J. Phys. A: Math. Theor. **40** (2007) 5415–5426 doi:10.1088/1751-8113/40/20/011

Optimality of private quantum channels

Jan Bouda[1,2] **and Mario Ziman**[1,3]

[1] Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic
[2] Seibersdorf Research, Austria
[3] Research Center for Quantum Information, Slovak Academy of Sciences, Dubravská cesta 9, 845 11 Bratislava, Slovakia

E-mail: xbouda1@fi.muni.cz and ziman@savba.sk

Received 2 August 2006, in final form 5 February 2007
Published 30 April 2007
Online at stacks.iop.org/JPhysA/40/5415

Abstract
We addressed the question of optimality of private quantum channels. We have shown that the Shannon entropy of the classical key necessary to securely transfer the quantum information is lower bounded by the entropy exchange of the private quantum channel $\mathcal{E}$ and the von Neumann entropy of the ciphertext state $\varrho^{(0)}$. Based on these bounds we have shown that decomposition of private quantum channels into orthogonal unitaries (if they exist) optimizes the entropy. For non-ancillary single-qubit PQC we have derived the optimal entropy for the arbitrary set of plaintexts. In particular, we have shown that except when the (closure of the) set of plaintexts contains all states, one bit key is sufficient. We characterized and analysed all the possible single-qubit private quantum channels for an arbitrary set of plaintexts. For the set of plaintexts consisting of all qubit states we have characterized all possible approximate private quantum channels and we have derived the relation between the security parameter and the corresponding minimal entropy.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.−a

1. Introduction

Quantum cryptography [1, 2] (for a popular review see [3]) is a rapidly developing branch of quantum information processing. The results of quantum cryptography include quantum key distribution [4, 5], quantum secret sharing [6, 7], quantum oblivious transfer [8, 9] and other cryptographic protocols [10]. 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 (according to time, space or communication complexity) 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 [11–13] and quantum key [14], authentication of quantum information [15], secret sharing of quantum information [7, 16], quantum data hiding [17] and even commitment to a quantum bit [2], oblivious transfer of quantum information [2] and others.

In this paper we concentrate on private quantum channels (PQC), i.e. on schemes for perfect encryption of quantum information using a pre-distributed classical key, originally introduced in [11]. Our aim is to analyse the optimal encryption of an arbitrary set of quantum states. In section 2 we define the problem in general settings and investigate the elementary properties of private quantum channels including their optimality. Further, in section 3 we focus on PQC for an arbitrary set of qubit states. We will restrict ourselves to encryption schemes without ancillas. The approximate private quantum channels (APQC) for a single qubit are investigated in section 4.

2. Private quantum channels and optimality

Consider a subset $\mathcal{P} \subset \mathcal{S}(\mathcal{H})$ of quantum states. Its encryption is expressed by a completely positive trace-preserving linear map $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H} \otimes \mathcal{H}_{\text{anc}})$, where $\mathcal{H}_{\text{anc}}$ describes some ancillary system and $\mathcal{B}(\mathcal{H})$ stands for the set of bounded linear operators. The encryption consists of two steps: (i) addition of an ancilla in the state $\xi_{\text{anc}}^{(j)}$ and (ii) subsequent application of the unitary transformation U_j with the probability p_j satisfying the following identity

$$\mathcal{E}[\varrho] = \sum_j p_j U_j \left(\varrho \otimes \xi_{\text{anc}}^{(j)}\right) U_j^\dagger = \varrho^{(0)} \tag{1}$$

for all states $\varrho \in \mathcal{P}$. The triple $[\mathcal{P}, \mathcal{E}, \varrho^{(0)}]$ satisfying equation (1) defines a private quantum channel (PQC). This definition establishes a communication quantum channel for which an eavesdropper gains no information by intercepting the transmitted messages. The indistinguishability of different convex decomposition of the same state ($\varrho^{(0)}$) guarantees the security of PQC.

The secure communication via PQC is successful only if the sender and the receiver share the same classical key $(j_1, \ldots, j_n)$ corresponding to the sequence of unitary operations $(U_{j_1}, \ldots, U_{j_n})$. The encryption as defined in equation (1) can be viewed as a noisy operation $\mathcal{E}$ caused by the environment interacting with the system and ancilla. Consequently, the decryption depends on our ability to inverse such noise. Therefore, only unitary decompositions of PQC channels are of interest [18, 19]. The decryption itself is similarly like encryption composed of two steps: (i) an application of a unitary operation according to a shared classical key and (ii) discarding of the ancilla. The size of the classical key is quantified by its Shannon entropy ($H = -\sum_j p_j \log_2 p_j$) and our aim is to address the question of the optimal encryption scheme that enables us to securely communicate an arbitrary set of qubit plaintexts $\mathcal{P}$. The PQC with the smaller entropy is better, because less amount of classical information must be distributed prior to secure transmission of quantum states. The authors

in [11] analysed two cases: (i) encryption of all qubit states (optimal key $H = 2$), and (ii) encryption of real superpositions (optimal key $H = 1$), i.e. the equatorial plane in the Bloch sphere picture.

Before we get to a specific case of single-qubit PQC let us introduce some important notions and properties of private quantum channels. Due to linearity the PQC transformation $\mathcal{E}$ encrypts not only the set $\mathcal{P}$, but also arbitrary trace-preserving linear combination of its elements, i.e. the whole set $\overline{\mathcal{P}}_{\rm tp} = \{\varrho = \sum_k q_k \varrho_k$: such that $\varrho_k \in \mathcal{P}, \sum_k q_k = 1, q_k$ is real$\}$. The set of operations $U'_j = VU_j$ (V is unitary) forms a PQC $[\mathcal{P}, \mathcal{E}', \varrho^{(0)'}]$ ($\varrho^{(0)'} = V\varrho^{(0)}V^\dagger$), providing that the quadruple $[\mathcal{P}, \mathcal{E}, \varrho^{(0)}]$ establishes a PQC for the plaintexts in $\mathcal{P}$. We note that ancilla states $\xi^{(j)}_{\rm anc}$ and probabilities p_j remain the same for both $\mathcal{E}', \mathcal{E}$.

