Low-dimensional quite noisy bound entanglement with a cryptographic key

2011 J. Phys. A: Math. Theor. 44 035301

(http://iopscience.iop.org/1751-8121/44/3/035301)

IOP Publishing Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. **44** (2011) 035301 (16pp) doi:10.1088/1751-8113/44/3/035301

Low-dimensional quite noisy bound entanglement with a cryptographic key

Łukasz Pankowski[1,2] **and Michał Horodecki**[2]

[1] Institute of Informatics, University of Gdańsk, Gdańsk, Poland
[2] Institute of Theoretical Physics and Astrophysics, University of Gdańsk, Gdańsk, Poland

E-mail: lukpank@o2.pl

Received 7 September 2010, in final form 8 November 2010
Published 13 December 2010
Online at stacks.iop.org/JPhysA/44/035301

Abstract

We provide a class of bound entangled states that have a positive distillable secure key rate. The smallest state of this kind is $4 \otimes 4$. Our class is a generalization of the class presented in Horodecki *et al* (2008 *IEEE Trans. Inf. Theory* **54** 2621–5). It is much wider, containing, in particular, states from the boundary of PPT entangled states (all of the states in the previous class were of this kind) and also states inside the set of PPT entangled states, even approaching the separable states. This generalization comes at a price: for the wider class, a positive key rate requires, in general, apart from the *one-way* Devetak–Winter protocol (used in the previous case) also the recurrence preprocessing and thus is effectively a *two-way* protocol. We also analyze the amount of noise that can be admixtured to the states of our class without losing the key distillability property which may be crucial for experimental realization. The wider class contains key-distillable states with higher entropy (up to 3.524, as opposed to 2.564 for the previous class).

PACS numbers: 03.67.Hk, 03.67.Ac

(Some figures in this article are in colour only in the electronic version)

1. Introduction

Quantum cryptography, pioneered by Wiesner [2], allows one to obtain a cryptographic key based on physical impossibility of eavesdropping. Namely, if the transmitted signal is encoded into quantum states, then by reading it, the eavesdropper always introduces noise into the signal. Thus, Alice and Bob—the parties who want to communicate privately—can measure the level of noise and detect whether their transmission is secure (even if the noise was solely due to eavesdropping). There are two types of quantum key distribution protocols: *prepare and measure* (as the original BB84 protocol [3]) and protocols based on a shared entangled state (originated from Ekert's protocol [4]). For some time, security proofs of prepare and measure protocols had been based on showing equivalence to the distillation (by local operations and classical communication) of maximally entangled states (the first such proof is due to Shor and Preskill [5]). It has led to a belief that the security of the quantum cryptography is always connected to the distillation of maximally entangled states (this issue was perhaps first touched upon by Gisin and Wolf [6]).

This belief suggested that one could not obtain a secure key from bound entangled states [7], i.e. states from which maximally entangled states cannot be distilled. In contrast, the key-distillable bound entangled states have been found [8] and examples of low-dimensional states have been provided [1]. The multipartite case was also considered [9]. There are two approaches to obtaining the cryptographic key from bound entangled partial positive transpose (PPT) states: one is based on approximating the private bit with a PPT state [8, 10] and the other on mixing orthogonal private bits [1].

This paper continues the second approach. The low-dimensional key-distillable states with a PPT[3] (hence, bound entangled) presented in [1] were lying on the boundary of PPT states and the existence of the key-distillable states inside of PPT states was argued by the continuity argument, without giving the explicit form of those inner states. In this paper we present a wider class of PPT entangled key-distillable states including states inside the set of PPT states even approaching the set of separable states. We analyze the properties of this class, and provide some more general criteria of key distillability, by exploiting the criterion provided in [11]. This criterion was earlier applied to analyze some PPT states in [12] (see also [13] in this context).

The motivation behind the search for new bound entangled states with a distillable key is two-fold. First of all, there is a fundamental open question, whether from all entangled states one can draw a secure key. To approach this question, one needs, in particular, to gather more phenomenology on the issue of drawing a key from bound entangled states. In this paper, we have pushed this question a bit by showing explicitly that PPT key-distillable states can be in the interior of PPT states, even, approaching the set of separable states. Also our general criterion of key distillability can serve for finding to what extent entanglement can provide for a secure key.

Another motivation comes from recent experiments, where bound entanglement was implemented in labs [14–18]. In the experiments, usually, a four-partite bound entangled Smolin state was used, which allows for a number of non-classical effects being manifestations of true entanglement content of such a state. We believe that low-dimensional bound entangled key-distillable states are also good candidates for experimental implementation, providing a non-classical effect—the possibility of distilling a secure key. This requires states which are robust against noise, to facilitate the process of preparing them in a lab. In this paper, we analyze the robustness of key-distillable states as well as providing very noisy states, having, in particular, a relatively large entropy (about 3.5 bits versus 4 bits of maximal possible entropy). Last but not least, the key-distillable bound entangled states are strictly related to the effect of superactivation of quantum capacity [19], and our class may be further analyzed in this respect (in this paper, we have provided some exemplary calculations).

The paper is organized as follows. In section 2 we review basic facts about the general theory of distillation of a secure key from quantum states of [10]. In particular, we describe a technique called privacy squeezing. In section 3 we introduce our class of states which are PPT and key distillable. We verify that they lie inside the set of PPT states, touching the set of separable states. Moreover, we check the robustness of the property of key distillability.

