Limits and restrictions of private quantum channel

Jan Bouda[1] and Mario Ziman[1,2]

[1] Faculty of Informatics, Masaryk University,
Botanická 68a, 602 00 Brno, Czech Republic

[2] Research Center for Quantum Information, Slovak Academy of Sciences
Dubravská cesta 9, 845 11 Bratislava, Slovakia

June 15, 2005

Abstract

We study private quantum channels on a single qubit, which encrypt given set of plaintext states **P**. Specifically, we determine all achievable states $\rho^{(0)}$ (average output of encryption) and for each particular set **P** we determine the entropy of the key necessary and sufficient to encrypt this set. It turns out that single bit of key is sufficient when the set **P** is two dimensional. However, the necessary and sufficient entropy of the key in case of three dimensional **P** varies continuously between 1 and 2 bits depending on the state $\rho^{(0)}$. Finally, we derive private quantum channels achieving these bounds. We show that the impossibility of universal NOT operation on qubit can be derived from the fact that one bit of key is not sufficient to encrypt qubit.

1 Introduction

Quantum cryptography [14, 5] (for a popular review see [16]) is a rapidly developing branch of quantum information processing. The results of quantum cryptography include quantum key distribution [3, 12], quantum secret sharing [19, 9], quantum oblivious transfer [4, 10] and other cryptographic protocols [17]. Quantum cryptography has two main goals: solutions to classical cryptographic primitives, and quantum cryptographic primitives.

The first goal is to design solutions of cryptographic primitives, which achieve a higher (provable) degree of security than their classical counterparts. The degree of security should be better than the security of any known classical solution, or it should be of the degree that is even not achievable by using classical information theory at all. Another alternative is to design a solution which is more efficient[1] than any classical solution of comparable security.

The second class of cryptosystems is motivated by the evolution of applications of quantum information processing, regardless whether their purpose is cryptographic, communication complexity based or algorithmic. These cryptosystems are designed to manipulate quantum information. As applications of quantum information processing start to challenge a number of their classical counterparts, the need to secure quantum communications in general is getting more urgent. Therefore, there is a large class of quantum primitives which should secure quantum communication in the same way as classical communication is secured. These primitives include encryption of quantum information using both classical [1, 6, 23] and quantum key [21], authentication of quantum information [2], secret sharing of quantum information [9, 15], quantum data hiding [11] and even commitment to a quantum bit [5], oblivious transfer of quantum information [5] and others.

In this paper we concentrate on the encryption of quantum information with classical key [1] described and explained in Section 2. At the end of Section 2 we introduce notation and one theorem we will be using through the remaining sections. To begin our analysis, in Section 3 we investigate for a given set $\mathbf{P}$ the set of all possible states $\rho^{(0)}$ such that there exists a private quantum channel $\hat{\mathbf{E}}$ with the property $\forall\rho \in \mathbf{P} : \hat{\mathbf{E}}(\rho) = \rho^{(0)}$ and we determine that it forms a ball within the Bloch sphere centered in $\frac{1}{2}\mathbb{1}$. In the Sections 4–7 we derive all possible private quantum channels for a given set $\mathbf{P}$ and state $\rho^{(0)}$ and analyze necessary and sufficient entropy of the key of such PQC. We also explicitly construct PQCs achieving this bound. Another interesting result contained in Section 7 is that any PQC encrypting given set $\mathbf{P}$ of two linearly independent states encrypts also any two-dimensional set $\mathbf{P}'$ parallel to $\mathbf{P}$ and lying in the plane spanned by $\mathbf{P}$ and $\frac{1}{2}\mathbb{1}$.

We conclude our paper in Section 8 by few comments on possible generalizations of the described techniques to systems of higher dimension.

2 Private quantum channel

The private quantum channel [1] is a general framework designed to perfectly encrypt an arbitrary quantum system using a classical key.

Definition 2.1. Let $\mathbf{P} \subseteq \mathcal{S}(\mathcal{H}_{1,\ldots,n})$ be a set of n-qubit states[2], $\hat{\mathbf{E}} = \{(p_i, U_i)\}_i$ be a superoperator, where each U_i is a unitary operator on $\mathcal{H}_{1,\ldots,m}, n \leq m$, $p_i \geq 1$ and $\sum_i p_i = 1$. Let ρ_{anc} be an $(m-n)$ qubit density matrix and $\rho^{(0)}$ be an m-qubit density matrix. Then $[\mathbf{P}, \hat{\mathbf{E}}, \rho_{anc}, \rho^{(0)}]$ is a **private quantum**

[1] According to time, space or communication complexity.

[2] To make the definition easier we work with qubits. To obtain an equivalent definition for arbitrary quantum systems A it suffices to replace $\mathcal{H}_{1,\ldots,n}$ by $\mathcal{H}_A$ and $\mathcal{H}_{n+1,\ldots,m}$ by $\mathcal{H}_{anc}$.

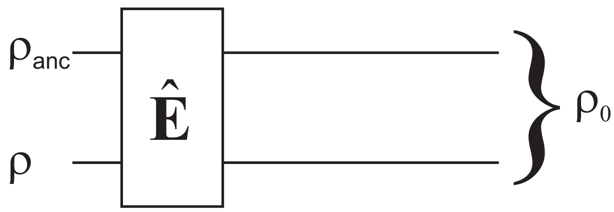

Figure 1: Encryption using PQC.

channel (PQC) if and only if for all $\rho \in \mathbf{P}$ it holds that

$$\hat{\mathbf{E}}(\rho \otimes \rho_{anc}) = \sum_i p_i U_i (\rho \otimes \rho_{anc}) U_i^\dagger = \rho^{(0)}. \qquad (1)$$

The definition of the private quantum channel establishes the following cryptosystem. Alice wants to establish a communication (quantum) channel with Bob with the property that any state $\rho \in \mathbf{P}$ will be transmitted securely. The security in this case means that Eve gets no advantage (information) by intercepting the transmitted message.

The encryption of the plaintext is done in the way that one operator, chosen randomly out of the operators $\{U_i\}_i$, is applied to the plaintext system. The operator U_i is chosen with probability p_i. The classical key specifies which of the unitary operators was applied. The unitary operators U_i are acting on $\mathcal{H}_{1,\ldots,m}$, while the state ρ is only n-qubit state. The encryption operation U_i is performed on the Hilbert space $\mathcal{H}_{1,\ldots,m}$, the plaintext space $\mathcal{H}_{1,\ldots,n}$ is a subspace of $\mathcal{H}_{1,\ldots,m}$. The encryption operation is defined on the (possibly) larger space than the plaintext to allow optional encryption of the plaintext together with an ancillary system. The encryption operators, therefore, act on a tensor product of the plaintext Hilbert space $\mathcal{H}_{1,\ldots,n}$ and the ancillary Hilbert space $\mathcal{H}_{n+1,\ldots,m}$, which is originally factorized (decoupled) from the plaintext. The ancillary Hilbert space is initially in the state ρ_{anc} (see Figure 1).

The security of the scheme can be explained in the following way: Without knowledge of the key (i.e. without specific knowledge about which of the operators was used) any initial state $\rho \in \mathbf{P}$ together with the ancilla appears to be in the state $\rho^{(0)}$ after the encryption. The state $\rho^{(0)}$ is the same for all $\rho \in \mathbf{P}$, it is independent of the input state. It means that all states from the set $\mathbf{P}$ are physically indistinguishable after the encryption.

A dual point of view of the security is also possible. Let us denote by $\mathbf{C} = \hat{\mathbf{E}}[\mathbf{P}]$ the set of all ciphertexts, i.e. $\rho_i^{(c)} = U_i \rho U_i^\dagger \in \mathbf{C}$ for each encryption operation U_i and plaintext state $\rho \in \mathbf{P}$. The encryption key (represented by the sequence $i_1, \ldots, i_n$) is used also for the decryption. The only difference in the case of the decryption is that the inverse operations $U_i^\dagger$ are applied, i.e. $\rho_i^{(c)} \mapsto U_i^\dagger \rho_i^{(c)} U_i = \rho \in \mathbf{P}$. Formally the decryption procedure induces a transformation $\hat{\mathbf{D}}[\rho] = \sum_i p_i U_i^\dagger \rho U_i$. It describes the result of a decryption of a particular ciphertext without knowledge which key was used to encrypt it. The probabilities $\{p_i\}_i$ are the same as in the case of Eq. (1), because the probability that the key U_i was used is p_i. In general, each encryption operation U_i defines a different set of ciphertexts $\mathbf{C}_i$. The linear span $\overline{\mathbf{C}}_i$ is just rotated set of plaintexts $\overline{\mathbf{P}}$.

From Eq. (1) it follows that the information about the ciphertext contained in the plaintext is $I(\rho_P : \rho_C) = 0$. However, from the symmetry of the mutual information it follows that the information about plaintext contained in the ciphertext is also 0, therefore, the dual equation also holds

$$\hat{\mathbf{D}}(\rho) = \sum_i p_i U^{\dagger}{}_i(\rho) U_i = \rho^{(1)}, \tag{2}$$

where $\rho^{(1)}$ is fixed for all ciphertext states ρ. The superoperator $\hat{\mathbf{D}} = \{(p_i, U^{\dagger}{}_i)\}_i$ is not an inverse of the superoperator $\hat{\mathbf{E}}$ in the standard meaning. It describes the result of a decryption of a particular ciphertext without knowledge which key was used to decrypt it.

