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

Adam Rutkowski,[1,2,*] Michał Studziński,[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 Center, 81-824 Sopot, Poland*

A quantum private states of a dimension d (so called pdits) is composed from a $d \otimes d$ A,B part called a "key", and A',B' called "shield", shared between Alice (subsystems A,A') and Bob (subsystems B,B') 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 $\psi_{ABA'B'E}$ of the pdit state $\rho_{ABA'B'}$. Pdits (especially pbits) are of great importance in quantum cryptography and have been studied extensively for some time. 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 $\mathcal{SEP}$, showing that for a fixed dimension of the key part d_k the distance increases with d_s. We provide explicit examples of PPT states (in d dimensions) which are nearly as far from separable ones as possible.

Let us consider the following state [1]:

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

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

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

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

We formulate and prove the following lemmas and theorem concerning our construction of private states [1]

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

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

where $0 \leq q \leq 1$.

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

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i, \qquad (3)$$

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

$$\frac{1}{2}||\rho_{ABA'B'} - \gamma_0||_1 = \frac{1}{1+\frac{d_s}{d_k-1}}, \qquad (4)$$

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

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

$$\rho_{ABA'B'} = p\gamma_0 + \frac{q}{d}\sum_{i=1}^{d}\gamma_i, \qquad (5)$$

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

$$\mathrm{dist}(\rho_{ABA'B'}, \mathcal{SEP}) \geq 2 - \frac{2}{d_k} - \frac{2}{1+\frac{d_s}{d_k-1}}, \qquad (6)$$

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

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

$$\mathrm{dist}(\rho, \mathcal{SEP}) \geq 2 - \epsilon, \qquad (7)$$

where c is constant.

---

* fizar@ug.edu.pl

[1] Adam Rutkowski, Michał Studziński, Piotr Ćwikliński, and Michał Horodecki, Phys. Rev. A **91**, 012335 (2015).