---

[3] If a state has PPT then one cannot distill the maximally entangled state from it. It is a long-standing open question whether PPT is also a necessary condition for the non-distillability of maximal entanglement [27] (for recent developments, see [28]).

We also give the explicit form of an important subset of our states as mixtures of pure states in section 4. In sections 5 and 6 we examine entropic properties of our states and their relation with the Smith–Yard superactivation of the quantum capacity phenomenon. Finally, in section 7, we provide a general sufficient condition for distilling a private key from quantum states of local dimensions not less than 4.

2. Preliminaries

Let us first recall some important concepts of classical key distillation from quantum states, covered in detail in [10].

A general state containing at least one bit of a perfectly secure key is called the *private bit* or *pbit* [10]. A private bit in its so-called X-form is given by

$$\gamma(X) = \frac{1}{2}\begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix} \tag{1}$$

where X is an arbitrary operator satisfying $\|X\| = 1$ (here and throughout the paper, we use the trace norm, that is, the sum of the singular values of an operator). The private bit has four subsystems: $ABA'B'$ where the block matrix (1) represents the AB subsystem and the blocks are operators acting on an $A'B'$ subsystem. Subsystems A and B are single-qubit subsystems while dimensions of A' and B' must be greater or equal to 2; we assume dimensions A' and B' are equal and denote them by d. Subsystem AA' belongs to Alice while subsystem BB' belongs to Bob. Every state presented in the block matrix form throughout the paper has this structure. The bit of key contained in a private bit is obtained by measuring subsystems A and B are in the standard basis; therefore, subsystem AB is called the *key part* of the state, while subsystem $A'B'$ is called the *shield* of the state, as it protects correlations contained in the key part from an eavesdropper. Note that it may happen that Eve possesses a copy of the shield subsystem (when, e.g., the shield consists of two flag states—states with disjoint support) yet it does not hurt because the very presence of the shield subsystem in Alice and Bob's hands protects the bit of key.

For a general state with $ABA'B'$ subsystems (i.e. not necessarily a private bit) one can infer the possibility of distillation of a private key using the method called *privacy squeezing* [10]. Namely, we consider the following types of protocols: one measures the key part in the standard basis and classically process the outcomes (cf [11] for two-qubit states). Given a protocol of this type we would like to know whether it can distill the key from the state. To this end, we construct a two-qubit state in the following way: one applies to the original state the so-called *twisting* operation, i.e. a unitary transformation of the following form:

$$U = \sum_{ij} |ij\rangle_{AB}\langle ij| \otimes U_{ij}^{A'B'}, \tag{2}$$

and perform partial trace over $A'B'$. Now, it turns out that if we apply the protocol to the original state we obtain no less key than we would obtain from the above two-qubit state using the same protocol.

Therefore, if we apply a cleverly chosen twisting, we may infer key distillability of the original state, by examining a two-qubit state (i.e. a much simpler object). This technique is called *privacy squeezing*. The role of twisting is to 'squeeze' the privacy present in the original state into its key part, where it is then more easily detectable, e.g., by protocols designed for two-qubit states (see, e.g., [11, 20, 21]).

To explain why the two-qubit state cannot give more key than the original state (within the considered class of protocols) we invoke the following result of [10]. One considers a state of three systems: a quantum one, Eve's system, and two classical ones, the registers holding the outcomes of measurement of the key part (the state is therefore called a *ccq state*). Now it turns out that twisting does not change this state. However, in the considered class of protocols, Alice and Bob use only classical registers, so the output of such protocols depends solely on the ccq state. Thus the key obtained with and without twisting is exactly the same. This holds, even though twisting is a non-local operation and the resulting state can be more powerful in all other respects (such as drawing the key by some other type of protocol). Next, if we additionally trace out the shield, i.e. the subsystem $A'B'$, this means that the resulting ccq state differs from the original ccq state only by Eve having, in addition, the shield. Thus, if any key can be obtained from it, it can only be less secure than the key obtained from the original ccq state.

It turns out that for any 'spider' state, i.e. state of the form

$$\varrho = \begin{bmatrix} C & & & D \\ & E & F & \\ & F^\dagger & E' & \\ D^\dagger & & & C' \end{bmatrix} \tag{3}$$

(where we have omitted zero blocks for clarity), there exists such a twisting operation that the matrix elements of the two-qubit state, obtained by tracing out the $A'B'$ subsystem after applying the twisting, are equal to the trace norms of the corresponding blocks in the original state:

$$\sigma = \begin{bmatrix} \|C\| & & & \|D\| \\ & \|E\| & \|F\| & \\ & \|F\| & \|E'\| & \\ \|D\| & & & \|C'\| \end{bmatrix} \tag{4}$$

(we use here that $\|A\| = \|A^\dagger\|$ for the trace norm). This twisting is in a sense optimal for the spider states. We call the two-qubit state (4) the *privacy-squeezed state* of the original state. If a spider state satisfies $\|C\| = \|C'\|$ and $\|E\| = \|E'\|$, then its privacy-squeezed state is a Bell diagonal state.

For a deeper discussion of the privacy squeezing see [10], although the name *spider state* is not used there.