From the mathematical point of view the encryption transformation $\hat{\mathbf{E}}$ is defined as a convex combination of unitary maps. Using the ancilliary system the encryption can be still defined only in terms of the system under consideration. Tracing out the ancilla we obtain a map $\hat{\mathbf{E}}_s$ with the action defined by $\hat{\mathbf{E}}_s[\rho] = \mathrm{Tr}_{anc}\hat{\mathbf{E}}[\rho \otimes \rho_{anc}]$. The usage of ancilla results in most general form of the quantum channel, i.e. $\hat{\mathbf{E}}_s[\rho] = \sum_i p_i \hat{\mathbf{G}}_i[\rho]$ with $\hat{\mathbf{G}}_i[\rho] = \mathrm{Tr}_{anc}[U_i \rho \otimes \rho_{anc} U^{\dagger}{}_i]$. However, for the decryption the ancilliary system is necessary. In this paper we will analyze PQC without additional ancillas, so the encryption is formally a convex combination of unitary transformations. It means the encryption is described by a unital completely positive map, i.e. it preserves the total mixture $\frac{1}{2}\mathbb{1}$.

Finally, we will introduce one definition and one theorem, which will be used through this paper.

Definition 2.2. Let $\mathbf{P} = \{\rho_i | i \in \mathbf{I}\}$, where $\mathbf{I}$ is an index set. We define the set $\overline{\mathbf{P}}$ as

$$\overline{\mathbf{P}} = \left\{ \rho = \sum_{i \in \mathbf{I}} \lambda_i \rho_i \middle| \rho_i \in \mathbf{P}, \lambda_i \in \mathbb{R}, \sum_{i \in \mathbf{I}} \lambda_i = 1 \right\}. \tag{3}$$

Especially in the case when $\mathbf{P} = \{\rho_1, \rho_2\}$ the set $\overline{\mathbf{P}}$ contains all operators of the form $\lambda\rho_1 + (1-\lambda)\rho_2$.

From now on we will denote the maximally mixed state[3] in $\overline{\mathbf{P}}$ as $\overline{\rho}$.

Theorem 2.3. *Let $[\mathbf{P}, \hat{\mathbf{E}}, \rho^{(0)}]$ be a PQC. Then $\hat{\mathbf{E}}(\rho) = \rho^{(0)}$ for any operator $\rho \in \overline{\mathbf{P}}$. Note that we are interested only in operators ρ with nonnegative eigenvalues, since the operators with negative eigenvalue(s) are not valid quantum states.*

Proof. The proof follows from the linearity of $\hat{\mathbf{E}}$. □

[3] I.e. the state nearest to the maximally mixed state $\frac{1}{2}\mathbb{1}$ according to the trace distance. It is also the nearest state in the Bloch ball.

3 Achievable states $\rho^{(0)}$

In this section we will derive several results on PQC on a single qubit. Our first question is 'What are the possible states $\rho^{(0)}$ given a specific set $\mathbf{P}$?'. In [1] it was proved that the only possible candidate for the state $\rho^{(0)}$ is $\frac{1}{2}\mathbb{1}$, whenever $\frac{1}{2}\mathbb{1}$ can be expressed as a convex combination of states from $\mathbf{P}$. We will generalize this result for any set $\mathbf{P}$ to calculate the minimal entropy of the key necessary and sufficient to encrypt a specific set $\mathbf{P}$.

All information about the action of $\hat{\mathbf{E}}$ we have is its behaviour on the set of plaintexts $\mathbf{P}$. Each element of this set is transformed into the fixed state $\rho^{(0)}$. This determines the channel $\hat{\mathbf{E}}$ completely, or incompletely depending on the set $\mathbf{P}$. However, in the case of incomplete specifications the choice of the channel $\hat{\mathbf{E}}$ has no impact on the security. Under the action of the channel $\hat{\mathbf{E}}$ each operator $\rho \in \overline{\mathbf{P}}$ is transformed into $\rho^{(0)}$. This follows directly from the linearity of the transformation $\hat{\mathbf{E}}$.

Let us assume a PQC given by operators $\{(p_i, U_i)\}_i$ with some $\rho^{(0)}$. By applying the unitary transformations $U'_i = VU_i$ (V is unitary) we obtain that $\sum_i p_i U'_i \rho U'^{\dagger}_i = \sum_i p_i V U_i \rho U_i^{\dagger} V^{\dagger} = V \rho^{(0)} V^{\dagger} = \rho'^{(0)}$ is fixed for all plaintext states. It follows that the unitarily transformed PQC is again a PQC with unitarily transformed average output state. Moreover, a convex combination of two PQC channels $\hat{\mathbf{E}}_1, \hat{\mathbf{E}}_2$ for the given set $\mathbf{P}$ is again a PQC channel for $\mathbf{P}$. In particular, $\hat{\mathbf{E}} = \pi_1 \hat{\mathbf{E}}_1 + \pi_2 \hat{\mathbf{E}}_2$ is PQC with $\rho^{(0)} = \pi_1 \rho_1^{(0)} + \pi_2 \rho_2^{(0)}$, i.e. $\hat{\mathbf{E}}[\rho] = \rho^{(0)}$ for all $\rho \in \mathbf{P}$. Thus, for a given set of plaintexts $\mathbf{P}$ the set of all possible private quantum channels is convex. The set of achievable states is convex as well. It is formed by orbits of states under the action of the whole unitary group.

For any TCP map $\hat{\mathbf{E}}$ the following inequality holds

$$D(\rho, \sigma) \geq D(\hat{\mathbf{E}}(\rho), \hat{\mathbf{E}}(\sigma)) \tag{4}$$

for the distance measure $D(\rho, \sigma) = \mathrm{Tr}|\rho - \sigma|$ on mixed states, i.e. two quantum states ρ, σ cannot become more distinguishable after applying a TCP transformation. We have already mentioned that we consider that the encryption superoperator $\hat{\mathbf{E}}$ is unital (we do not consider the ancilla here) and therefore from Eq. (4) we have

$$D\left(\rho, \frac{1}{2}\mathbb{1}\right) \geq D\left(\rho^{(0)}, \frac{1}{2}\mathbb{1}\right), \tag{5}$$

where $\rho \in \overline{\mathbf{P}}$ is any state in the set $\overline{\mathbf{P}}$ and $\rho^{(0)} = \hat{\mathbf{E}}(\rho)$ is fixed for all states $\rho \in \overline{\mathbf{P}}$. We use the fact that for unital maps $\hat{\mathbf{E}}[\frac{1}{2}\mathbb{1}] = \frac{1}{2}\mathbb{1}$. Especially this equation holds for the state $\overline{\rho}$, which is the most mixed density operator in $\overline{\mathbf{P}}$ (the nearest point to $\frac{1}{2}\mathbb{1}$ in the Bloch ball).

Therefore the condition is that given the set of plaintext states $\overline{\mathbf{P}}$ any achievable state $\rho^{(0)}$ fulfills the condition

$$D\left(\overline{\rho}, \frac{1}{2}\mathbb{1}\right) \geq D\left(\rho^{(0)}, \frac{1}{2}\mathbb{1}\right). \tag{6}$$

As a consequence, we obtain the result of [1] that the state $\rho^{(0)} = \frac{1}{2}\mathbb{1}$ whenever $\frac{1}{2}\mathbb{1}$ is contained in the convex span of the set $\mathbf{P}$.

Provided that the most mixed state $\overline{\rho}$ in $\overline{\mathbf{P}}$ is not $\frac{1}{2}\mathbb{1}$, the state $\rho^{(0)}$ must have the same or a smaller distance from $\frac{1}{2}\mathbb{1}$ than $\overline{\rho}$. This is the necessary condition each candidate to the state $\rho^{(0)}$ must obey. In this sense the set of potential candidates $\rho^{(0)}$ forms a ball within the Bloch ball, with the center in $\frac{1}{2}\mathbb{1}$ and the radius given by the distance of $\overline{\rho}$ and $\frac{1}{2}\mathbb{1}$. Let us denote this ball (set of allowed states) by b. This condition is necessary, it remains to verify whether it is also sufficient, i.e. whether for a given $\mathbf{P}$ and $\forall\ \rho^{(0)} \in b$ there exists a suitable TCP superoperator $\hat{\mathbf{E}}_{\rho^{(0)}}$, or equivalently whether the set of all achievable states coincides with those allowed by inequality (6).

In what follows we will analyze the achievability of $\rho^{(0)}$. Let us first consider two trivial cases. When $\mathbf{P}$ has only a single member, then there is nothing to encrypt. If the set $\mathbf{P}$ contains at least four linearly independent members, then $\overline{\mathbf{P}}$ already spans the whole Bloch ball and $\frac{1}{2}\mathbb{1} \in \overline{\mathbf{P}}$. It follows that the PQC maps all states to $\frac{1}{2}\mathbb{1}$, so the set of achievable states contains only single element. In subsequent sections we will analyze the remaining two cases: i) set $\overline{\mathbf{P}}$ is two-dimensional, and ii) set $\overline{\mathbf{P}}$ is three-dimensional.