In what follows we will restrict ourselves to PQC schemes using a fixed ancilla state, i.e. $\xi^{(j)}_{\rm anc} = \varrho_{\rm anc}$ for all j. Thus for PQC we have

$$\mathcal{E}[\varrho] = \sum_j p_j U_j(\varrho \otimes \varrho_{\rm anc})U_j^\dagger = \varrho^{(0)}. \tag{2}$$

Such a restricted definition was used in the original work [11] and it is sufficient for our purposes, because in the next sections we will consider only PQC schemes without ancillas. The general case deserves a deeper investigation, but it is beyond the scope of this paper. Let us analyse the optimality for private quantum channels with a fixed state of the ancilla.

The entropy exchange function $S_{\rm ex}(\varrho, \mathcal{E})$ quantifies the amount of quantum information lost in quantum environment due to interaction resulting in the transformation $\mathcal{E}$ providing that the initial state of the system is ϱ. In our case the state ϱ describes the system together with the ancilla, because both of them are transmitted via the quantum channel together. Due to the Stinespring theorem each quantum channel $\mathcal{E}$ can be expressed as a unitary transformation on a larger system, i.e. $\mathcal{E}[\varrho] = {\rm Tr}_{\rm env} G(\varrho \otimes |0\rangle\langle 0|)G^\dagger = \sum_j A_j \varrho A_j^\dagger$, where G is a unitary transformation describing the interaction with the environment. The entropy exchange is defined as the von Neumann entropy of the environment state after the interaction, i.e. $S_{\rm ex}(\varrho, \mathcal{E}) = S(\omega_{\rm env})$ with $\omega_{\rm env} = {\rm Tr}_{\rm system}[G(\varrho \otimes |0\rangle\langle 0|)G^\dagger] = \sum_{jk} {\rm Tr}\big[A_j \varrho A_k^\dagger\big]|j\rangle\langle k|$. This quantity does not depend on particular Kraus representation, because different Kraus representations of the same quantum channel are related by unitary transformation. Since PQCs are always random unitary channels, it follows that $\omega_{\rm env} = \sum_{jk} \sqrt{p_j p_k}\, {\rm Tr}\big[U_j \varrho U_k^\dagger\big]|j\rangle\langle k|$. From the definition of the von Neumann entropy [20] as the minimum of the Shannon entropy over all projective measurements the following inequality holds $S(\omega_{\rm env}) \leqslant S({\rm diag}_{\mathcal{B}}[\omega_{\rm env}])$ for arbitrary state $\omega_{\rm env}$. Thus, the equality is achieved if the basis $\mathcal{B}$ coincides with the eigenbasis of the density operator $\omega_{\rm env}$. The operation ${\rm diag}_{\mathcal{B}}$ cancels all off-diagonal terms in the description of the density matrix in the basis $\mathcal{B}$. In our case we have $S({\rm diag}[\omega_{\rm env}]) = H(\{p_k\})$, i.e. the entropy of the shared key equals to the entropy of the diagonal elements of the state $\omega_{\rm env}$. Hence, we obtain the following lower bound on the key entropy

$$H(\{p_k\}) \geqslant \max_{\varrho} S_{\rm ex}(\varrho, \mathcal{E}). \tag{3}$$

The left side of this inequality does depend on the particular convex decomposition of the quantum channel $\mathcal{E}$, but the right-hand side is independent of the particular realization of $\mathcal{E}$. Therefore, the smallest possible entropy of the key H is given by the maximum of the entropy exchange. We have seen that this inequality is saturated only if the environment state is diagonal, i.e. ${\rm Tr}\big[U_j \varrho U_k^\dagger\big] = 0$ for $j \neq k$. Choosing $\varrho \sim I$ we obtain the orthogonality condition for unitary transformations U_j, i.e. ${\rm Tr}\big[U_j U_k^\dagger\big] = 0$ for $j \neq k$. Thus, convex decomposition into orthogonal unitary transformations saturates the above inequality. The right side is independent of the Kraus representation (decomposition)

of $\mathcal{E}$ and, moreover, for random unitary channels the maximum of $S_{\rm ex}$ is achieved for the total mixture, because the diagonal elements are independent of the state ϱ, i.e. $\mathrm{diag}[\omega_{\rm env}] = \mathrm{diag}\big[\sum_{jk}\sqrt{p_j p_k}\,\mathrm{Tr}\big(U_j\varrho U_k^\dagger\big)|j\rangle\langle k|\big] = \sum_j p_j|j\rangle\langle j|$ for all states ϱ. As a result we have obtained that the optimal realization of PQC minimizing the entropy of classical key is achieved for the encryption with mutually orthogonal unitary transformations. The open question is whether such orthogonal decomposition exists for all random unitary channels, or at least for all PQCs.

For a mixture of pure states $\varrho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$ the following inequality holds $S(\varrho) \leqslant H(\{p_j\})$. Consider a pure state $|\psi\rangle \in \overline{\mathcal{P}}_{\rm tp}$. Encryption operation $\mathcal{E}$ results in a mixture $\varrho^{(0)} = \sum_j p_j|\psi_j\rangle\langle\psi_j|$ with $|\psi_j\rangle = U_j|\psi\rangle$, i.e. we can use the entropy of the state $\varrho^{(0)}$ to bound the entropy of the key from below

$$H(\{p_j\}) \geqslant S(\varrho^{(0)}). \tag{4}$$

The previous lower bound in equation (3) determines the optimal value of the classical key entropy for a given PQC $\mathcal{E}$, but this bound enables us to limit the key entropy of PQC based on the state $\varrho^{(0)}$. This inequality suggests that the smaller the entropy of $\varrho^{(0)}$, the more optimal PQC could exist. For a given set of plaintexts this means that the most optimal PQC should be the one with the purest possible state $\varrho^{(0)}$. However, this bound is not achievable in general. For instance, the encryption of all single-qubit states requires $H = 2$, but the entropy of the maximally mixed single-qubit state is $S\big(\varrho^{(0)} = \frac{1}{2}I\big) = 1$.

