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

Michał Studziński[1,2], Adam Rutkowski[1,2], Piotr Ćwikliński[1,2] and Michał Horodecki[1,2]

[1] *Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

[2] *National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland*

## I. MOTIVATION AND MAIN RESULTS

A quantum private states of a dimension $d$ (so called pdits) is composed from a $d \otimes d$ $AB$ part called "key", and $A'B'$ called "shield", shared between Alice (subsystems $AA'$) and Bob (subsystems $BB'$) in such a way that the local von Neumann measurements on the key part in a particular basis will make its results 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 of great importance in quantum cryptography and have been studied extensively for some time [10–15].

In our poster we would like to present the new construction the set of private states of a dimension $d$ which contain all previously known examples of pdits. We examine a bunch of properties for this new class like the trace distance to a pdit in the maximally entangled form [1]. For a certain but wide subclass we also present that this distance scales inversely with the dimension of the shield part $d_s$ and gives the lower bound for the distance from the set of separable states. Using our construction we are also able to show that we do not need many copies of pdits [Badzią̧g et al., Phys. Rev. A 90, 012301 (2014)] to boost the distance from the set of separable states ($\mathcal{SEP}$), which is somehow more "natural" way to obtain states with certain properties. At the end we provide also explicit calculations of a family of states such that the $2-\epsilon$ distance from $\mathcal{SEP}$ obtained in [Beigi et al., J. Math. Phys. 51, 042202, (2010)] and [Badzią̧g et al., Phys. Rev. A 90, 012301 (2014)] is recovered, such that the scaling of $\epsilon$ with the distance is improved, $d \propto 1/\epsilon^3$, as opposed to $d \propto 2^{(log(4/\epsilon))^2}$ from Badzią̧g et al.

## II. GENERAL IDEA OF CONSTRUCTION

Our goal is to construct set of states $\rho_{ABA'B'}$ which has PPT property [2] and they are close to pdits in the maximally entangled form. We postulate that all states which we want to consider have the following structure:

$$\rho_{ABA'B'} = \sum_{l=0}^{d} \omega_l \in \mathcal{B}\left(\mathcal{H}_{d_k} \otimes \mathcal{H}_{d_k} \otimes \mathcal{H}_{d_s} \otimes \mathcal{H}_{d_s}\right), \tag{2}$$

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. (2). First of all, we define the term $\omega_0$ as:

$$\omega_0 = \sum_{i,j=0}^{d_k-1} |i\rangle\langle j| \otimes |i\rangle\langle j| \otimes a_{ij}^{(0,0)}, \tag{3}$$

---

[1] For example maximally entangled form of pdit with dimension of the key part $d_k = 2$ have a following representation:

$$\gamma_0 = \frac{1}{2}\begin{pmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{pmatrix}, \tag{1}$$

where $X$ is an arbitrary operator with trace norm equal to one.

[2] PPT (Positive Partial Transposition)

where every $a_{ij}^{(0,0)} \in \mathcal{B}\left(\mathcal{H}_{d_s} \otimes \mathcal{H}_{d_s}\right)$. The rest of elements $\omega_l$, for $1 \leq l \leq \frac{1}{2}d_k(d_k-1)$ from Eq. (2) are given by the following formula

$$\begin{aligned}\omega_l = |i\rangle\langle i| \otimes |j\rangle\langle j| \otimes a_{00}^{(i,j)} + |i\rangle\langle j| \otimes |j\rangle\langle i| \otimes a_{01}^{(i,j)} + \\ + |j\rangle\langle i| \otimes |i\rangle\langle j| \otimes a_{10}^{(i,j)} + |j\rangle\langle j| \otimes |i\rangle\langle i| \otimes a_{11}^{(i,j)},\end{aligned} \tag{4}$$

where indices $i, j = 0, \ldots, d_k - 1$ for $i < j$.

Let us introduce the following notation, namely:

$$A^{(i,j)} = \begin{pmatrix} a_{00}^{(i,j)} & a_{01}^{(i,j)} \\ a_{10}^{(i,j)} & a_{11}^{(i,j)} \end{pmatrix}, \tag{5}$$

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

$$A^{(0,0)} = \begin{pmatrix} a_{00}^{(0,0)} & \cdots & a_{0,d_k-1}^{(0,0)} \\ \vdots & \ddots & \vdots \\ a_{d_k-1,0}^{(0,0)} & \cdots & a_{d_k-1,d_k-1}^{(0,0)} \end{pmatrix}. \tag{6}$$

Then, there is also explicit connection between positivity of the state $\rho_{ABA'B'}$ and each submatrix $A^{(i,j)}$ and positivity of $\rho_{ABA'B'}^{\mathrm{T}_{A'}\mathrm{T}_{B'}}$ and each block $A^{(i,j)}$ after partial transposition on the system $\mathrm{T}_{B'}$, which can be quite easily deduced from the block structure of states $\rho_{ABA'B'}$ (see Observation 1 in). At the end of this section is worth to remind again that thanks to proper choice of the all blocks from (3) (5) (6) we can recover all known forms of pdits. As an example we recover one of the pdit given in [13]. Let us put $\gamma^{\mathrm{V}} = \mathcal{B}\left(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s}\right)$ then choosing $a_{00}^{(0,0)} = \mathbb{1}/d_s^2$, $a_{01}^{(0,0)} = \mathrm{V}/d_s^2$, $a_{10}^{(0,0)} = \mathrm{V}/d_s^2$, $a_{11}^{(0,0)} = \mathbb{1}/d_s^2$ then we have

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

where $\mathrm{V} = \sum_{i=0}^{d_s-1} |ij\rangle\langle ji|$ 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.