3. Distilling key from PPT mixtures of private states

Here, we construct a class of bound entangled states which are key distillable. They are mixtures of four orthogonal private bits of some special form. We provide a sufficient condition to distill the cryptographic key from our class. The condition given in this section is generalized to an arbitrary state in section 7.

3.1. Definition of the class

Let us consider a class of states

$$\varrho = \lambda_1\gamma_1^+ + \lambda_2\gamma_1^- + \lambda_3\gamma_2^+ + \lambda_4\gamma_2^- \tag{5}$$

which is a mixture of four orthogonal private bits which could be considered analogs to the Bell states. The construction is possible in dimension $2d \otimes 2d$, with $d \geqslant 2$.

The four private bits are given by

$$\gamma_1^{\pm} = \gamma(\pm X), \quad \gamma_2^{\pm} = \sigma_x^A \gamma(\pm Y) \sigma_x^A \tag{6}$$

where σ_x^A is a Pauli matrix σ_x applied on subsystem A, and by $\gamma(X)$ we mean a private bit written in its X-form (1).

States given by (5) and (6) have the block matrix form (of the mixture of four private bits)

$$\varrho = \frac{1}{2}\begin{bmatrix} (\lambda_1+\lambda_2)\sqrt{XX^\dagger} & & & (\lambda_1-\lambda_2)X \\ & (\lambda_3+\lambda_4)\sqrt{YY^\dagger} & (\lambda_3-\lambda_4)Y & \\ & (\lambda_3-\lambda_4)Y^\dagger & (\lambda_3+\lambda_4)\sqrt{Y^\dagger Y} & \\ (\lambda_1-\lambda_2)X^\dagger & & & (\lambda_1+\lambda_2)\sqrt{X^\dagger X} \end{bmatrix}. \tag{7}$$

Definition 1. *We define the class $\mathcal{C}$ as the class of states given by (5) and (6) with operators X and Y related by*

$$Y = \frac{X^\Gamma}{\|X^\Gamma\|} \tag{8}$$

where the superscript Γ denotes the partial transposition in Alice versus Bob cut, and satisfying the following conditions: the diagonal blocks of (7), i.e. operators $\sqrt{XX^\dagger}$, $\sqrt{X^\dagger X}$, $\sqrt{YY^\dagger}$, $\sqrt{Y^\dagger Y}$ are all PPT-invariant, i.e., must satisfy $A = A^\Gamma$. (Relation (8) and PPT-invariance of the diagonal blocks are necessary to obtain simple conditions for the state to be PPT, given in section 3.2.)

In particular, the PPT-invariance of the diagonal blocks holds for

$$X = \frac{1}{u}\sum_{i,j=0}^{d-1} u_{ij}|ij\rangle\langle ji| \tag{9}$$

where u_{ij} are elements of some unitary matrix on $\mathcal{C}^d$ and

$$u = \sum_{i,j=0}^{d-1} |u_{ij}|. \tag{10}$$

For the operator X given by (9) we have

$$\|X^\Gamma\| = \frac{d}{u}, \qquad \frac{1}{\sqrt{d}} \leqslant \|X^\Gamma\| \leqslant 1 \tag{11}$$

where the minimum is achieved for the unimodular unitary [1] and the maximum for the identity matrix.

We will sometimes write ϱ_U to denote the subclass of class $\mathcal{C}$ with the operator X given by (9) or to stress using a concrete unitary in the definition of X; in particular, we will consider the subclass ϱ_H where u_{ij} are elements of the Hadamard unitary matrix.

In the case of $d = 2$ we will also consider the subclass of class $\mathcal{C}$ with operators X and Y given by

$$Y = qY_{U_1} + (1-q)\sigma_x^{A'} Y_{U_2} \sigma_x^{A'}, \quad X = \frac{Y^\Gamma}{\|Y^\Gamma\|} \tag{12}$$

where

$$Y_U = \frac{1}{d}\sum_{i,j=0}^{d-1} u_{ij}|ii\rangle\langle jj|. \tag{13}$$

Unitaries U_1 and U_2 must have the same global phase, i.e. $\alpha_1 = \alpha_2$ in the parametrization of a single-qubit unitary given by (A.1) in the appendix. In particular, one may take $U_1 = U_2$.

We also use an alternative parametrization in terms of p, α and β given by

$$p \equiv \lambda_1 + \lambda_2 \in [0, 1] \tag{14}$$

$$\alpha \equiv \frac{\lambda_1 - \lambda_2}{\lambda_1 + \lambda_2} \in [-1, 1] \tag{15}$$

$$\beta \equiv \frac{\lambda_3 - \lambda_4}{\lambda_3 + \lambda_4} \in [-1, 1]. \tag{16}$$

On the other hand, the original parameters λ_i can be expressed using p, α and β as follows:

$$\lambda_{1,2} = \frac{1 \pm \alpha}{2} p \tag{17}$$

$$\lambda_{3,4} = \frac{1 \pm \beta}{2} (1 - p). \tag{18}$$

Both parametrizations are directly related to the privacy-squeezed version of the states given by (5) and (6), and constructed according to formula (4):

$$\sigma = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| = \frac{1}{2} \begin{bmatrix} p & & & \alpha p \\ & (1-p) & \beta(1-p) & \\ & \beta(1-p) & (1-p) & \\ \alpha p & & & p \end{bmatrix} \tag{19}$$

where the Bell states ψ_i are given by

$$\begin{aligned} |\psi_{1,2}\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\psi_{3,4}\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned} \tag{20}$$

Thus, λ_i are the eigenvalues of the privacy-squeezed state, p reports the balance between correlations and anti-correlations, while α and β report how coherences are damped.