In Sections 4–6 we will adopt analytical approach to prove that for all states $\rho^{(0)} \in b$ given a set of plaintext states $\mathbf{P}$ there exists a PQC sending the set $\mathbf{P}$ to $\rho^{(0)}$. In Section 7 we will analyze concrete PQC realizations as well as the minimal entropy of the key for a given set $\mathbf{P}$ and $\rho^{(0)}$. We will show an easily understandable geometrical method how to construct PQCs for encryption of the given set of plaintexts.

4 General remarks

In our analysis we will exploit the geometric picture of the Bloch ball (see Appendix). In both cases we will define specific representatives of the set of plaintexts $\overline{\mathbf{P}}$. We will choose the basis of the state space as four operators ξ_j represented by mutually orthogonal Bloch vectors $\vec{v}_j$. In particular, we will rotate the coordinate system (this rotation is just unitary change of the basis operators) to work with not necessarily positive, but trace-one operators

$$\begin{array}{rclcl} \xi_x & = & \frac{1}{2}(\mathbb{1} + \alpha S_x) & \leftrightarrow & \vec{v}_x = (\alpha, 0, 0) \\ \xi_y & = & \frac{1}{2}(\mathbb{1} + \beta S_y) & \leftrightarrow & \vec{v}_y = (0, \beta, 0) \\ \xi_z & = & \frac{1}{2}(\mathbb{1} + S_z) & \leftrightarrow & \vec{v}_z = (0, 0, 1) \\ \xi_0 & = & \frac{1}{2}\mathbb{1} & \leftrightarrow & \vec{v}_0 = (0, 0, 0) \end{array} \tag{7}$$

The S-basis is just a suitably rotated σ-basis (basis consisting of Pauli operators), i.e. $S_j = U\sigma_j U^\dagger$ for some unitary U.

This new operator basis shares all the properties of the original Pauli basis. In fact, the operators S_x, S_y, S_z specify only a rotated Cartesian coordinate system. Each private quantum channel $\hat{\mathbf{E}}$ induces a contraction of the given set $\overline{\mathbf{P}}$ into the state $\rho^{(0)}$. Our first aim is to explicitly specify the maximally mixed state in $\overline{\rho} \in \overline{\mathbf{P}}$. The second goal will be to show the achievability of this state, i.e. the construction of the PQC that transforms the whole set of plaintexts states into the state $\rho^{(0)}$ having the same mixedness (i.e. distance from $\frac{1}{2}\mathbb{1}$) as $\overline{\rho}$. In particular, $\rho^{(0)} = V\overline{\rho}V^{\dagger}$ (V is unitary). Let us denote by s the mixedness of $\overline{\rho}$. Then the PQC $\hat{\mathbf{E}}_{\rho^{(0)}}$ acts (in a suitably chosen basis) as follows: $\hat{\mathbf{E}}_{\rho^{(0)}}[\xi_j] = \rho^{(0)} = \frac{1}{2}(\mathbb{1} + s \cdot S_z)$ for all $\xi_j \in \overline{\mathbf{P}}$. Its action on the linear complement of $\overline{\mathbf{P}}$ must be defined in a way that the whole transformation is TCP. The existence of such PQC will be proved in subsequent sections.

5 Two states

Given two linearly independent states $\mathbf{P} = \{\rho_1, \rho_2\}$ the set $\overline{\mathbf{P}}$ defines a line crossing the Bloch sphere in two pure states, e.g. $|\psi_1\rangle, |\psi_2\rangle$. The mixedness of $\rho_\lambda = \lambda\rho_1 + (1-\lambda)\rho_2$ (i.e. the distance from the total mixture) is characterized by the length of the corresponding Bloch vector $\vec{r}_\lambda$. In particular, $|\vec{r}_\lambda|^2 = \lambda^2|\vec{r}_1|^2 + (1-\lambda)^2|\vec{r}_2|^2 + 2\lambda(1-\lambda)\vec{r}_1 \cdot \vec{r}_2$ can be easily minimized (with respect to λ) providing that we use two pure states $|\psi_j\rangle \leftrightarrow \vec{r}_j$. In this case $|\vec{r}_1| = |\vec{r}_2| = 1$ and $\vec{r}_1 \cdot \vec{r}_2 = |\vec{r}_1| \cdot |\vec{r}_2| \cos\theta$ with $\theta \in [0, \pi]$ being an angle between the vectors. The minimum we obtain by calculating the equation

$$\frac{d}{d\lambda}[\lambda^2 + (1-\lambda)^2 - 2\lambda(1-\lambda)\cos\theta] = 2(2\lambda - 1)(1 - \cos\theta) = 0 \tag{8}$$

The minimum is achieved for $\lambda = 1/2$, i.e. for the equal mixture of two pure states from $\overline{\mathbf{P}}$ and reads $|\vec{r}_{\min}| = \sqrt{\frac{1}{2}(1+\cos\theta)}$. For general (nonpure) states $\rho_1 \leftrightarrow \vec{r}_1$ and $\rho_2 \leftrightarrow \vec{r}_2$ the state $\rho_\lambda = \lambda\rho_1 + (1-\lambda)\rho_2$ is maximally mixed for the value $\lambda = (|\vec{r}_2|^2 - \vec{r}_1 \cdot \vec{r}_2)/|\vec{r}_1 - \vec{r}_2|^2$.

Let us assume that the state $|\psi_1\rangle$ corresponds to the North Pole of the Bloch ball and the y coordinate of $|\psi_2\rangle$ vanishes, i.e. we choose the operator basis S_x, S_y, S_z such that $|\psi_1\rangle\langle\psi_1| = \frac{1}{2}(\mathbb{1}+S_z)$ and $|\psi_2\rangle\langle\psi_2| = \frac{1}{2}(\mathbb{1}+\sin\theta S_x+\cos\theta S_z)$. In other words, the state $|\psi_2\rangle$ is represented by the vector $\vec{r}_2 = (\sin\theta, 0, \cos\theta)$. The norm of the vector $\vec{r}_\lambda$ is minimal for $\lambda_{\min} = 1/2$, i.e. $\vec{r}_{\min} = (\frac{1}{2}\sin\theta, 0, \frac{1}{2}(1+\cos\theta))$ with norm $|\vec{r}_{\min}| = \sqrt{\frac{1}{2}(1+\cos\theta)}$.

The possible quantum private channels form a set

$$\hat{\mathbf{E}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1-\cos\theta) & a & \frac{1}{2}\sin\theta \\ 0 & 0 & b & 0 \\ 0 & \frac{1}{2}\sin\theta & c & \frac{1}{2}(1+\cos\theta) \end{pmatrix} \tag{9}$$

and the complete positivity with respect to parameters a, b and c must be verified. Our aim is to find at least one valid TCP transformation. Therefore, let us consider that only the parameter b is nonvanishing[4] (i.e. we set $a = c = 0$).

[4] We will show that even in this particular case there exists a completely positive superoperator.

In this case the matrix is symmetric, so the singular values coincide with the eigenvalues that read

$$\{\lambda_1, \lambda_2, \lambda_3\} = \{1, b, 0\}. \tag{10}$$

The complete positivity constraint [13] requires the validity of the following inequalities

$$1 + \lambda_1 - \lambda_2 - \lambda_3 \geq 0 \quad \Rightarrow \quad b \leq 2 \tag{11}$$
$$1 - \lambda_1 + \lambda_2 - \lambda_3 \geq 0 \quad \Rightarrow \quad b \geq 0 \tag{12}$$
$$1 - \lambda_1 - \lambda_2 + \lambda_3 \geq 0 \quad \Rightarrow \quad b \leq 0 \tag{13}$$
$$1 + \lambda_1 + \lambda_2 + \lambda_3 \geq 0 \quad \Rightarrow \quad b \geq -2. \tag{14}$$

It turns out that the only possibility to satisfy these conditions is that the value of b must set to zero, i.e. $b = 0$. As a result, we get that the channel $\hat{\mathbf{E}}$ with $b = 0$ is for sure completely positive for all values of $\cos\theta$. Consequently, for two linearly independent states the derived bound on the choice of the state $\rho^{(0)}$ is achievable. The achievability of the states inside the ball b we obtain from the fact that the set of PQCs encrypting given set $\mathbf{P}$ is convex as well as the set of all achievable states, see Section 3. Later we will specify the unitary transformations forming the private quantum channel explicitly.

6 Three linearly independent states

In case the set $\mathbf{P} = \{\rho_1, \rho_2, \rho_3\}$ contains precisely three linearly independent states, the set $\overline{\mathbf{P}}$ forms a plane and valid quantum states from this plane (the intersection with the Bloch ball) form a circle c. Since all points of the ball b, containing all possible candidates for the state $\rho^{(0)}$, have the distance from $\frac{1}{2}\mathbb{1}$ the same or smaller than the most mixed state from c, it follows that the circle c touches the ball b precisely in the middle of the circle c. Moreover, this point $\overline{\rho} = \rho^{(0)}$ is the most mixed state from c.