3. Single-qubit private quantum channels

In the previous section we have shown that the optimal realization of a fixed PQC consists of orthogonal unitary transformations. However, the more general question is the optimal PQC for a given set of plaintexts $\mathcal{P}$. The first question is to specify the states $\varrho^{(0)}$ achievable by PQC. As we have argued at the end of the previous section the purer the state $\varrho^{(0)}$, the smaller could be the entropy of the classical key. Using the fact that the arbitrary trace-preserving linear map cannot increase the trace distance between two states ($D(\varrho,\sigma) = \mathrm{Tr}|\varrho - \sigma|$) we obtain

$$\delta = \min_{\varrho\in\overline{\mathcal{P}}_{\rm tp}} D\left(\varrho\otimes\varrho_{\rm anc}, \frac{1}{N}I\right) \geqslant D\left(\varrho^{(0)}, \frac{1}{N}I\right), \tag{5}$$

where $N = \dim(\mathcal{H}\otimes\mathcal{H}_{\rm anc})$ is the dimension of the system together with the ancilla. This inequality restricts the possible states $\varrho^{(0)}$ to the δ vicinity around the total mixture $\frac{1}{N}I$, but the achievability of all such states must be proved, see below.

3.1. Single-qubit ancilla-free PQCs

The PQC channel is a special random unitary channel, hence it is unital (preserves the total mixture $\frac{1}{N}I$). This feature makes it easy to analyse all PQCs for a single qubit, i.e. for a two-dimensional quantum system, if we restrict ourselves to PQC without ancillas (ancilla-free PQC). Under such a condition the PQCs are just single-qubit unital channels that coincide with random unitary channels, i.e. each single-qubit unital channel can be expressed as a convex combination of unitary transformations [21]. In what follows we will use the Bloch sphere representation of qubit states, i.e. as three-dimensional real vectors $\vec{r}$ specifying the state $\varrho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})$, where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli operators. The unital quantum channels $\mathcal{E}$ correspond to Bloch vector transformations $\vec{r} \to \vec{r}' = T\vec{r}$, where T is a 3×3 real matrix with coefficients $T_{jk} = \mathrm{Tr}(\sigma_j\mathcal{E}[\sigma_k])$. Each unital quantum channel can be written

via two unitary transformations U, V and a specific quantum channel $\Phi_{\mathcal{E}}$ in the following way $\mathcal{E}[\varrho] = U\Phi_{\mathcal{E}}[V^{\dagger}\varrho V]U^{\dagger}$. The operation $\Phi_{\mathcal{E}}$ is just the convex combination of mutually orthogonal unitary transformations (Pauli operators $I, \sigma_x, \sigma_y, \sigma_z$), i.e. $\Phi_{\mathcal{E}}[\varrho] = \sum_j p_j \sigma_j \varrho \sigma_j$. In Bloch sphere representation this corresponds to the product of three matrices (singular value decomposition) $T = R_U D R_V$, where R_U, R_V are the corresponding rotations of the Bloch sphere around its origin and $D = \mathrm{diag}\{\lambda_1, \lambda_2, \lambda_3\}$ is a diagonal matrix with λ_j being singular values of the matrix T (for details see [21, 22]). They are related to the probabilities p_j via the following identities

$$\begin{aligned} p_x &= \tfrac{1}{4}(1 + \lambda_1 - \lambda_2 - \lambda_3) \\ p_y &= \tfrac{1}{4}(1 - \lambda_1 + \lambda_2 - \lambda_3) \\ p_z &= \tfrac{1}{4}(1 - \lambda_1 - \lambda_2 + \lambda_3) \\ p_0 &= 1 - p_x - p_y - p_z. \end{aligned} \tag{6}$$

To guarantee the positivity the parameters $\lambda_1, \lambda_2, \lambda_3$ are constrained by the inequalities $p_j \geqslant 0$.

In the previous section we have shown that orthogonal decompositions of a given channel $\mathcal{E}$ are the optimal ones (in the sense of the key entropy). Moreover, the entropy of the classical keys is the same for quantum channels $\mathcal{E}$ and $\Phi_{\mathcal{E}}$ (they are unitarily equivalent). Therefore it is sufficient to analyse only the so-called Pauli channels $\Phi_{\mathcal{E}}$, for which the optimal realization is clearly a convex combination of Pauli unitary rotations. Let us start with the specification of possible sets of plaintexts $\overline{\mathcal{P}}_{\mathrm{tp}}$. The smallest possible set consists of a single plaintext ($\mathcal{P}^1 = \{\varrho\}$), but in this case the situation is trivial, because there is nothing to hide. We recall that the set of plaintexts is publicly known. The largest possible set contains all qubit states, i.e. $\mathcal{P}^4 = \mathcal{S}(\mathcal{H})$. We can meet with such case whenever the set $\mathcal{P}$ contains four (not only three!) mutually independent quantum states (Bloch vectors). The mutual independence means that one of them cannot be written as some trace-preserving linear combination of the others. The trace-preserving linear combinations form a set covering the whole Bloch sphere, i.e. $\overline{\mathcal{P}}_{\mathrm{tp}} = \mathcal{S}(\mathcal{H})$. For this maximal possible set of plaintexts the optimal private quantum channel is represented by the completely depolarizing channel mapping all states into the total mixture, i.e. $\Phi_{\mathcal{E}}[\varrho] = \frac{1}{4}(\varrho + \sigma_x\varrho\sigma_x + \sigma_y\varrho\sigma_y + \sigma_z\varrho\sigma_z) = \frac{1}{2}I$ for all ϱ. Thus a classical key of the length of two bits is necessary for the encryption of the whole Bloch sphere, i.e. $H = 2$ [11].