A subclass of class $\mathcal{C}$ with X defined by (9) has been considered in [1]:

$$\tilde{\varrho} = \lambda_1 \gamma_1^+ + \lambda_3 \gamma_2^+. \tag{21}$$

Class $\mathcal{C}$ is much wider than (21); in particular, it contains key-distillable PPT states arbitrary close to the separable states, but this comes with a price: we have to, in general, use the recurrence preprocessing to obtain a positive key rate for (5) while for (21) the sole Devetak–Winter protocol is enough [1].

3.2. *Sufficient PPT conditions*

For the states of class $\mathcal{C}$ to be PPT (so that maximal entanglement cannot be distilled from them) it is sufficient to satisfy the following conditions:

$$|\lambda_1 - \lambda_2| \leqslant (1 - \lambda_1 - \lambda_2) \|X^\Gamma\|^{-1} \tag{22}$$

$$|\lambda_3 - \lambda_4| \leqslant (\lambda_1 + \lambda_2) \|X^\Gamma\| \tag{23}$$

or equivalently

$$|\alpha| \leqslant \min(1, \alpha_1) \tag{24}$$

$$|\beta| \leqslant \min\left(1, \alpha_1^{-1}\right) \tag{25}$$

where

$$\alpha_1 = \frac{1-p}{p}\|X^\Gamma\|^{-1}. \tag{26}$$

In particular, if $p = \tilde{\lambda}_1$ where $\tilde{\lambda}_1$ is given by (27), we have $\alpha_1 = 1$. Moreover, if $\alpha = \alpha_1\beta$ then ϱ is a PPT-invariant state.

For the subclass (21), the above PPT conditions collapse to a single PPT-invariant state, on the boundary of PPT states, which satisfies

$$\lambda_1 = \tilde{\lambda}_1 \equiv \frac{1}{1+\|X^\Gamma\|}. \tag{27}$$

3.3. Key distillability

We shall derive here a general sufficient condition for key distillability of the spider states with a Bell diagonal privacy-squeezed state, which easily follows from combining the privacy squeezing technique with the result of [11] on key distillation from two-qubit states. It is enough for our purposes, as states of our class are of that form. (In section 7 we extend the key-distillability condition to arbitrary states by exploiting twirling.)

Proposition 1. *Let ϱ be a state of the form*

$$\varrho = \begin{bmatrix} C & & & D \\ & E & F & \\ & F^\dagger & E' & \\ D^\dagger & & & C' \end{bmatrix} \tag{28}$$

satisfying $\|C\| = \|C'\|$ and $\|E\| = \|E'\|$, i.e. ϱ is a state having a Bell diagonal privacy-squeezed state. If

$$\max(\|D\|, \|F\|) > \sqrt{\|C\|\|E\|}, \tag{29}$$

then Alice and Bob can distill the cryptographic key by first measuring the key part of many copies of the state ϱ and then using the recurrence [22, 23] and Devetak–Winter protocol [24].

Remark 1. Note that, interestingly, condition (29) is equivalent to requiring that one of the matrices

$$\begin{bmatrix} \|C\| & \|D\| \\ \|D^\dagger\| & \|E\| \end{bmatrix}, \qquad \begin{bmatrix} \|C\| & \|F\| \\ \|F^\dagger\| & \|E\| \end{bmatrix} \tag{30}$$

is not a positive one.

Remark 2. Note that the right-hand side of equation (29) can also be written as $\frac{1}{2}\sqrt{p_e(1-p_e)}$ where p_e is the probability of error (i.e. anticorrelation) when the key part is measured in the standard basis.

Proof of proposition 1. We apply the privacy squeezing technique described in section 2, i.e. we show that the privacy-squeezed state of ϱ is key distillable by a protocol based on measuring the state locally in the standard basis and classical postprocessing. This implies that ϱ is also key distillable.

The privacy-squeezed state is precisely of the form (4) with $\|C\| = \|C'\|$ and $\|E\| = \|E'\|$, i.e. it is a Bell diagonal state which can be written as

$$\sigma = \frac{1}{2}\begin{bmatrix} a & & & d \\ & e & f & \\ & f & e & \\ d & & & a \end{bmatrix}. \tag{31}$$

For such a state it was shown in [11] that if $\max(|d|, |f|) > \sqrt{ae}$ then one can distill the key by measuring the state locally in the standard basis, and processing the resulting classical data (actually, by using the recurrence followed by the Devetak–Winter protocol). This is precisely the type of protocol allowed by the privacy-squeezing technique described in section 2. In our case, the above conditions are simply the ones given in (29). ☐

Due to the form (19) of the privacy-squeezed state of the states from our class, we immediately obtain suitable conditions:

Corollary 1. *Let ϱ be a state defined by formulas (5) and (6) with arbitrary X and Y satisfying $\|X\| = \|Y\| = 1$. If*

$$|\lambda_1 - \lambda_2| > \sqrt{(\lambda_1 + \lambda_2)(1 - \lambda_1 - \lambda_2)} \tag{32}$$

or equivalently if

$$|\alpha| > \sqrt{\frac{1-p}{p}}, \tag{33}$$

then Alice and Bob can distill the cryptographic key by first measuring the key part of many copies of the state ϱ and then using the recurrence and the Devetak–Winter protocol.