To solve the general case explicitely, we will exploit the tools of analytic geometry. A plane determined by three points $A = \vec{r}_1$, $B = \vec{r}_2$, $C = \vec{r}_3$ reads $ax + by + cz + d = 0$, where

$$d = \det(\vec{r}_1\ \vec{r}_2\ \vec{r}_3) \tag{15}$$
$$a = \det(\vec{1}\ \vec{r}_2\ \vec{r}_3) \tag{16}$$
$$b = \det(\vec{r}_1\ \vec{1}\ \vec{r}_3) \tag{17}$$
$$c = \det(\vec{r}_1\ \vec{r}_2\ \vec{1}). \tag{18}$$

The symbol $\vec{1} = (1, 1, 1)^T$ denotes a column vector. The distance from the origin of the coordinate system (the total mixture) equals to

$$s = \frac{|d|}{\sqrt{a^2 + b^2 + c^2}}. \tag{19}$$

This number coincides (if $s \leq 1$) with the distance between the maximally mixed state $\overline{\rho} \in \overline{\mathbf{P}}$ and the total mixture. It follows that we can use directly the given set of plaintext states $\{\rho_1, \rho_2, \rho_3\}$ as the basis. However, for our purposes it will be useful to choose operators $\xi_1, \xi_2, \xi_3 \in \overline{\mathbf{P}}$ of the form given in Eq. (7). Let us assume that the set $\overline{\mathbf{P}}$ does not contain the total mixture. In this case

$$a = \beta \qquad b = \alpha \qquad c = d = \alpha\beta \tag{20}$$

and

$$s = |\vec{s}| = \frac{|\alpha\beta|}{\sqrt{\alpha^2\beta^2 + \beta^2 + \alpha^2}}. \tag{21}$$

The question is, whether the transformations $\xi_j \mapsto \rho^{(0)} = \frac{1}{2}(\mathbb{1} + s \cdot S_z) = \hat{\mathbf{E}}[\xi_j]$ is completely positive, or not. Due to the unitality of the PQC channels, the transformation $\hat{\mathbf{E}}$ is completely specified as

$$\hat{\mathbf{E}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & s/\alpha & s/\beta & s \end{pmatrix}. \tag{22}$$

Our task is only to verify the condition of complete positivity. The singular values of $\hat{\mathbf{E}}$ reads $\{\lambda_1, \lambda_2, \lambda_3\} = \{0, 0, s\sqrt{1 + \frac{1}{\alpha^2} + \frac{1}{\beta^2}}\}$. It follows that the map is completely positive if and only if $0 \leq 1 - s\sqrt{1 + \frac{1}{\alpha^2} + \frac{1}{\beta^2}}$. Inserting the derived result for the value of s into this complete positivity constraint, we find that it is always satisfied, because

$$0 \leq 1 - s\sqrt{1 + \frac{1}{\alpha^2} + \frac{1}{\beta^2}} = 1 - \frac{|\beta\alpha|}{\sqrt{\beta^2 + \alpha^2 + \beta^2\alpha^2}}\sqrt{\frac{\beta^2\alpha^2 + \alpha^2 + \beta^2}{\beta^2\alpha^2}} = 1 - 1 = 0. \tag{23}$$

As a result we obtain that it is always possible to define private quantum channel so that the norm bound is saturated and the state $\rho^{(0)} = \overline{\rho}$ is achievable. Let us note that the value of s is always less than 1, which is in agreement with the fact that $\rho^{(0)}$ is a quantum state (it belongs to the Bloch ball). The fact that for a given set of states $\mathbf{P}$ it is always possible to find a unital channel $\hat{\mathbf{E}}$ such that $\forall\ \rho \in \mathbf{P} : \hat{\mathbf{E}}(\rho) = \rho^{(0)}$, where $\rho^{(0)}$ is the closest state to the total mixture belonging to the linear span of the set $\mathbf{P}$, is interesting *per se*.

The case when $\rho^{(0)}$ lies inside (not on the surface) the ball b we obtain again from the convexity of the set of private quantum channels as discussed in Section 3.

7 Realizations of PQC and entropy of the key

So far, we studied the existence of PQC with states $\rho^{(0)}$ for a given set of plaintexts $\overline{\mathbf{P}}$. Next we will analyze the optimal realizations of these private quantum channels, i.e. we will ask the question: how many classical bits one needs to design the PQC. These classical bits represent the key that must be shared between sender and receiver to perfectly encrypt/decrypt the quantum states from plaintext. The efficiency of PQC is quantified by the entropy ($H(p) = -\sum_j p_j \log_2 p_j$) of the probability distribution of unitary transformations that specify the length of the shared classical key. It is known [1] that the ideal realization of PQC for general qubit states requires two bits. It is realized by arbitrary collection of four unitary transformations $\{U_k\}_k$ satisfying the following orthogonality condition $\mathrm{Tr}(U_j^\dagger U_k) = 2\delta_{jk}$. Each of these transformations is applied with the same probability $p = 1/4$, i.e. $H(p) = 2$.

Each private quantum channel $\hat{\mathbf{E}}$ is a convex combination of unitary transformations. Our task is to find a representation for arbitrary PQC, which is optimal. The action channel $\hat{\mathbf{E}}$ can be written in the form $\hat{\mathbf{E}}[\rho] = U\Phi_{\hat{\mathbf{E}}}[V\rho V^\dagger]U^\dagger$, where U, V are unitary transformations. For qubit unital channels the induced transformation $\Phi_{\hat{\mathbf{E}}}$ is diagonal, i.e. $\Phi_{\hat{\mathbf{E}}} = \mathrm{diag}\{1, \lambda_1, \lambda_2, \lambda_3\}$. It turns out that these transformations are of a simple form and can be written as convex combination of four Pauli transformations

$$\Phi_{\hat{\mathbf{E}}}[\rho] = p_0\rho + p_x\sigma_x\rho\sigma_x + p_y\sigma_y\rho\sigma_y + p_z\sigma_z\rho\sigma_z \tag{24}$$

Consequently, the original transformation $\hat{\mathbf{E}}$ is realized by four unitary transformations $W_j = U\sigma_j V$, i.e. $\hat{\mathbf{E}}[\rho] = \sum_j p_j W_j \rho W^\dagger{}_j$. Since the probabilities do not change, the PQCs $\hat{\mathbf{E}}$ and $\Phi_{\hat{\mathbf{E}}}$ can be realized with the same entropy. In fact, this holds in general: two unitarily equivalent PQCs can be always realized with the same efficiency, i.e. with the classical keys of the same entropy. Thus, it is sufficient to analyze the optimality of the realization of Pauli channels $\Phi_{\hat{\mathbf{E}}}$. Finding the singular values corresponding to $\hat{\mathbf{E}}$ we obtain the diagonal elements $\lambda_1, \lambda_2, \lambda_3$ of $\Phi_{\hat{\mathbf{E}}}$. The probabilities p_j are related to these values λ_k via the following equations

$$\begin{array}{rcl} p_x &=& \frac{1}{4}(1+\lambda_1-\lambda_2-\lambda_3) \\ p_y &=& \frac{1}{4}(1-\lambda_1+\lambda_2-\lambda_3) \\ p_z &=& \frac{1}{4}(1-\lambda_1-\lambda_2+\lambda_3) \\ p_0 &=& 1-p_x-p_y-p_z \end{array} \tag{25}$$

The entropy rate of the given PQC $H(\hat{\mathbf{E}}) = H(p)$, $p = \{p_j\}_j$, is given by the entropy of the distribution p. Let $\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$, where $\{|\psi_j\rangle\}_j$ is a set of not necessarily orthogonal quantum states. It follows that $S(\rho) = S(\sum_j p_j|\psi_j\rangle\langle\psi_j|) \leq H(p)$ and the inequality is saturated if and only if $\{|\psi_j\rangle\}_j$ are mutually orthogonal. Let us consider any pure plaintext state $|\psi\rangle$ and let $|\psi_j\rangle = U_j|\psi\rangle$. It is clear that

$$S(\hat{\mathbf{E}}(|\psi\rangle\langle\psi|)) = S(\rho) = S\left(\rho^{(0)}\right) \leq H(p). \tag{26}$$

Therefore the entropy of the encryption operation can always be bounded from below by the entropy of $\rho^{(0)}$ as long as $\overline{\mathbf{P}}$ contains at least one pure state. This always holds in the case of qubit, however, not in general for systems of larger dimension. In example in the case of two qubits we can define the set

$\mathbf{P} = \{1/4\mathbb{1}, 1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)\}$. It is clear that $\overline{\mathbf{P}}$ contains no pure state, it is encrypted by the superoperator

$$\{(1/2, \mathbb{1}), (1/2, \mathbb{1} \otimes \sigma_x)\} \tag{27}$$

and $\rho^{(0)} = \frac{1}{4}\mathbb{1}$.

The limit (26) is saturated only if the encoding operators U_j generate mutually orthogonal (noncommuting) states (ciphertexts) for each given plaintext. In particular, if we consider a PQC for all possible states of a qubit, this limit can be achieved only (up to unitary equivalence) by encoding with the identity and the *universal NOT* operation. However, this map is not completely positive, and therefore unphysical [7].