Our aim is to investigate the minimal length of the classical key for other possible sets of plaintexts $\mathcal{P}$. In principle, there are only two remaining options: the set $\overline{\mathcal{P}}_{\mathrm{tp}}$ is generated either by two states ($\mathcal{P}_2 = \{\varrho_1, \varrho_2\}$), or by three states ($\mathcal{P}_3 = \{\varrho_1, \varrho_2, \varrho_3\}$). The goal is to find the dependence of the key entropy on particular properties of these generating states. In the Bloch sphere picture the sets $\overline{\mathcal{P}}^2_{\mathrm{tp}}$ and $\overline{\mathcal{P}}^3_{\mathrm{tp}}$ can be illustrated as lines and planes, respectively, intersecting the Bloch sphere (for details see [22]). It is known [11] that for the so-called real qubits, i.e. real superpositions of two orthogonal pure states, only a single bit is sufficient to establish a private quantum channel. Such states form a particular set of plaintexts consisting of all equatorial states of the Bloch sphere. Using this result we can conclude that there exists a private quantum channel for the arbitrary set $\overline{\mathcal{P}}^2_{\mathrm{tp}}$ with the entropy $H = 1$. This can be seen directly from the Bloch sphere representation, because real superpositions form a circle containing the centre of the Bloch sphere, but each line associated with $\overline{\mathcal{P}}^2_{\mathrm{tp}}$ belongs to some plane containing the total mixture. Therefore, the real qubit encryption PQC scheme works for all lines belonging to the corresponding real qubit plane. However, it is not known whether for a specific set of plaintexts (not containing the total mixture) we cannot do better and establish a PQC with $H < 1$.

3.2. All ancilla-free PQCs

In what follows we will address the following question: which single-qubit unital maps constitute a PQC? Except the trivial case ($\mathcal{P}^1$), the set $\overline{\mathcal{P}}_{\rm tp}$ contains at least two pure states $|\psi_1\rangle, |\psi_2\rangle \in \overline{\mathcal{P}}_{\rm tp}$. The PQC maps these two states into the state $\varrho^{(0)}$. Using the Bloch sphere representation this means that $\vec{r}_1 \to \vec{r}_1' = \vec{s}$ and $\vec{r}_2 \to \vec{r}_2' = \vec{s}$, where $\vec{r}_1, \vec{r}_2$ correspond to pure states, respectively, and $\vec{s}$ is associated with $\varrho^{(0)}$. Using the explicit form of Pauli channels ($\Phi_{\mathcal{E}} \leftrightarrow D = \mathrm{diag}\{\lambda_x, \lambda_y, \lambda_z\}$) the identity $\vec{r}_1' - \vec{r}_2' = \vec{0}$ results in the system of equations $\lambda_j(r_{1j} - r_{2j}) = 0$ for all components $j = x, y, z$. These equalities hold only if $\lambda_j = 0$, or $r_{1j} = r_{2j}$. If none of the λs vanishes ($\lambda_x\lambda_y\lambda_z \neq 0$), then necessarily $\vec{r}_1 = \vec{r}_2$, i.e. the states are identical. Therefore at least one of the λ_j must vanish. Choose $\lambda_z = 0$. The complete positivity constraint [21] restricts the possible values of λ_x, λ_y so that the inequality $|\lambda_x \pm \lambda_y| \leqslant 1$ specifies all possible (non-ancillary) single-qubit private quantum channels, i.e. the general single-qubit PQC is up to a unitary rotation represented in its optimal form as follows:

$$\mathcal{E}[\varrho] = \tfrac{1}{4}((1+b)\varrho + (1+a)\sigma_x\varrho\sigma_x + (1-a)\sigma_y\varrho\sigma_y + (1-b)\sigma_z\varrho\sigma_z) \tag{7}$$

such that $a = \lambda_x - \lambda_y, b = \lambda_x + \lambda_y$ and complete positivity constraints $|a| \leqslant 1, |b| \leqslant 1$. The (optimal) entropy of the classical key necessary for establishing the general PQC channel equals

$$H(\mathcal{E}) = 2 - \tfrac{1}{4}[h(a) + h(b)], \tag{8}$$

where $h(x) = (1+x)\log(1+x) + (1-x)\log(1-x)$.

3.3. Two linearly independent states

Consider a set of plaintexts $\mathcal{P}_{xy} = \{\varrho_z = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)\}$ with x, y fixed. Each PQC given by $D = \mathrm{diag}(\lambda_x, \lambda_y, 0)$ enables us to transmit these sets securely. In the Bloch sphere representation these sets form lines parallel to the line connecting the poles of the Bloch sphere. Without loss of generality we can assume that sets $\overline{\mathcal{P}}_{xy}$ are the most general sets of type $\overline{\mathcal{P}}^2_{\rm tp}$. Indeed, the arbitrary set $\overline{\mathcal{P}}^2_{\rm tp}$ is just a unitarily rotated set $\overline{\mathcal{P}_{xy}} = \{\varrho_z = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)\}$ for some values x, y. In particular, given a set $\mathcal{P}^2$ as a segment of the line l crossing the Bloch sphere, it is always possible to choose the coordinate system in the following way: the x axis is given by the centre of the Bloch sphere ($\frac{1}{2}I$) and the middle point of the segment of the line l (most mixed state in $\overline{P}^2_{\rm tp}$), the y axis is perpendicular to the plane given by the whole line l and the total mixture. This choice of the new coordinates corresponds to a unitary rotation of the Pauli operators $\sigma_j \to S_j = U\sigma_j U^\dagger$. In this basis the line is given by the states $\varrho_{z'} = \frac{1}{2}(I + x'S_x + z'S_z)$ for some fixed x'. For instance, the states in $\mathcal{P}_{xy}$ can be transformed into this form by a suitable rotation around the z axis. Therefore, the analysis of $\overline{\mathcal{P}}^2_{\rm tp}$ reduces to the analysis of this type of states. Using the expression for the distance between an arbitrary state $\varrho \leftrightarrow \vec{r}$ and the total mixture $D\big(\varrho, \frac{1}{2}I\big) = |\vec{r}|$ it follows that the closest state from the general set of plaintexts $\overline{\mathcal{P}}_{\rm tp}$ is always the one associated with the shortest Bloch vector. For the states of the form $\varrho_{z'}$ the minimum is achieved for $z' = 0$, i.e. for the state $\varrho_{\rm min} = \frac{1}{2}(I + x'S_x)$, for which $D\big(\varrho_{\rm min}, \frac{1}{2}I\big) = \delta = |x'|$. The solution for real qubits guarantees the existence of PQC with $H = 1$ and $\varrho^{(0)} = \frac{1}{2}I$ (i.e. $\delta = 0$), but PQCs for other states $\varrho^{(0)}$ are possible as well. Nevertheless, the formula for the entropy for a general PQC channel guarantees that H cannot be smaller than 1, i.e. $H \geqslant 1$. Although we cannot improve the entropy rate for $\overline{\mathcal{P}}^2_{\rm tp}$