Corollary 1 also holds if one uses $|\lambda_3 - \lambda_4|$ as the left-hand side of (32) or equivalently $|\beta|$ as the left-hand side of (33); however, in our paper, we do not use these conditions.

Observation 1. *For a state of class $\mathcal{C}$ to be both PPT and key distillable using corollary 1 it must satisfy both (24) and (33). For a given value of the parameter p there exists α satisfying both conditions iff $p \in (\frac{1}{2}, p_{\max})$ where*

$$p_{\max} = \frac{1}{1 + \|X^\Gamma\|^2}. \tag{34}$$

3.4. Tolerable white noise

We consider that δ is the *tolerable noise* of a key distillation protocol for a state ϱ if for any $\epsilon < \delta$ the state ϱ_ϵ with ϵ of the white noise admixtured

$$\varrho_\epsilon = (1 - \epsilon)\varrho + \epsilon\frac{I}{d^2} \tag{35}$$

remains key distillable with that protocol.

Having $p > \frac{1}{2}$, the tolerable noise of the Devetak–Winter protocol with the recurrence preprocessing for class $\mathcal{C}$ is given by

$$\delta = 1 - \frac{1}{\sqrt{8\left(\lambda_1^2 + \lambda_2^2\right) - 4(\lambda_1 + \lambda_2) + 1}} \tag{36}$$

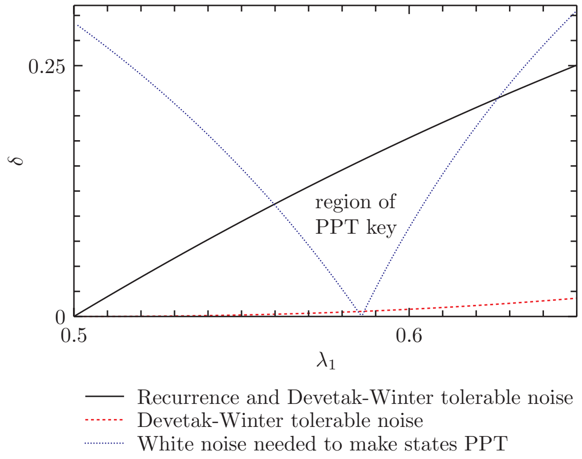

Figure 1. Comparison of $\tilde{\varrho}_H$ tolerable noise in the case of using the Devetak–Winter protocol with and without the recurrence preprocessing.

$$= 1 - \frac{1}{\sqrt{4\left(1+\alpha^2\right)p^2 - 4p + 1}}. \tag{37}$$

In particular for a key-distillable PPT state $\tilde{\varrho}_H$ with $\lambda_1 = \tilde{\lambda}_1$ where $\tilde{\lambda}_1$ is given by (27) the tolerable noise for the Devetak–Winter protocol with the recurrence preprocessing (36) is approximately equal to 0.155 while for the sole Devetak–Winter protocol it is approximately equal to 0.005, i.e. it is 31 times smaller. See figure 1.

3.5. *Separability*

Given a state ϱ_U of class $\mathcal{C}$ with X given by (9) and $d = 2$, i.e. ϱ is a state of $4 \otimes 4$ system, we may try to decompose ϱ into a mixture of four two-qubit states. The particular decomposition, which we propose below, is possible if

$$|\lambda_3 - \lambda_4| \leqslant (1 - \lambda_1 - \lambda_2)\|X^\Gamma\| \tag{38}$$

or equivalently if

$$|\beta| \leqslant \|X^\Gamma\|. \tag{39}$$

All of the four two-qubit states in our decomposition are Bell diagonal states with the same set of eigenvalues. Thus, the two qubit states are separable (and, hence, ϱ is separable) if all their eigenvalues are less than or equal to $\frac{1}{2}$.[4] For our decomposition this occurs if, additionally to (38), the following conditions are satisfied:

$$\lambda_1 \leqslant \tfrac{1}{2} \tag{40}$$

$$\lambda_2 \leqslant \tfrac{1}{2} \tag{41}$$

$$|\lambda_3 - \lambda_4| \leqslant (\lambda_1 + \lambda_2)\|X^\Gamma\| \tag{42}$$

---

[4] This can be directly verified by the positivity of the partial transpose [29, 30].

or equivalently, additionally to (39), the following conditions are satisfied:

$$|\alpha| \leqslant \frac{1-p}{p} \tag{43}$$

$$|\beta| \leqslant \frac{p}{1-p}\|X^\Gamma\|. \tag{44}$$

Note that conditions (42) and (44) are identical to the PPT conditions for ϱ given by (23) and (25), respectively.