Next we shall study the realization of PQC when the set of plaintexts is two-dimensional and three-dimensional, respectively, and the state $\rho^{(0)}$ is the maximally mixed one from the set $\overline{\mathbf{P}}$. For two-dimensional set of plaintexts the induced transformation is $\Phi_{\hat{\mathbf{E}}} = \mathrm{diag}\{1, 0, 0, 1\}$, i.e. $\lambda_1 = \lambda_2 = 0$ and $\lambda_3 = 1$. It follows that

$$\Phi_{\hat{\mathbf{E}}}[\rho] = \frac{1}{2}\rho + \frac{1}{2}\sigma_z\rho\sigma_z \tag{28}$$

and one bit is sufficient for encoding.

One can specify the precise form of unitary transformations, but the explicit calculation is quite lengthy. Instead, we will use the geometric picture of Bloch sphere to guess the unitaries.

Two states

Let us suppose that the set $\mathbf{P} = \{\rho_1, \rho_2\}$ has only two (linearly independent) states. By Theorem 2.3 it also encrypts any state on the line segment $l \subseteq \overline{\mathbf{P}}$ defined by the points corresponding to the states ρ_1 and ρ_2 in the Bloch ball. Let us choose the state $\rho^{(0)}$ as the point where the line segment l touches the ball[5] b (see fig. 2), i.e. $\rho^{(0)} = \overline{\rho}$. It is clear that this point is in the center of the line segment l, since the extremal points of this line segment are on the surface of the Bloch ball.

We will design a specific superoperator $\hat{\mathbf{E}}$, which encrypts this line segment to the state $\rho^{(0)}$. This superoperator can be realized using two unitary operators with uniform distribution,

$$\hat{\mathbf{E}}(\rho) = \frac{1}{2}\mathbb{1}\rho\mathbb{1} + \frac{1}{2}U\rho U^\dagger, \tag{29}$$

where U is the unitary operation, which realizes the rotation of the Bloch ball by 180 degrees around the axis intersecting points $\rho^{(0)}$ and $\frac{1}{2}\mathbb{1}$. It is easy to see that such a superoperator takes any state ρ from l to a convex combination of the original state ρ and the state which lies on the line l in the same distance from

[5] Of possible candidates to the state $\rho^{(0)}$.

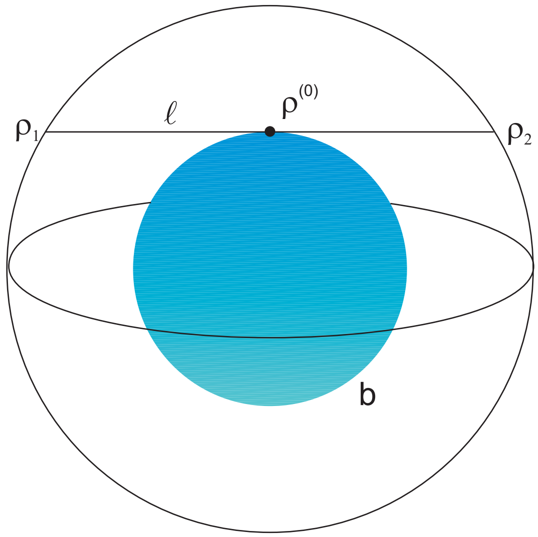

Figure 2: Encrypting line segment l.

$\rho^{(0)}$, but on the opposite half line (starting in the point $\rho^{(0)}$). The consequence is that the convex combination

$$\frac{1}{2}\rho + \frac{1}{2}U\rho U^\dagger = \rho^{(0)}. \tag{30}$$

The way to achieve any other point lying on the surface of the ball b is straightforward. For any such point $\rho'^{(0)}$ there exists a two dimensional rotation $R_{\rho^{(0)},\rho'^{(0)}}$, which rotates the point $\rho^{(0)}$ to the point $\rho'^{(0)}$. This rotation is realized by some unitary operation $U_{\rho^{(0)},\rho'^{(0)}}$ on the density operators. Therefore, the superoperator encrypting the whole line segment l into the point $\rho'^{(0)}$ is

$$\hat{\mathbf{E}}(\rho) = \frac{1}{2}U_{\rho^{(0)},\rho'^{(0)}}\mathbb{1}\rho\mathbb{1}U^\dagger{}_{\rho^{(0)},\rho'^{(0)}} + \frac{1}{2}U_{\rho^{(0)},\rho'^{(0)}}U\rho U^\dagger U^\dagger{}_{\rho^{(0)},\rho'^{(0)}}. \tag{31}$$

This superoperator has again Kraus decomposition with only two unitary operators, and therefore only a single bit of key is needed. The method how to achieve any $\rho'^{(0)} \in b$ (not only on the surface) is based on the method of encryption of three linearly independent states and will be discussed later in this section.

In this way we have demonstrated that one bit of key is sufficient to encrypt set $\mathbf{P}$ containing two linearly independent states. It remains to verify whether one bit is also necessary. There might e.g. exist some encryption operation $\{(p_1, U_1), (p_2, U_2)\}, p_1 + p_2 = 1, p_1 \neq p_2$ encrypting the set $\mathbf{P}$. Clearly the entropy of the key of such an operation is smaller than one. We will prove that one bit is necessary by showing that any encryption superoperator $\hat{\mathbf{E}}$ encrypting a line l encrypts also the line l', which is parallel to l and intersects $\frac{1}{2}\mathbb{1}$. Then the

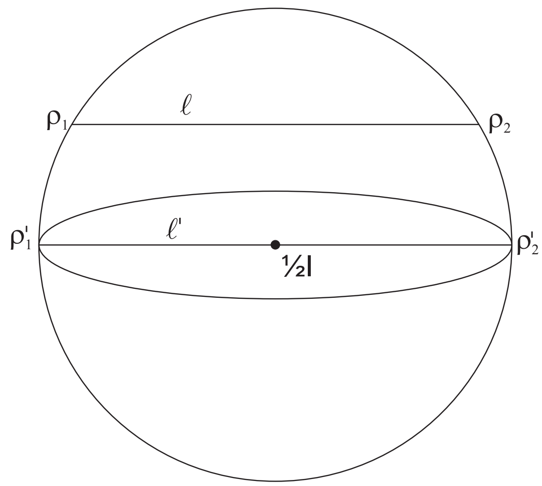

Figure 3: Encryption of l encrypts also l'.

derived inequality (26) implies that one bit is indeed necessary, since $S(\frac{1}{2}\mathbb{1}) = 1$. Also, $\hat{\mathbf{E}}$ can be used to encrypt a classical bit ($\{|0\rangle, |1\rangle\}$) and this result is in accordance with [26].

Let us denote ρ_1 and ρ_2 the extremal points of the line segment l (lying on the surface of the Bloch ball, see figure 3) and ρ_1' and ρ_2' the extremal points of the line segment l'. Let us express each of the points ρ_1' and ρ_2' as a linear combination of the points ρ_1, ρ_2 and $\frac{1}{2}\mathbb{1}$. It is easy to see that the coordinates of the points satisfy

$$\rho_1' = x\rho_1 + y\rho_2 + z\frac{1}{2}\mathbb{1} \quad \Leftrightarrow \quad \rho_2' = y\rho_1 + x\rho_2 + z\frac{1}{2}\mathbb{1}. \tag{32}$$

This relation holds for extremal points of any line segment parallel to l and lying in the plane spanned by l and $\frac{1}{2}\mathbb{1}$. Let $\hat{\mathbf{E}}$ encrypts l to some state $\rho^{(0)}$. Then from linearity and unitality of $\hat{\mathbf{E}}$ we obtain

$$\hat{\mathbf{E}}(\rho_1') = x\hat{\mathbf{E}}(\rho_1) + y\hat{\mathbf{E}}(\rho_2) + z\frac{1}{2}\mathbb{1} = y\hat{\mathbf{E}}(\rho_1) + x\hat{\mathbf{E}}(\rho_2) + z\frac{1}{2}\mathbb{1} = \hat{\mathbf{E}}(\rho_2') \tag{33}$$

since $\hat{\mathbf{E}}(\rho_1) = \hat{\mathbf{E}}(\rho_2) = \rho^{(0)}$ from assumption that $\hat{\mathbf{E}}$ encrypts l. It follows that $\hat{\mathbf{E}}$ encrypts any line segment parallel to l lying in the plane spanned by l and $\frac{1}{2}\mathbb{1}$.