we are still curious about the possibility of $\varrho^{(0)} = \varrho_{\min}$. A direct calculation gives us that the encryption $\left(\frac{1}{2}, I\right)\left(\frac{1}{2}, S_x\right)$ establishes a PQC with the desired property, i.e.

$$\varrho^{(0)} = \tfrac{1}{2}(\varrho_{z'} + S_x \varrho_{z'} S_x) = \tfrac{1}{2}(1 + x' S_x) = \varrho_{\min} \tag{9}$$

with the entropy of the key $H = 1$. In fact, an arbitrary state within the sphere $|\vec{r}| \leqslant \delta = |x'|$ is achievable with the entropy $H = 1$.

3.4. Three linearly independent states

The sets $\mathcal{P}_x = \left\{\varrho_{yz} = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)\right\}$ for a fixed x and arbitrary y, z represent up to unitary rotations the most general sets of plaintexts of the type $\overline{\mathcal{P}}^3_{\text{tp}}$, i.e. planes in the Bloch sphere representation perpendicular to the x axis. In this case not all PQCs (up to unitary rotation) are suitable, but only those, for which $\lambda_y = \lambda_z = 0$ and $\lambda_x \neq 0$. This class of PQCs is more powerful, because it encrypts not only the sets $\overline{\mathcal{P}}^2_{\text{tp}}$, but also the sets $\overline{\mathcal{P}}^3_{\text{tp}}$. These channels correspond to so-called phase damping channels, i.e. they describe the most general pure decoherence processes [23]. Using a suitably rotated PQC of this form ($D = \text{diag}\{\lambda_x, 0, 0\}$) we can encrypt any possible set $\overline{\mathcal{P}}^2_{\text{tp}}$ and $\overline{\mathcal{P}}^3_{\text{tp}}$ with the entropy

$$H = 2 - \tfrac{1}{2}[(1 + \lambda_x)\log(1 + \lambda_x) + (1 - \lambda_x)\log(1 - \lambda_x)]. \tag{10}$$

It follows that the smallest possible value of the entropy is the same for both types of sets and equals $H = 1$, i.e. except the plaintexts containing the whole set of states $\overline{\mathcal{P}}_{\text{tp}} = \mathcal{S}(\mathcal{H})$, a single bit classical key is sufficient to establish a private quantum channel transmitting all plaintexts $\varrho \in \overline{\mathcal{P}}_{\text{tp}}$ for arbitrary set $\mathcal{P}$, for which $\overline{\mathcal{P}}_{\text{tp}} \neq \mathcal{S}(\mathcal{H})$.

3.5. Optimality

The optimal value is achieved for $\lambda_x = 1$, i.e. the corresponding private quantum channels are unitarily equivalent to

$$\Phi^{\text{opt}}_{\mathcal{E}}[\varrho] = \tfrac{1}{2}(\varrho + \sigma_x \varrho \sigma_x). \tag{11}$$

We have analysed the achievability of states $\varrho^{(0)} \neq \frac{1}{2}I$ for sets $\overline{\mathcal{P}}^2_{\text{tp}}$ and the question is whether the situation is similar as it was in the case of sets $\overline{\mathcal{P}}^3_{\text{tp}}$. In particular, $\varrho_{\min} = \frac{1}{2}(I + x\sigma_x)$ is the state with the smallest length of the Bloch vector among all states in $\mathcal{P}_x$. Is it possible to design a PQC such that $\varrho^{(0)} = \varrho_{\min}$? The answer is simple, because the PQC given in equation (11) satisfies this property, i.e. $\Phi^{\text{opt}}_{\mathcal{E}}[\mathcal{P}_x] = \frac{1}{2}(I + x\sigma_x)$. Since all other sets $\overline{\mathcal{P}}^3_{\text{tp}}$ are just unitarily rotated sets $\mathcal{P}_x$, it follows that the states $\varrho_{\min}$ are achievable in general. For a general PQC $[\overline{\mathcal{P}}^3_{\text{tp}}, D = \text{diag}\{\lambda_x, 0, 0\}, \varrho^{(0)}]$ the allowed states $\varrho^{(0)}$ are inside the sphere determined by the condition $|\vec{r}| \leqslant \delta$. In particular, $D\left(\varrho^{(0)}, \frac{1}{2}I\right) = |\lambda_x x| = |ax| \leqslant \delta$ and the entropy H is given by the formula in equation (10), i.e. it increases as the distance $D\left(\varrho^{(0)}, \frac{1}{2}I\right)$ is decreasing. Denote by θ the distance $D\left(\varrho^{(0)}, \frac{1}{2}I\right)$. Then for a given value of θ the corresponding PQC transformation is $D = \text{diag}\{\theta/\delta, 0, 0\}$.