The decomposition into the four two-qubit states has the form

$$\begin{aligned} \varrho_U = {} & \frac{|u_{00}|}{u}\varrho_{00}(|00\rangle_{AA'}, |10\rangle_{AA'}; |00\rangle_{BB'}, |10\rangle_{BB'}) \\ & + \frac{|u_{01}|}{u}\varrho_{01}(|00\rangle_{AA'}, |11\rangle_{AA'}; |01\rangle_{BB'}, |10\rangle_{BB'}) \\ & + \frac{|u_{10}|}{u}\varrho_{10}(|01\rangle_{AA'}, |10\rangle_{AA'}; |00\rangle_{BB'}, |11\rangle_{BB'}) \\ & + \frac{|u_{11}|}{u}\varrho_{11}(|01\rangle_{AA'}, |11\rangle_{AA'}; |01\rangle_{BB'}, |11\rangle_{BB'}) \end{aligned} \tag{45}$$

where u_{ij} are the elements of the unitary matrix on $\mathcal{C}^2$ used to define the operator X in (9), u is given by (10) and ϱ_{ij} denote the two-qubit states given by

$$\varrho_{ij} = \frac{1}{2}\begin{bmatrix} \lambda_1+\lambda_2 & & & (\lambda_1-\lambda_2)e^{i\phi_{ij}} \\ & \lambda_3+\lambda_4 & (\lambda_3-\lambda_4)\|X^\Gamma\|^{-1}e^{i\phi_{ij}} & \\ & (\lambda_3-\lambda_4)\|X^\Gamma\|^{-1}e^{-i\phi_{ij}} & \lambda_3+\lambda_4 & \\ (\lambda_1-\lambda_2)e^{-i\phi_{ij}} & & & \lambda_1+\lambda_2 \end{bmatrix} \tag{46}$$

where ϕ_{ij} comes from the polar decomposition of u_{ij}

$$u_{ij} = |u_{ij}|e^{i\phi_{ij}}. \tag{47}$$

The local basis of Alice and Bob for each of the two-qubit states are given in (45) in parentheses.

3.6. *PPT key arbitrary close to separability*

One can obtain key from some $4 \otimes 4$ PPT states lying arbitrary close to the set of separable states. That is, one can easily select a single-parameter subclass of class $\mathcal{C}$ satisfying PPT conditions and approaching some separable state with $p = \frac{1}{2}$ such that for any other state in this class, no matter how close to the separable state, the key condition (33) is satisfied. Note that if we chose a separable state with $p \neq \frac{1}{2}$ as the final state the key condition would be violated before reaching that final state; thus, we would not approach with the key-distillable states arbitrary close to the set of separable states.

Such a class of states, a subclass of ϱ_H, is illustrated in figure 2. The dashed line represents the subclass $\tilde{\varrho}_H$, given by (21), a mixture of two pbits (γ_1^+ and γ_2^+) which in alternate parametrization is equivalent to $p \in [0, 1]$ and $\alpha = \beta = 1$. As shown in [1], this class contains exactly one (boundary) PPT entangled state obtained by setting $p = \tilde{\lambda}_1$ where $\tilde{\lambda}_1$ is given by (27), otherwise the states are NPT.

The solid line represents a class of PPT key-distillable states obtained by setting $p \in (\frac{1}{2}, p_{\max})$, $\alpha = \min(1, \alpha_1)$ and $\beta = \min\left(1, \alpha_1^{-1}\right)$, where $p_{\max} = (1 + \|X^\Gamma\|^2)^{-1} = \frac{2}{3}$, see observation 1, while α_1 is given by (26), i.e. $\alpha_1 = \frac{1-p}{p}\sqrt{2}$ in the considered case. In the range

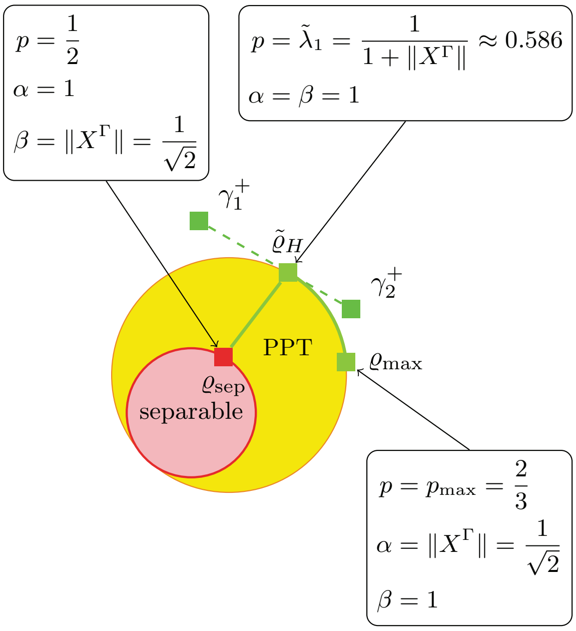
$p = \frac{1}{2}$
$\alpha = 1$
$\beta = \|X^\Gamma\| = \frac{1}{\sqrt{2}}$
$p = \tilde\lambda_1 = \frac{1}{1+\|X^\Gamma\|} \approx 0.586$
$\alpha = \beta = 1$
γ_1^+
$\tilde\varrho_H$
γ_2^+
PPT
$\varrho_{\max}$
ϱ_{sep}
separable
$p = p_{\max} = \frac{2}{3}$
$\alpha = \|X^\Gamma\| = \frac{1}{\sqrt{2}}$
$\beta = 1$

Figure 2. A class of key-distillable PPT entangled states: (*a*) the solid line from $\tilde\varrho$ on the boundary of the PPT entangled states (inclusive) to the boundary of the set of separable states, arbitrary close to ϱ_{sep}; (*b*) the arc of PPT-invariant states starting in $\tilde\varrho$ and approaching arbitrary close to $\tilde\varrho_{\max}$.