## III. PROPERTIES OF THE NEW CLASS OF STATES

In this section we would like to summarize the main results obtained for the class of states given by the formula (2). First of all we calculate trace distance between states $\rho_{ABA'B'}$ defined in equation (2) and the set of pdits in the maximally entangled form (Theorem 1). Next we show that this distance scales inversely proportional to the dimension of the shield part $d_s$ for some special, but very wide subclass of states given in (2) (Lemma 2). At the end we explain that for this specific subclass we are able calculate the lower bound for the trace distance from the set of separable states $\mathcal{SEP}$. We show that this bound scales inversely with the dimensions of the shield part (Lemma 3). At the end we present also technical Theorem 4 which improves known scaling given in [17] of the trace distance for the states given by (2), which are $2-\epsilon$ close to $\mathcal{SEP}$.

Before we formulate above mentioned results let us rewrite state from (2) in more convenient form

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i, \quad \text{with} \quad \gamma_0 = \frac{1}{\operatorname{Tr}\omega_0}\omega_0, \qquad \gamma_i = \frac{1}{\operatorname{Tr}\omega_i}\omega_i, \tag{7}$$

with $p + q = 1$ and $d = \frac{1}{2}d_k(d_k-1)$. Now we are ready to formulate first theorem which states the trace distance from the set of pdits in the maximally entangled form $\gamma_0$:

**Theorem 1.** *Let us assume that we are given with $\rho_{ABA'B'}$ as in Eq. (2) and the pdit $\gamma_0$ in its maximally entangled form, then the following statement holds:*

$$||\rho_{ABA'B'} - \gamma_0||_1 = q. \tag{8}$$

To formulate the rest results mentioned at the begin of this section we need specific choice of the operators $\omega_0, \omega_k$ given in. In our construction we can choose all matrices $a_{ij}^{(0,0)} = a$, where $0 \leq i, j \leq d_k$ and all matrices $a_{mn}^{(i,j)} = b$, where $0 \leq m, n \leq 1$ and $0 \leq i, j \leq \frac{1}{2}d_k(d_k - 1)$ with $i < j$ as:

$$\mathrm{spec}(a) = \left\{ \frac{1}{d_s^2}, \ldots, \frac{1}{d_s^2} \right\}, \qquad \mathrm{spec}(b) = \left\{ \frac{1}{d_s}, \ldots, \frac{1}{d_s} \right\}. \tag{9}$$

We also assume that which have such spectra are invariant under partial transposition with respect to the system $B'$. This assumption may look very rigorous but it is quite easy to construct set of matrices satisfying above constraints (see for example [17]). Using all above facts we can formulate

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

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d} \gamma_i, \tag{10}$$

*where $q = 1 - p$, $d = \frac{1}{2}d_k(d_k - 1)$ and states $\gamma_0, \gamma_i$ are given by Eqs* (3), (4), *together with* (9). *Then the trace distance from the set of private dits in maximally entangled form is equal to*

$$\mathrm{dist}\left(\rho_{ABA'B'}, \gamma_0\right) = \frac{1}{1 + \frac{d_s}{d_k - 1}}, \tag{11}$$

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

Now we can formulate theorem which gives mentioned lower bound on trace distance between our wide subclass of states and the set of separable states $\mathcal{SEP}$:

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

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d} \gamma_i, \tag{12}$$

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

$$\mathrm{dist}(\rho_{ABA'B'}, \mathcal{SEP}) \geq 2 - \frac{2}{d_k} - \frac{1}{1 + \frac{d_s}{d_k - 1}}, \tag{13}$$

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

Finally we can improve the scaling of the trace distance for states, which are $2 - \epsilon$ close to the separable states $\mathcal{SEP}$:

**Theorem 4.** *For an arbitrary $\epsilon > 0$ there exists a PPT state $\rho$ acting on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ with $d \leq \frac{c}{\epsilon^3}$ such that:*

$$\mathrm{dist}(\rho, \mathcal{SEP}) \geq 2 - \epsilon, \tag{14}$$

*where c is constant. The sate is given by (10).*

We have found analytically that constant $c < 48$. This result considerably improves the bound obtained in [17].

---


[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society Press, New York, Bangalore, India, December 1984, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptology **5**, 3 (1992), ISSN 0933-2790.
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), quant-ph/0003004.
[5] N. Gisin, R. Renner, and S. Wolf, in *Algorithmica* (Springer-Verlag, 2000), pp. 482–500.

[6] N. Gisin and S. Wolf, in *Advances in Cryptology - CRYPTO 2000*, edited by M. Bellare (Springer Berlin Heidelberg, 2000), vol. 1880 of *Lecture Notes in Computer Science*, pp. 482–500, ISBN 978-3-540-67907-3, URL `http://dx.doi.org/10.1007/3-540-44598-6_30`.

[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998), quant-ph/9801069.

[8] Horodecki, R., Europhysics News **41**, 21 (2010), URL `http://dx.doi.org/10.1051/epn/2010603`.

[9] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005), quant-ph/0309110.

[10] Ł. Pankowski and M. Horodecki, J. Phys. A: Math. Theor. **44**, 035301 (2011), quant-ph/1008.1226.

[11] R. Augusiak and P. Horodecki, Phys. Rev. A **80**, 042307 (2009).

[12] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008), quant-ph/0506203.

[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009), quant-ph/0506189.

[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 (20141), quant-ph/1305.0848.

[17] P. Badziąg, K. Horodecki, M. Horodecki, J. Jenkinson, and S. J. Szarek, Phys. Rev. A **90**, 012301 (2014).

[18] S. Beigi and P. W. Shor, J. Math. Phys. **51**, 042202 (2010).