As a result we have derived that the optimal entropy of the classical key for arbitrary (two or three dimensional) set of plaintexts equals $H = 1$. Moreover, we have found the dependence of the optimal entropy on the distance θ between the state $\varrho^{(0)}$ and the total mixture (see also figure 1)

$$H\left(\overline{\mathcal{P}}^2_{\text{tp}}, \theta\right) = 1 \tag{12}$$

$$H\left(\overline{\mathcal{P}}^3_{\text{tp}}, \theta\right) = 2 - \tfrac{1}{2}[(1 + \theta/\delta)\log(1 + \theta/\delta) + (1 - \theta/\delta)\log(1 - \theta/\delta)]. \tag{13}$$

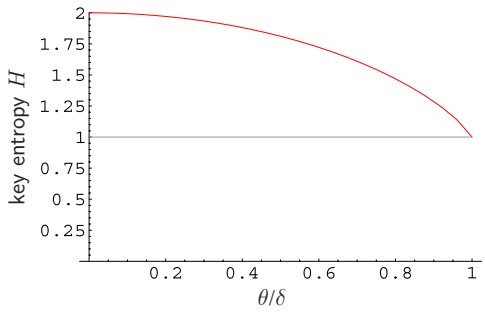

Figure 1. Optimal entropy as a function of the distance $\theta = D(\varrho^{(0)}, \frac{1}{2}I)$ for the arbitrary set of plaintexts characterized by the parameter $\delta = \min_{\varrho \in \overline{\mathcal{P}}_{\rm tp}} D(\varrho, \frac{1}{2}I)$. The upper line describes the dependence for sets of plaintexts containing three independent states (planes) and the lower (constant) line describes the situation for plaintexts containing only two independent states (lines).

4. Approximate private quantum channels

Approximate private quantum channels (APQC) generalize the ideal version in the following sense. The quadruple $[\mathcal{P}, \mathcal{E}, \varrho_{\rm anc}, \epsilon]$ constitutes an ϵ-private quantum channel (ϵ-PQC), if

$$D(\mathcal{E}[\varrho_1 \otimes \varrho_{\rm anc}], \mathcal{E}[\varrho_2 \otimes \varrho_{\rm anc}]) \leqslant \epsilon \tag{14}$$

for all $\varrho_1, \varrho_2 \in \mathcal{P}$. As before, the encryption operation $\mathcal{E}$ consists of a mixture of unitary transformations U_j applied with probabilities p_j. Similarly, the decryption operation is given by the application of the inverse operations $U_j^\dagger$ according to a shared classical key represented by the sequence of unitaries $U_{j_1}, \ldots, U_{j_n}$. In such generalization of PQC the transmission is still perfect and ϵ quantifies the security of the protocol, i.e. the distinguishability of the transferred states.

We are not going to discuss the problem of optimality for such generalization in its full generality, but we will pay attention to encryption of the qubit states without using any additional ancillas. The set of all approximate private quantum channels is a specific subset of all random unitary channels determined by the value of ϵ. As we have mentioned, the arbitrary single-qubit unital channel can be written as a convex combination of unitary transformations and upto unitary transformations the general unital qubit channel $\mathcal{E}$ is specified by three parameters $\lambda_x, \lambda_y, \lambda_z$ related to probabilities p_0, p_x, p_y, p_z via equation (6). The entropy achieves its optimal value (minimum) for the orthogonal unitary decomposition of $\mathcal{E}$; hence it equals the entropy of this probability distribution, $H = -\sum_j p_j \log p_j$.

It follows that each unital qubit channel establishes an ϵ-PQC, but we still need to specify the particular value ϵ and then analyse the optimal entropy as a function of the degree of privacy for different sets of plaintexts $\mathcal{P}$. Let us analyse the case when the set of plaintexts $\mathcal{P}$ consists of all quantum states, i.e. $\mathcal{P}$ equals the Bloch sphere. For a given PQC $\mathcal{E}$ (i.e. arbitrary unital channel) we have

$$\begin{aligned}\epsilon &= \max_{\varrho_1, \varrho_2 \in \mathcal{S}(\mathcal{H})} D(\mathcal{E}[\varrho_1], \mathcal{E}[\varrho_2]) = \max_{\vec{r}_1, \vec{r}_2} \sqrt{\sum_j \lambda_j^2 |r'_{1j} - r'_{2j}|^2} \\ &= 2\max\{|\lambda_x|, |\lambda_y|, |\lambda_z|\} \equiv 2\lambda_{\max}. \end{aligned} \tag{15}$$

Without loss of generality we can assume that $|\lambda_x| \leqslant |\lambda_y| \leqslant |\lambda_z| = \epsilon/2$. Our aim is to analyse and relate the functions $\epsilon = \epsilon(\lambda_x, \lambda_y, \lambda_z)$ and $H = H(\lambda_x, \lambda_y, \lambda_z)$. In particular we

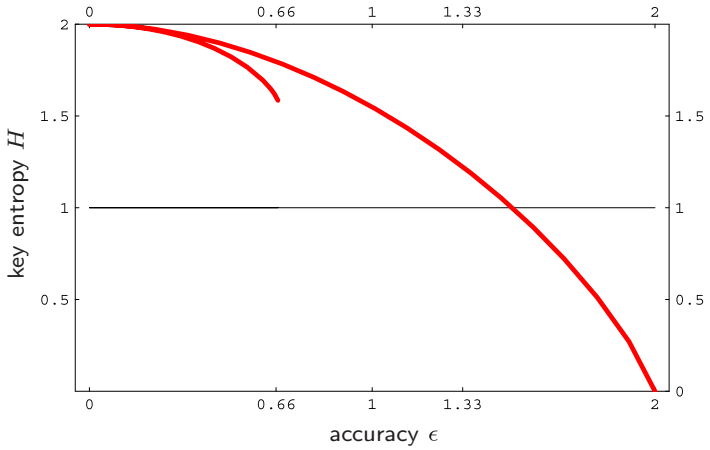

Figure 2. The dependence of the entropy of the optimal key H for a given degree of secrecy ϵ is depicted for all depolarizing channels characterized by $\lambda_x = \lambda_y = \lambda_z = \lambda \in [-1/3, 1]$.

are interested in two questions: (i) given ϵ what is the optimal approximative PQC, i.e. with the minimal entropy H, and (ii) given the entropy H what is the most perfect PQC, i.e. with the smallest ϵ.