From Eq. (33) we can also easily determine the state $\rho'^{(0)} = \hat{\mathbf{E}}(\rho_1')$, i.e. the state where $\hat{\mathbf{E}}$ sends the line segment l'. It is the state $\rho^{(0)}$ shifted towards $\frac{1}{2}\mathbb{1}$, from the equation

$$\hat{\mathbf{E}}(\rho_1') = x\hat{\mathbf{E}}(\rho_1) + y\hat{\mathbf{E}}(\rho_2) + z\frac{1}{2}\mathbb{1} = (x+y)\rho^{(0)} + z\frac{1}{2}\mathbb{1}. \tag{34}$$

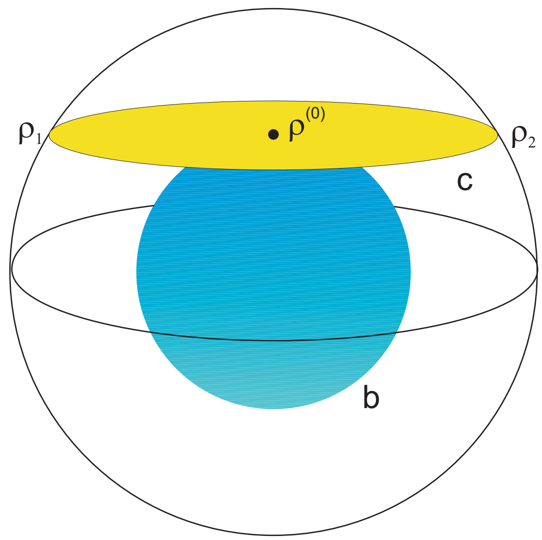

Figure 4: Encryption of the circle c.

The ratio between $(x+y)$ and z determines the distance from $\frac{1}{2}\mathbb{1}$.

We can also derive an analogical result for PQC encrypting a circle in the Bloch sphere. In this case the fact that it also encrypts all parallel circles implies that this PQC establishes an approximative encryption of the whole Bloch sphere, as defined in [18]. Also, in general, PQC encrypting any set $\overline{\mathbf{P}}$ in any Hilbert space encrypts also all spaces parallel in the superplane spanned by $\overline{\mathbf{P}}$ and $\frac{1}{d}\mathbb{1}$. This will be discussed in detail in a separate paper.

Three states

In case the set $\mathbf{P}$ contains precisely three linearly independent states ρ_1, ρ_2, ρ_3, their linear span is a plane and valid quantum states from this plane (the intersection with the Bloch ball) form a circle c (see figure 4). Since all points of the ball b, containing all possible candidates for the state $\rho^{(0)}$, have the distance from $\frac{1}{2}\mathbb{1}$ the same or smaller than the most mixed state from c, it follows that the circle c touches the ball b precisely in the middle of the circle c. Moreover, this point $\overline{\rho} = \rho^{(0)}$ is the most mixed state from c.

Following analogical argumentation as in the case of the two states, we construct the TCP superoperator, which encrypts the whole circle and sends it to $\rho^{(0)}$. This superoperator is the same as in the case of two states, it is the superoperator (29). The operator U is the rotation around the axis of the circle c. The saturation of any other point on the surface of the ball b is the same as in the case of two states, see Eq. (31).

Using this result we may also design a PQC, which encrypts a set $\mathbf{P}$ of two linearly independent states into the arbitrary state $\rho^{(0)}$ inside the ball b

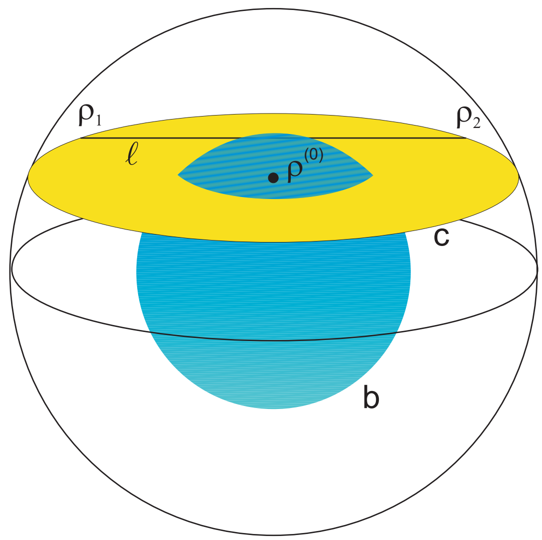

Figure 5: Encryption of the line l with $D(\rho^{(0)}, 1/2\mathbb{1}) < D(\overline{\rho}, 1/2\mathbb{1})$.

by using just single bit of key. The ball b is now specified by the given line l associated with the set $\overline{\mathbf{P}}$. The state $\rho^{(0)}$ specifies uniquely a sphere g of the radius $r = D(\rho^{(0)}, \frac{1}{2}\mathbb{1})$, centered in total mixture and containing this state on its surface. There exists a tangent plane κ to this sphere determined by the original line l. This plane is generated by three linearly independent states and following the reasoning of this subsection, it can be encrypted into its maximally mixed state by PQC with $H(\hat{\mathbf{E}}) = 1$. However, the maximally mixed state equals to the only point in the intersection of the plane with the sphere (see figure 5). This point is unitarily equivalent to $\rho^{(0)}$. It means that the original set $\overline{\mathbf{P}}$ given by two linearly independent states (forming the line in the plane, $l \in \kappa$) is encrypted by the same PQC (up to unitary transformation) into the state $\rho^{(0)}$.

Let us now proceed with the analytic approach to see how large key is required to encrypt the set $\overline{\mathbf{P}}$ into arbitrary state $\rho^{(0)} \in b$. For three-dimensional set of plaintexts we have a unique PQC that transforms $\overline{\mathbf{P}}$ into the state $\rho^{(0)}$. The singular values of the corresponding mapping $\hat{\mathbf{E}}$ reads $\{\lambda_1, \lambda_2, \lambda_3\} = \{0, 0, s\sqrt{1 + \frac{1}{\alpha^2} + \frac{1}{\beta^2}}\}$. It follows that

$$\begin{aligned} p_0 = p_z &= (1 + s\sqrt{1 + \tfrac{1}{\alpha^2} + \tfrac{1}{\beta^2}})/4 \\ p_x = p_y &= (1 - s\sqrt{1 + \tfrac{1}{\alpha^2} + \tfrac{1}{\beta^2}})/4 \end{aligned} \tag{35}$$

The parameter s corresponds to the distance between the state $\rho^{(0)}$ and the total mixture. It is bounded by the inequality $s \leq \frac{|\alpha\beta|}{\sqrt{\alpha^2\beta^2 + \alpha^2 + \beta^2}}$. Except the case when this inequality is saturated we need four unitary transformations to realize the PQC. For maximal value of s two unitary transformations are sufficient. Moreover, they are used with equal probabilities. It means that the limiting case ($\rho^{(0)} = \overline{\rho}$) for two-dimensional and three-dimensional set of plaintexts has the same entropy rates.

If you examine the dependence of the probabilities $\{p_i\}_i$ on the parameter s, then you realize that to encrypt three states a single bit of key is sufficient if $\rho^{(0)}$ is on the surface of the ball b (see the beginning of this section). However, as the state $\rho^{(0)}$ is getting closer to $\frac{1}{2}\mathbb{1}$, the entropy of the key grows up to two bits.

The key question is whether the derived bound on entropy of PQC encrypting the given set of three linearly independent states is also necessary, i.e. whether it is possible for given $\mathbf{P}$ and $\rho^{(0)}$ design a PQC with lower entropy of key than in the derived example. Let us recall the proof that one bit of key is necessary to encrypt the set of two linearly independent plaintexts, see Section 5. It immediately follows that one bit is also necessary to encrypt plaintext containing at least three linearly independent states.

The final step is to prove that also the entropy of the private quantum channel encrypting three dimensional set $\mathbf{P}$, with $D(\rho^{(0)}, \frac{1}{2}\mathbb{1}) < D(\overline{\rho}, \frac{1}{2}\mathbb{1})$, realized using the Pauli channel is minimal. Let us introduce the entropy exchange $S_{ex}(\rho_A, \hat{\mathbf{E}})$ [22] as the quantity measuring the part of quantum information which is lost into the environment under the action of the channel $\hat{\mathbf{E}}$ providing that the system is initially prepared in the state ρ_A. Provided that the channel $\hat{\mathbf{E}}$ on the system A is realized using unitary operation G on a larger system AE, where E is the environment, the entropy of exchange is defined as the von Neumann entropy of the reduced density matrix of the environment after applying the operation G. It turns out that this entropy is independent of concrete realization of the superoperator.

In particular, any channel $\hat{\mathbf{E}}$ has unitary representation $\hat{\mathbf{E}}[\rho_A] = \mathrm{Tr}_E[G(\rho_A \otimes |0\rangle\langle 0|)G^\dagger] = \sum_j A_j \rho_A A^\dagger{}_j$ with $G = \sum_j A_j \otimes |j\rangle\langle 0|$. It is known that the entropy of the environment state $\omega_E = \mathrm{Tr}_A[G(\rho_A \otimes |0\rangle\langle 0|)G^\dagger] = \sum_{jk} \mathrm{Tr}[A_j \rho_A A^\dagger{}_k]|j\rangle\langle k|$ does not depend on the particular Kraus representation.

In our case this function is the lower bound of the entropy of the key $H(\{p_k\}_k)$, i.e. $H(\{p_k\}_k) \geq \max_{\rho_A} S_{ex}(\rho, \hat{\mathbf{E}})$. This inequality follows from the fact that $S(\omega_E) \leq S(\mathrm{diag}_{\mathcal{B}}[\omega_E])$[6] (definition of von Neumann entropy as minimum of Shannon entropy ovel all measurements) and for PQC channels we have $\mathrm{diag}_{\mathcal{B}}[\omega_E] = \sum_k p_k \mathrm{Tr}[U_k \rho_A U^\dagger{}_k]|k\rangle\langle k|$. Using the the trace properties and normalization of ρ_A we obtain $\mathrm{diag}_{\mathcal{B}}[\omega_E] = \{p_k\}_k$, i.e. $S(\mathrm{diag}_{\mathcal{B}}[\omega_E]) = H(\{p_k\}_k)$.