$p \in (\frac{1}{2}, \tilde\lambda_1]$ the class is represented as a straight line from the PPT state of the previous class $\tilde\varrho_H$ on one end ($p = \tilde\lambda_1$) and approaches arbitrary close to the separable state ϱ_{sep} ($p = \frac{1}{2}$) on the other end. In the range $p \in [\tilde\lambda_1, p_{\max})$ the states are PPT-invariant and lie on the boundary of PPT entangled states; they are represented as an arc from the PPT state of the previous class $\tilde\varrho_H$ on one end ($p = \tilde\lambda_1$) and approach arbitrary close to the state $\varrho_{\max}$ ($p = p_{\max}$) on the other end. In the range $p \in (\tilde\lambda_1, p_{\max})$ one could take $\alpha < \alpha_1$, such that the key condition (33) is still satisfied, to enter inside the class of PPT states.

4. States ϱ_H as mixtures of Bell states with 'flags'

States of the class ϱ_H are separable in the $AB : A'B'$ cut, i.e. subsystems AB and $A'B'$ of ϱ_H are only classically correlated. A state from ϱ_H can be decomposed into a mixture of four states. Each of the four states has a Bell state ψ_i on the subsystem AB and some corresponding state on $A'B'$.

One can select parameters $p \in [0, 1]$, $\alpha \in [-1, 1]$, and $\beta \in [-1, 1]$ satisfying both the PPT conditions (24) and (25) and the key condition (33), and prepare a corresponding PPT key-distillable state from the class ϱ_H which has the form

$$\varrho_H = \sum_{i=1}^{4} q_i |\psi_i\rangle\langle\psi_i|_{AB} \otimes \varrho_{A'B'}^{(i)} \tag{48}$$

where the Bell states ψ_i are given by (20) and the correlated states are as follows:

$$\varrho^{(1)} = \alpha\frac{1}{2}(P_{00} + P_{\psi_3}) + (1-\alpha)\frac{I}{4} \tag{49}$$

$$\varrho^{(2)} = \alpha\frac{1}{2}(P_{11} + P_{\psi_4}) + (1-\alpha)\frac{I}{4} \tag{50}$$

$$\varrho^{(3,4)} = \beta P_{\chi_\pm} + (1-\beta)\tfrac{1}{2}(P_{00} + P_{11}) \tag{51}$$

where P_ψ denotes the projector onto a pure state ψ and

$$\chi_\pm = \frac{1}{\sqrt{2\pm\sqrt{2}}}(|00\rangle \pm |\psi_1\rangle) \tag{52}$$

$$q_1 = q_2 = \frac{p}{2} \tag{53}$$

$$q_3 = q_4 = \frac{1-p}{2}. \tag{54}$$

5. Maximizing von Neumann entropy

In this section, we find $4\otimes 4$ key-distillable PPT states with a quite high von Neumann entropy for two subclasses of class $\mathcal{C}$ and summarize the results in the table in section 5.3.

5.1. *For states of the class ϱ_U*

Here, we find the supremum of the von Neumann entropy of the subclass ϱ_U of class $\mathcal{C}$ with X given by (9) consisting of states that are both PPT and key distillable by corollary 1. Let us denote this set of states as $\mathcal{PK}_d$, subscripted with the dimension of the unitary used to define the operator X.

As ϱ is a mixture of four orthogonal private bits its von Neumann entropy is given by

$$S(\varrho_U) = H(p) + p\left(H\left(\frac{1-\alpha}{2}\right) + S(\sqrt{X^\dagger X})\right) + (1-p)\left(H\left(\frac{1-\beta}{2}\right) + S(\sqrt{Y^\dagger Y})\right) \tag{55}$$

where

$$S(\sqrt{X^\dagger X}) \leqslant 2\log_2 d \tag{56}$$

$$S(\sqrt{Y^\dagger Y}) = \log_2 d \tag{57}$$

and the maximal value in (56) is achieved if the unitary used to define X in (9) is unimodular. A unimodular unitary also maximizes the allowed range of p given by observation 1, as it achieves a minimum of $\|X^\Gamma\|$. Hence, to maximize the entropy, it is enough to consider a unimodular unitary. The supremum is achieved for a state with $p = p_{\max}$, $\beta = 0$ and $\alpha = \sqrt{\frac{1-p}{p}}$ (which no longer satisfies our key-distillability condition); thus,

$$\sup_{\varrho_U\in\mathcal{PK}_d} S(\varrho_U) = \sup_{p\in(\frac{1}{2},p_{\max})}\left((1+p)\log_2 d + (1-p) + H(p) + pH\left(\frac{1-\sqrt{\frac{1-p}{p}}}{2}\right)\right) \tag{58}$$

where $p_{\max} = (1+\|X^\Gamma\|^2)^{-1}$ comes from observation 1.

In particular, for $d = 2$, i.e. ϱ being $4\otimes 4$ states, the supremum is achieved for the state having $p = p_{\max} = 2/3$ which gives

$$\sup_{\varrho_U\in\mathcal{PK}_2} S(\varrho_U) \approx 3.319. \tag{59}$$

The supremum corresponds to a state $\varrho_{\max}$ in figure 2 but with $\beta = 0$.