Consider λ_z is fixed and $|\lambda_x| \leqslant |\lambda_y| \leqslant |\lambda_z|$, i.e. the security parameter $\epsilon = 2|\lambda_z|$ is fixed. For unital single-qubit channels the conditions of complete positivity (see equation (6)) read

$$1 - \lambda_z \geqslant \pm(\lambda_x - \lambda_y) \qquad 1 + \lambda_z \geqslant \pm(\lambda_x + \lambda_y). \tag{16}$$

The values $\lambda_x, \lambda_y, \lambda_z$ satisfying these conditions form a tetrahedron with vertices associated with the orthogonal unitary transformations $I, \sigma_x, \sigma_y, \sigma_z$. Since these vertices are unitarily related, the whole tetrahedron can be divided into four unitarily equivalent parts containing channels with the same values of entropy. It follows that it is sufficient to analyse only two regions (forming a particular single part): with strictly positive values ($\lambda_x, \lambda_y, \lambda_z \geqslant 0$) and with strictly negative values ($\lambda_x, \lambda_y, \lambda_z \leqslant 0$).

Intuitively, the geometric picture suggests that the most optimal APQC should shrink the Bloch sphere symmetrically, i.e. $|\lambda_x| = |\lambda_y| = |\lambda_z| = \lambda$. However, not for all positive, or negative combinations of $\lambda_x, \lambda_y, \lambda_z$ such transformation is associated with some completely positive map, i.e. the probabilities p_j in equation (6) are not positive. Let us assume that $\lambda_x = \lambda_y = \lambda_z = \lambda$ then

$$H_I = 2 - \tfrac{1}{4}[(1 + 3\lambda)\log(1 + 3\lambda) + 3(1 - \lambda)\log(1 - \lambda)]. \tag{17}$$

However, the transformation is physical (and entropy makes sense) only if $-\frac{1}{3} \leqslant \lambda \leqslant 1$. Using the relation $\epsilon = 2|\lambda|$ we obtain the dependence of the entropy on the approximation (security) parameter ϵ (see figure 2) for this class of channels. As we can see from figure 2 for smaller values of the security parameter ϵ the channels given by negative values of λ are more optimal. Indeed, one can test numerically that these points are optimal among all possible private quantum channels for $\epsilon \in [0, 2/3]$. Let us note that the point $\lambda = -1/3$ corresponds to the best physical approximation of the universal NOT operation (given by unphysical values $\lambda_x = \lambda_y = \lambda_z = -1$). At this point the entropy equals $H = 1.585$. In the interval $2/3 \leqslant \epsilon \leqslant 0.958$ the optimal entropy is constant because the optimal depolarizing

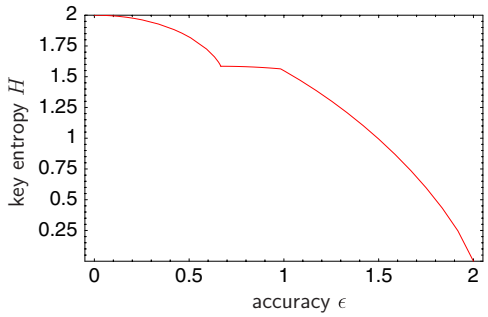

Figure 3. The optimal entropy of the key H with respect to the accuracy ϵ for single-qubit approximate private quantum channels. The optimal values are achieved for depolarizing channels except the interval $2/3 \leqslant \epsilon \leqslant 0.9826$, when the optimal APQC is given by phase damping channels.

channel is still the best approximation of the universal NOT ($\lambda = -1/3$). After that interval the entropy decreases again until its minimal value $H = 0$ is achieved (for $\epsilon = 2$).

While the depolarizing channels are optimal in the region of channels with the positive λs for each value of ϵ, in the negative region these channels are optimal only for $\epsilon \in [0, 2/3]$, because for other values the 'depolarizing' channels are not physical. Let us remark that in the previous paragraph we have discussed the optimality for depolarizing channels, but for $\epsilon > 2/3$ these are no longer optimal. We have found numerically that the channels parametrized as follows: $\lambda_z = -\lambda$ (also for $\lambda \geqslant 1/3$) and $\lambda_x = \lambda_y = -\kappa$ ($\kappa \leqslant \lambda$) are optimal. The inequalities (16) result in the bound $\kappa \leqslant (1-\lambda)/2$, which is nontrivial only if $\lambda > 1/3$. In fact, only in this case the condition $\kappa \leqslant \lambda$ holds. The minimal entropy for $\lambda > 1/3$ is achieved for $\kappa = (1-\lambda)/2$ when

$$H_{II} = \tfrac{1}{2}[3 + \lambda - (1-\lambda)\log(1-\lambda) - (1+\lambda)\log(1+\lambda)] \tag{18}$$

and $\epsilon = 2\lambda$. For a given ϵ this function should be compared with the entropy for depolarizing channel H_I for $\lambda \geqslant 1/3$. If $|\lambda| = 0.4913$ ($\epsilon = 0.9826$) these two functions coincide, i.e. $H_I = H_{II}$.

We have found that the optimal entropy for a given value of the security parameter is given by the following function (see figure 3)

$$H = \begin{cases} H_1(-\epsilon) & \text{for} \quad 0 \leqslant \epsilon \leqslant 2/3 \\ H_2(\epsilon) & \text{for} \quad 2/3 \leqslant \epsilon \leqslant 0.9826 \\ H_1(\epsilon) & \text{for} \quad 0.9826 \leqslant \epsilon \leqslant 2, \end{cases} \tag{19}$$

where $H_1(\epsilon) = 2 - \frac{1}{4}\left[\left(1 + \frac{3}{2}\epsilon\right)\log\left(1 - \frac{3}{2}\epsilon\right) + 3\left(1 - \frac{\epsilon}{2}\right)\log\left(1 - \frac{\epsilon}{2}\right)\right]$ and $H_2(\epsilon) = \frac{1}{2}\left[3 + \frac{\epsilon}{2} - \left(1 - \frac{\epsilon}{2}\right)\log\left(1 - \frac{\epsilon}{2}\right) - \left(1 + \frac{\epsilon}{2}\right)\log\left(1 + \frac{\epsilon}{2}\right)\right]$. This function characterizes optimal approximate private quantum channels for the encryption of the whole state space. Discussing the optimality of APQC for general sets of plaintexts is beyond the scope of this paper. The main obstacle is that the analysis cannot be reduced to some typical sets like it was in the case of perfect PQC. Let us note that for APQC not all the trace-preserving linear combinations must be encrypted with the given security ϵ. A similar result for approximatively private quantum channels has been derived also in [24], where also the optimality for qubit was discussed using different methods and slightly different definition of the security parameter ϵ.