In what follows we will show that for qubit the inequality is saturated for decomposition into orthogonal unitaries, i.e. for Pauli channels. From the previous paragraph it is clear that it is sufficient to show that for some ρ the induced enviroment state ω_E is diagonal. Hence, we have to verify the conditions under which the identity $\mathrm{Tr}[U_j \rho U^\dagger{}_k] = 0$ holds for $j \neq k$. In such case the inequality is saturated. It is easy to see that by choosing $\rho = \frac{1}{2}\mathbb{1}$ this is the condition for

[6] The $\mathrm{diag}_{\mathcal{B}}[\omega_E]$ is the all-zero matrix except for the diagonal elements, which are equal to diagonal elements of ω_E in the basis $\mathcal{B}$.

orthogonality of transformations U_j and this justifies our statement.

We have shown that for orthogonal decomposition of the channel $\hat{\mathbf{E}}$ the entropy of the inequality is saturated, i.e. entropy of the key equals to entropy exchange and this is indeed the maximal value of entropy exchange. Fortunately, the entropy exchange does not depend on the particular decomposition and therefore the entropy of the key cannot be lower for another decompositions. It turns out that for qubits any unital channel can be written as a convex combination of orthogonal unitaries. However, for larger systems this is not the case in general. Consequently, the qubit PQC channel with minimal entropy of the key is the one with orthogonal encoding operations, i.e. the corresponding Pauli channel $\Phi_{\hat{\mathbf{E}}}$.

The necessary and sufficient entropy of the key is 1 when $\rho^{(0)} = \overline{\rho}$ and it grows up to 2 bits as the state $\rho^{(0)}$ approaches $\frac{1}{2}\mathbb{1}$. Therefore, it is natural to express the entropy as a function of the parameter

$$r = \frac{D(\rho^{(0)}, 1/2\mathbb{1})}{D(\overline{\rho}, 1/2\mathbb{1})}, \tag{36}$$

where the radius of the Bloch ball is 1.

Let us use the parametrization of states $\rho_1, \rho_2, \rho_3 \in \mathbf{P}$ introduced in the Eq. (7) and put $s = D(\rho^{(0)}, 1/2\mathbb{1})$ and $p = D(\overline{\rho}, 1/2\mathbb{1}) = |\alpha\beta|/\sqrt{1+\alpha^2+\beta^2}$. Comparing it with the Eq. (35) we obtain that the probabilites reads $p_0 = p_z = \frac{1}{4}(1+r)$ and $p_x = p_y = \frac{1}{4}(1-r)$, where we used the relation $r = s/p$. The evaluation of the entropy for this realization of PQC channel leads us to formula

$$H(\{p_j\}_j) = -\sum_j p_j \log_2 p_j = 2 - \frac{1}{2}\left[(1+r)\log_2(1+r) + (1-r)\log_2(1-r)\right], \tag{37}$$

where $0 \leq r \leq 1$. It is easy to see that $1 \leq H(\{p_j\}_j) \leq 2$. The graph of the function $H(\{p_j\}_j)$ depending on the variable r is on the Figure 6. Unfortunately, as we see from the graph, the entropy grows very fast as r goes to 0. In example for $r = 1/2$ the entropy is already $H(\{p_j\}_j) \approx 1.81128$.

8 Conclusion

All single-qubit private quantum channels

In this paragraph we will answer the following question: which unital maps constitute a PQC? We have shown that it is sufficient to consider only Pauli channels, i.e. the maps $\Phi_{\hat{\mathbf{E}}} = \mathrm{diag}\{1, \lambda_1, \lambda_2, \lambda_3\}$. Nontrivial private quantum channels are characterized by the property, that at least two pure states $|\psi_1\rangle, |\psi_2\rangle$ are mapped into the same state $\rho^{(0)}$. In the Bloch sphere parametrization ($\vec{r} = (r_x, r_y, r_z)$) this means that $\vec{r}_1 \mapsto \vec{r}_1' = \vec{s}$ and $\vec{r}_2 \mapsto \vec{r}_2' = \vec{s}$. Using these relations and explicit form of the Pauli channel we come to the following "PQC"

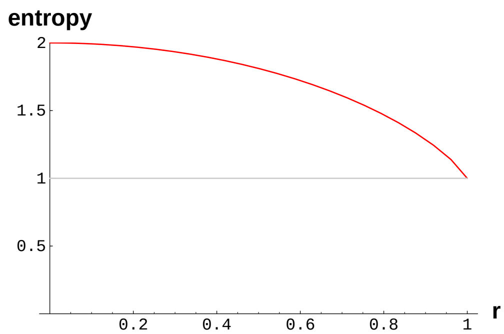

Figure 6: Dependency of the entropy on the variable r.

conditions $0 = \vec{r}_1' - \vec{r}_2'$, i.e. $\lambda_j(r_{1j} - r_{2j}) = 0$ for all components $j = x, y, z$. This equality is satisfied only if $\lambda_j = 0$ for some j, or $r_{1j} = r_{2j}$. Consider the case when none of the λs vanishes, i.e. $\lambda_1\lambda_2\lambda_3 \neq 0$. It follows that in order to fulfill the PQC conditions $r_{1j} = r_{2j}$ for every j. But it means that the states are the same. Therefore, at least one of the parameters λ_j must vanish. Otherwise the transformation does not correspond to private quantum channel. The complete positivity condition restricts the possible values of λ_1, λ_2 (we put $\lambda_3 = 0$) so that the inequality $|\lambda_1 \pm \lambda_2| \leq 1$ characterize all the possible qubit private quantum channels.

Multi-qubit generalization

This result can be generalized for a specific class of multi-qubit states. In each of the n qubits we choose a set of plaintexts $\overline{\mathbf{P}}_k$ in the corresponding Bloch ball. Each of the qubits can be encoded by PQC $\hat{\mathbf{E}}_k : \overline{\mathbf{P}}_k \mapsto \rho_k^{(0)}$. Following the single qubit results, we design a PQC on each of the qubits, which encrypts any state of the form

$$\sum_i \mu_i \rho_1^{(i)} \otimes \cdots \otimes \rho_n^{(i)}, \tag{38}$$

where $\forall i : \mu_i \in \mathbb{R}$, $\sum_i \mu_i = 1$ and $\forall i, k : \rho_k^{(i)} \in \overline{\mathbf{P}}_k$. Let us denote the set of such states by $\overline{\mathbf{P}}$. Note note that this set contains entangled states as well, because not only convex combinations of factorized states are allowed. The values of μ_i are arbitrary. Consider for instance two qubits. Using PQC encryption for $\mathbf{P} = \mathcal{S}(\mathcal{H})$ on each qubit enables us to encrypt each two-qubit (even entangled) quantum state.

Other implications

In this paper we derived the restriction that the state $\rho^{(0)}$ of the private quantum channel can be any state which has the distance from the maximally mixed state $\frac{1}{2}\mathbb{1}$ the same or smaller than the state $\overline{\rho}$, where $\overline{\rho}$ denotes the most mixed state in the linear span of $\mathbf{P}$. We showed that any of these states can be achieved in the case of the qubit and therefore this condition is also sufficient.

Further, we demonstrated that it is enough to use a single bit of key to encrypt the set $\overline{\mathbf{P}}$, which is spanned by two linearly independent states, and that any state of the previously described candidates to the state $\rho^{(0)}$ can be achieved. We derived the same result for the set $\overline{\mathbf{P}}$ containing three linearly independent states, but with the restriction that a single bit of the key suffices provided that the state $\rho^{(0)}$ has the same distance from $1/2\mathbb{1}$ as the state $\overline{\rho}$. As the distance of the state $\rho^{(0)}$ to $\frac{1}{2}\mathbb{1}$ approaches 0, the necessary and sufficient entropy of the key approaches 2.

As a special consequence of our derivation we obtain the result of [1] that the state $\rho^{(0)} = \frac{1}{2}\mathbb{1}$ when $\frac{1}{2}\mathbb{1}$ is in the convex span of $\mathbf{P}$ and two bits of the key are needed to encrypt a qubit. Another special consequence of the above derivations is the result of [1] that to encrypt real combinations of two orthogonal basis states it is necessary and sufficient to use a single bit of key. These real combinations form a circle on the surface of the Bloch ball with center coinciding with the center of the Bloch ball.

Moreover, from the discussion in Section 6 it follows that the impossibility of universal not operation on qubit [7, 8] can be derived from the fact that one bit of the key is not sufficient to encrypt a qubit.

Acknowledgements

Support of the project GAČR GA201/01/0413 is acknowledged. M.Z. acknowledges the support of the Slovak Academy of Sciences via the project CE-PI and of project INTAS (04-77-7289).

