-1}\lambda(\widetilde{b}) + p\lambda(\widetilde{a}) \geqslant 0, \quad \frac{q}{d_k-1}\lambda(\widetilde{b}) - p\lambda(\widetilde{a}) \geqslant 0. \end{aligned} \tag{A7}$$

From the above, we see that only nontrivial conditions are given by the second and fourth inequality, which are reduced (together) to equality

$$\frac{q}{d_k-1}\lambda(\widetilde{b}) - p\lambda(\widetilde{a}) = 0. \tag{A8}$$

We see that to ensure PPT property, it is enough to satisfy only one constraint, which depends only on eigenvalues of submatrices of γ_0 and γ_i.

APPENDIX B: CONSTRUCTION OF THE OPERATORS WITH SPECIFIC CONSTRAINTS ON SPECTRA

In Sec. II, we use a class of operators with the specific properties such that invariance is with respect to partial transposition on the B' system and the particular spectra. Now, we present one of the possible realization of such operators. Namely, let us take (see [17])

$$\begin{aligned} X &= \frac{1}{d_s\sqrt{d_s}}\sum_{i,j=1}^{d_s} u_{ij}|ij\rangle\langle ji|,\\ Y &= \sqrt{d_s}X^{T_{B'}} = \frac{1}{d_s}\sum_{i,j=1}^{d_s} u_{ij}|ii\rangle\langle jj|, \end{aligned} \tag{B1}$$

where u_{ij} are matrix elements of some unitary matrix $U \in M(d_s \times d_s,\mathbb{C})$ with $|u_{ij}| = \frac{1}{\sqrt{d_s}}$. It is easy to see that $(\mathbb{1}_B \otimes T_{B'})X = X$ and $(\mathbb{1}_B \otimes T_{B'})Y = Y$. Moreover, we can prove the following.

Fact 1. Matrices $\sqrt{XX^\dagger}$ and $\sqrt{YY^\dagger}$, where X,Y are given by the formula (B1), satisfy

$$\begin{aligned} \mathrm{spec}(\sqrt{XX^\dagger}) &= \left\{\frac{1}{d_s^2},\ldots,\frac{1}{d_s^2}\right\},\\ \mathrm{spec}(\sqrt{YY^\dagger}) &= \left\{\frac{1}{d_s},\ldots,\frac{1}{d_s},0,\ldots,0\right\}, \end{aligned} \tag{B2}$$

where d_s denotes the dimension of the shield part, and for every matrix we have d_s eigenvalues. Moreover, the multiplicity of $1/d_s^2$ is equal to d_s^2, the multiplicity of $1/d_s$ is equal to d_s, and, finally, the multiplicity of zeros is equal to $d_s(d_s - 1)$.

Proof. The proof is based on the following observation:

$$XX^\dagger = X^\dagger X = \frac{1}{d_s^4}, \quad YY^\dagger = Y^\dagger Y = \frac{1}{d_s^2}. \tag{B3}$$

Let us redefine X and Y, introducing $\widetilde{X} = d_s^2 X$ and $\widetilde{Y} = d_s\sqrt{d_s}Y$. We have that $\widetilde{X}\widetilde{X}^\dagger = \widetilde{X}^\dagger\widetilde{X} = \mathbb{1}$, and similarly for $\widetilde{Y}$. Thanks to this, we see that matrices $\widetilde{X},\widetilde{Y}$ are unitary, so their eigenvalues are $e^{i\varphi_i}$, for $i = 1,\ldots,d_s$. Now it is easy to deduce that

$$\begin{aligned} \mathrm{spec}(X) &= \left\{\frac{1}{d_s^2}e^{i\varphi_1},\ldots,\frac{1}{d_s^2}e^{i\varphi_{d_s}}\right\},\\ \mathrm{spec}(Y) &= \left\{\frac{1}{d_s}e^{i\varphi_1},\ldots,\frac{1}{d_s}e^{i\varphi_{d_s}}\right\}, \end{aligned} \tag{B4}$$

and

$$\begin{aligned}\operatorname{spec}(XX^\dagger) &= \left\{\frac{1}{d_s^4},\ldots,\frac{1}{d_s^4}\right\},\\ \operatorname{spec}(YY^\dagger) &= \left\{\frac{1}{d_s^2},\ldots,\frac{1}{d_s^2}\right\}.\end{aligned} \tag{B5}$$

In Eqs. (B4) and (B5), for simplicity we have omitted zeros in the spectra of spec(Y) and spec($YY^\dagger$). Moreover, they do not give us any nontrivial condition for positivity (see Appendix A). Finally, for $\sqrt{XX^\dagger},\sqrt{YY^\dagger}$, we simply have to take the square roots from every eigenvalue from the above spectra to obtain the desired result. ■

Now, in Lemma 2, we can directly substitute $\sqrt{XX^\dagger}$ instead of $a_{kl}^{(0,0)}$, where $0 \leqslant k,l \leqslant d_k - 1$, and $\sqrt{YY^\dagger}$ instead of $a_{mn}^{(i,j)}$, where $0 \leqslant m,n \leqslant 1$ and $0 \leqslant i,j \leqslant d_k - 1$; for $i < j$, we obtain the specific example of the pdit from our class.

[1] Charles H. Bennett and Gilles Brassard (unpublished).
[2] Artur K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] N. Gisin, R. Renner, and S. Wolf, Algorithmica, **34**, 389 (2002).
[6] N. Gisin and S. Wolf, in *Advances in Cryptology - CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, edited by M. Bellare (Springer, Berlin-Heidelberg, 2000).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[8] R. Horodecki, Europhys. News **41**, 21 (2010).
[9] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[10] Ł. Pankowski and M. Horodecki, J. Phys. A: Math. Theor. **44**, 035301 (2011).
[11] R. Augusiak and P. Horodecki, Phys. Rev. A **80**, 042307 (2009).
[12] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).
[14] K. Dobek, M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, and P. Horodecki, Phys. Rev. Lett. **106**, 030501 (2011).
[15] K. Banaszek, K. Horodecki, and P. Horodecki, Phys. Rev. A **85**, 012330 (2012).
[16] M. Ozols, G. Smith, and J. A. Smolin, Phys. Rev. Lett. **112**, 110502 (2014).
[17] P. Badziąg, K. Horodecki, M. Horodecki, J. Jenkinson, and S. J. Szarek, Phys. Rev. A **90**, 012301 (2014).
[18] K. Horodecki, Ph.D. thesis, University of Warsaw, 2008.
[19] S. Beigi and P. W. Shor, J. Math. Phys. **51**, 042202 (2010).