5. Conclusion

For single qubits we have characterized and analysed all possible ancilla-free private quantum channels and all possible approximate private quantum channels. We have shown that except the set of plaintexts $\mathcal{P}$ generating the whole set of states via trace-preserving linear combinations, i.e. if $\overline{\mathcal{P}}_{\rm tp} \neq \mathcal{S}(\mathcal{H})$, for arbitrary set of plaintexts one bit of the classical key is sufficient to establish a private quantum channel. However, if $\overline{\mathcal{P}}_{\rm tp} = \mathcal{S}(\mathcal{H})$ then two classical bits are necessary. In order to use a single bit of the key even in such case, one should employ an unphysical operation—universal NOT ($\mathcal{E}_{\rm NOT}$). The encryption of the single qubit based on the operations $\mathcal{I}, \mathcal{E}_{\rm NOT}$ (with equal probabilities) would map the arbitrary input state into the total mixture $\varrho^{(0)} = \frac{1}{2}(\mathcal{I}[\varrho] + \mathcal{E}_{\rm NOT}[\varrho]) = \frac{1}{2}(\varrho + \varrho^{\perp}) = \frac{1}{2}I$.

Except the results valid for single-qubit private quantum channels we have derived a bound on the optimal entropy for the arbitrary system. In particular we have shown that for PQC $[\mathcal{P}, \mathcal{E}, \varrho^{(0)}]$ the entropy of the key cannot be smaller than the entropy exchange $H \geqslant \max_{\varrho} S_{\rm ex}(\varrho, \mathcal{E})$. We have also shown that for a given random unitary channel $\mathcal{E}$ the decomposition into mutually orthogonal unitaries optimizes the entropy H. For qubits such decomposition always exists, but for larger dimensional systems its existence is an open problem. Except extending the results to larger systems, it would be of interest to perform similar analysis for private quantum channels involving the usage of ancilla in its full generality, i.e. including ancilla. This opens a lot of new possibilities and some improval is very likely to happen.

Acknowledgments

The work was supported by the project GAČR GA201/01/0413. MZ acknowledges the support of Slovak Academy of Sciences via the project CE-PI, APVT-123 and project INTAS (04-77-7289). JB acknowledges support of the Hertha Firnberg ARC stipend program and grant project GAČR 201/06/P338.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2001 Quantum cryptography *Rev. Mod. Phys.* (*Preprint* quant-ph/0101098)
[2] Bouda J 2004 Encryption of quantum information and quantum cryptographic protocols *PhD Thesis*, Faculty of Informatics, Masaryk university, Brno
[3] Gottesman D and Lo H K 2001 From quantum cheating to quantum security *Phys. Today* **53** (11) 22–9
[4] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* pp 175–9
[5] Ekert A 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661
[6] Hillery M, Bužek V and Berthiaume A 1999 Quantum secret sharing *Phys. Rev.* A **59** 1829
[7] Cleve R, Gottesman D and Lo H K 1999 How to share a quantum secret *Phys. Rev. Lett.* **85** 648–51
[8] Bennett C H, Brassard G, Crépeau C and Skubiczewska M H 1991 Practical quantum oblivious transfer *Proc. 11th Annual International Cryptology Conference on Advances in Cryptography* pp 351–66
[9] Crépeau C 1994 Quantum oblivious transfer *J. Mod. Opt.* **41** 2445–54
[10] Gruska J 1999 *Quantum Computing* (New York: Osborne McGraw-Hill)
[11] Ambainis A, Mosca M, Tapp A and de Wolf R 2000 Private quantum channels *FOCS 2000* pp 547–53
[12] Boykin P O and Roychowdhury V 2000 Optimal encryption of quantum bits *Preprint* quant-ph/0003059
[13] Oppenheim J and Horodecki M 2003 How to reuse a one-time pad and other notes on authentification, encryption and protection of quantum information *Preprint* quant-ph/0306161
[14] Leung D W 2002 Quantum Vernam cipher *Quantum Inform. Comput.* **2** 14–34
[15] Barnum H, Crépeau C, Gottesman D, Smith A and Tapp A 2002 Authentification of quantum messages *FOCS 2002* (*Preprint* quant-ph/0205128)

[16] Gottesman D 2000 On the theory of quantum secret sharing *Phys. Rev.* A **61** 042311
[17] Di Vincenzo D P, Hayden P and Terhal B M 2003 Quantum data hiding *Found. Phys.* **33** 1629–47
[18] Gregoratti M and Werner R F 2002 Quantum lost and found *Preprint* quant-ph/0209025
[19] Nayak A and Sen P 2007 Invertible quantum operations and perfect encryption of quantum states *Quantum Inform. Comput.* **7** 103–10
[20] Perez A 1999 *Quantum Theory: Concepts and Methods* (Dordrecht: Kluwer)
[21] Ruskai M B, Szarek S and Werner E 2002 An analysis of completely-positive trace-preserving maps on 2×2 matrices *Linear Algebra Appl.* **347** 159–87
[22] Bouda J and Ziman M 2005 Limits and restrictions of private quantum channel *Preprint* quant-ph/0506107
[23] Ziman M and Bužek V 2005 All (qubit) decoherences: complete characterization and physical implementation *Phys. Rev.* A **72** 022110
[24] Kerenidis I and Nagaj D 2006 On the optimality of quantum encryption schemes *J. Math. Phys.* **47** 092102