A Bloch sphere and qubit channels

Qubit (two-dimensional quantum system) provides us a very simple and illustrative picture of the state space. Any state can be expressed as a linear combination of the operators $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$. In particular, each operator $\rho = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})$ has a unit trace and if $|\vec{r}| \leq 1$, then it is also positive. Consequently, the state space forms a ball with the unit radius. The equivalence $\rho \leftrightarrow \vec{r}$ is called *Bloch sphere representation* (see for instance Refs. [22, 24]). From the orthogonality relation $\mathrm{Tr}\sigma_k\sigma_l = 2\delta_{kl}$ the parameters of state are given by a simple formula $\vec{r} = \mathrm{Tr}\rho\vec{\sigma}$, i.e. as the mean values of the hermitian operators (measurements) $\sigma_x, \sigma_y, \sigma_z$.

Let us describe the relation between the density operators $\mathcal{S}(\mathcal{H})$ (three-parametric subset) embedded in four-dimensional space of Hermitian operators and the Bloch sphere contained in three-dimensional space. Let us denote by ρ_j $(j = 1, 2, 3, 4)$ the basis of this space corresponding to four density operators. The vectors $\vec{r}_j$ represents the associated points in the Bloch sphere (in three dimensional real vector space). Only *trace-preserving linear combinations*, i.e.

$\rho = \sum_j a_j \rho_j$ with $\sum_j a_j = 1$ for real a_j, can be understand as linear combinations of the vectors within the Bloch sphere picture, i.e. $\vec{r} = \sum_j a_j \vec{r}_j$. In fact, Bloch sphere is situated in the three-dimensional space of Hermitian operators with unit trace, but only special linear combinations ($\sum_j a_j = 1$) of Bloch vectors has its counterparts in the original space of Hermitian operators.

The structure of qubit channels is known mainly due to work of Ruskai *et al.* [20, 25]. Let us now briefly present a corresponding geometrical picture. From the mathematical point of view [22, 24] the channels are described by linear trace-preserving completely positive maps $\hat{\mathbf{E}}$ defined on the set of operators. The complete positivity is guaranteed if the operator $\Omega_{\hat{\mathbf{E}}} = (\hat{\mathbf{E}} \otimes \mathbb{1})P_+$ is a valid quantum state[7]. Any qubit channel $\hat{\mathbf{E}}$ can be illustrated as an affine transformation of the Bloch vector $\vec{r}$, i.e. $\vec{r} \mapsto \vec{r}' = T\vec{r} + \vec{t}$, where T is a real 3x3 matrix and $\vec{t}$ is a translation. This form guarantees that the transformation $\hat{\mathbf{E}}$ is hermitian and trace preserving, but the complete positivity conditions define (nontrivial) constraints on possible values of parameters. In fact, the set of all completely positive trace-preserving maps forms a specific convex subset of all affine transformations.

Any matrix T can be written in the so-called singular value decomposition, i.e. $T = R_U D R_V$ with R_U, R_V corresponding to orthogonal rotations and $D = \mathrm{diag}\{\lambda_1, \lambda_2, \lambda_3\}$ being diagonal with λ_k the singular values of T. This means that any map $\hat{\mathbf{E}}$ is a member of less-parametric family of maps of the "diagonal form" $\Phi_{\hat{\mathbf{E}}}$. In particular $\hat{\mathbf{E}}[\rho] = U\Phi_{\hat{\mathbf{E}}}[V\rho V^\dagger]U^\dagger$ with U, V unitary operators. The reduction of parameters is very helpful, and most of the properties (also complete positivity) of $\hat{\mathbf{E}}$ is reflected by the properties of $\Phi_{\hat{\mathbf{E}}}$. The map $\hat{\mathbf{E}}$ is completely positive only if $\Phi_{\hat{\mathbf{E}}}$ is. Let us note that $\Phi_{\hat{\mathbf{E}}}$ is determined not only by the matrix D, but also by a new translation vector $\vec{\tau} = R_U \vec{t}$, i.e. under the action of the map $\Phi_{\hat{\mathbf{E}}}$ the Bloch sphere transforms as follows $r_j \mapsto r'_j = \lambda_j r_j + \tau_j$.

A special type of completely positive maps are the unital ones, i.e. those for which the total mixture (center of the Bloch sphere) is preserved. For these channels the translation term vanishes, $\vec{t} = \vec{\tau} = \vec{0}$, and the Bloch sphere is "shrinked" without shifting its center. In this case the analysis of all possible channels is quite simple, because the induced map $\Phi_{\hat{\mathbf{E}}}$ is uniquely specified only by three real parameters. Positivity of the transformation $\Phi_{\hat{\mathbf{E}}}$ corresponds to conditions $|\lambda_k| \leq 1$, i.e. all points lying inside a cube. The conditions of complete positivity [20, 25] demands the validity of the following four inequalities $|\lambda_1 \pm \lambda_2| \leq |1 \pm \lambda_3|$. This specifies the tetrahedron lying inside a cube of all positive unital maps with extremal points being four unitary transformations $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$.

It follows that each unital map is unitarily equivalent to the map of the form $\Phi_{\hat{\mathbf{E}}} = \mathrm{diag}\{1, \lambda_1, \lambda_2, \lambda_3\}$. The set of all unital channels is convex. Obviously the unitary channels are extremal points of this set. Let us consider a Pauli channel $\hat{\mathbf{P}}[\rho] = \sum_k p_k \sigma_k \rho \sigma_k$, i.e. a general convex combination of four Pauli unitary transformations. Rewriting this action in the Bloch sphere parameters

[7] P_+ is a projection onto maximally entangled state $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

we obtain the transformation

$$\hat{\mathbf{P}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-2(p_y+p_z) & 0 & 0 \\ 0 & 0 & 1-2(p_x+p_z) & 0 \\ 0 & 0 & 0 & 1-2(p_x+p_y) \end{pmatrix}. \qquad (39)$$

As a result we get that unital channels are unitarily equivalent to Pauli channel. Consequently, each unital channel $\hat{\mathbf{E}}$ can be written as a convex combination of (at least) four unitary channels. The probabilities are determined by the parameters of the induced map $\Phi_{\hat{\mathbf{E}}}$

$$\begin{aligned} p_x &= \tfrac{1}{4}(1+\lambda_1-\lambda_2-\lambda_3) \\ p_y &= \tfrac{1}{4}(1-\lambda_1+\lambda_2-\lambda_3) \\ p_z &= \tfrac{1}{4}(1-\lambda_1-\lambda_2+\lambda_3) \\ p_0 &= 1-p_x-p_y-p_z. \end{aligned} \qquad (40)$$

Unitary channels are rotations of the Bloch sphere. Unital channels are rotations combined with the deformation so that the output states form an ellipsoid centered in the total mixture. The values λ_j define the size of the ellipsoid along three main axes.

References

[1] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *FOCS 2000*, pages 547–553, 2000. quant-ph/0003101.

[2] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *FOCS 2002*, 2002. quant-ph/0205128.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, 1984.

[4] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 351–366, 1991.

[5] J. Bouda. *Encryption of quantum information and quantum cryptographic protocols*. PhD thesis, Faculty of Informatics, Masaryk University, september 2004.

[6] P. O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. quant-ph/0003059, 2000.

[7] V. Bužek, M. Hilery, and R. F. Werner. Optimal manipulations wih qubits: Universal not gate. *Phys. Rev. A*, 60:R2626–R2629, 1999.

[8] V. Bužek, M. Hilery, and R. F. Werner. Universal not gate. *J. Mod. Opt.*, 47:211–232, 2000.

[9] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 85:648–651, 1999. quant-ph/9901025.

[10] C. Crépeau. Quantum oblivious transfer. *J. Mod. Opt.*, 41(12):2445–2454, 1994.

[11] D. P. DiVincenzo, P. Hayden, and B. M. Terhal. Hiding quantum data. *Found. Phys.*, 33(11):1629–1647, 2003. quant-ph/0207147.

[12] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[13] A. Fujiwara and P. Algoet. One-to-one parametrization of quantum channels. *Phys. Rev. A*, 59(5):3290–3294, 1999.

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. quant-ph/0101098, 2001.

[15] D. Gottesman. On the theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, 2000. quant-ph/9910067.

[16] D. Gottesman and H.-K. Lo. From quantum cheating to quantum security. *Physics Today*, 53(11):22, 2000. quant-ph/0111100.

[17] J. Gruska. *Quantum computing*. Osborne McGraw-Hill, 1999.

[18] P. Hayden, D. W. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. quant-ph/0307104, 2003.

[19] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829, 1999. quant-ph/9806063.

[20] C. King and M. B. Ruskai. Minimal entropy of states emerging from noisy quantum channels. *IEEE Transactions on Information Theory*, 47:192–209, 2001.

[21] D. W. Leung. Quantum vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002. quant-ph/0012077.

[22] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[23] J. Oppenheim and M. Horodecki. How to reuse a one-time pad and other notes on authentication, encryption and protection of quantum information. quant-ph/0306161, 2003.

[24] J. Preskill. Lecture notes on quantum information processing. http://www.theory.caltech.edu/people/preskill/ph229/#lecture.

[25] M. B. Ruskai, S. Szarek, and E. Werner. An analysis of completely-positive trace-preserving maps on $\mathcal{M}_2$. quant-ph/0101003, 2001.

[26] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.