5.2. *For states of a class larger than ϱ_U*

For the subclass ϱ of class $\mathcal{C}$ with $d = 2$ and X and Y given by (12), we are able to obtain

$$S(\varrho) \approx 3.524 \tag{60}$$

for $U_1 = U_2 = H$, $q \approx 0.683$, $\beta = 0$ and α, p taken as in the previous subsection. It seems to be the supremum of the von Neumann entropy for this selection of operators X and Y.

5.3. *Summary*

Here, we summarize the results of maximizing von Neumann entropy of $4 \otimes 4$ key-distillable PPT states in the following table:

$S(\varrho)$	ϱ satisfying PPT and key conditions
2.564	Class $\tilde{\varrho}$ from [1] with $p = \tilde{\lambda}_1$, the maximum is achieved for $U = H$
3.319	Class ϱ_U, the supremum is described in section 5.1
3.524	Class $\mathcal{C}$ with Y given by (12), a supposed supremum is described in section 5.2

6. Distillability channel via erasure

In [19], it was shown that two zero-capacity channels, if combined together, can have nonzero capacity. One of the channels was related (through the so-called Choi–Jamiołkowski (CJ) isomorphism) to a bound entangled but key-distillable state, while the other was a so-called symmetrically extendable channel. In particular, they considered an example, where the first channel had the $4 \otimes 4$ CJ state from class (21) while the second one was the 50% erasure channel. In [25] a simpler scheme was proposed, which also allows us to observe this curious phenomenon.

The second approach amounts to sending a subsystem A' of a state defined in systems $ABA'B'$ through the 50% erasure channel and checking the coherent information of the resulting state. If it is positive one concludes that the capacity of a combined channel is also positive. Here, we shall use this approach to see how the presence of coherence β influences the phenomenon.

Coherent information after sending the A' subsystem through the 50% erasure channel is given by

$$I_{\mathrm{coh}} = \tfrac{1}{2}(S_{A'BB'} - S) + \tfrac{1}{2}(S_{BB'} - S_{ABB'}) \tag{61}$$

where S, $S_{A'BB'}$ and $S_{BB'}$ are given by (55), (62) and (63), respectively.

For a PPT state $\tilde{\varrho}$ given by (21) with X given by (9) and based on unimodular unitary and $\lambda_1 = \tilde{\lambda}_1$, where $\tilde{\lambda}_1$ is given by (27), the coherent information is positive starting from $d = 11$. For a similar state of our class with $p = \tilde{\lambda}_1$, $\alpha = 1$ and $\beta = 0$ the coherent information is positive starting from $d = 22$.

Formulas for $S_{A'BB'}$ and $S_{BB'}$ are as follows:

$$S(\varrho_{A'BB'}) = 1 + \tfrac{1}{2} S\left(p\sqrt{XX^\dagger} + (1-p)\sqrt{Y^\dagger Y}\right) \quad + \tfrac{1}{2} S\left(p\sqrt{X^\dagger X} + (1-p)\sqrt{YY^\dagger}\right) \tag{62}$$

$$S(\varrho_{BB'}) = 1 + \tfrac{1}{2} S_B\left(p\sqrt{XX^\dagger} + (1-p)\sqrt{Y^\dagger Y}\right) \quad + \tfrac{1}{2} S_B\left(p\sqrt{X^\dagger X} + (1-p)\sqrt{YY^\dagger}\right). \tag{63}$$

7. Condition for drawing a secure key from general states

From section 3.3, we have a sufficient condition for drawing the key in terms of norms of the nonzero blocks from states having a Bell diagonal privacy-squeezed state. In this section, we generalize that condition to the case of an arbitrary state.

Let us define two twirling operations (cf [23])

$$\Lambda_{XX} = \tfrac{1}{2}\big(\hat{I} \otimes \hat{I} + \hat{X} \otimes \hat{X}\big) \tag{64}$$

$$\Lambda_{ZZ} = \tfrac{1}{2}\big(\hat{I} \otimes \hat{I} + \hat{Z} \otimes \hat{Z}\big) \tag{65}$$

and one twirling with flags

$$\Lambda'_{XX}(\varrho) = \tfrac{1}{2}\big(\varrho \otimes |0\rangle\langle 0| + \hat{X} \otimes \hat{X}(\varrho) \otimes |1\rangle\langle 1|\big) \tag{66}$$

where $\hat{U}\varrho = U\varrho U^\dagger$ and X and Z are Pauli matrices.

Now, we give a sufficient condition to obtain the key from a general state.

Proposition 2. *For an arbitrary state*

$$\varrho = \begin{bmatrix} A & B & C & D \\ B^\dagger & E & F & G \\ C^\dagger & F^\dagger & H & I \\ D^\dagger & G^\dagger & I^\dagger & J \end{bmatrix} \tag{67}$$

if

$$\max(\|D\|, \|F\|) > \tfrac{1}{2}\sqrt{(\|A\| + \|J\|)(\|E\| + \|H\|)} \tag{68}$$

then Alice and Bob can distill the cryptographic key by first applying twirling $\Lambda'_{XX} \circ \Lambda_{ZZ}$ to the key part, measuring the key part of many copies of the state ϱ and then using the recurrence and the Devetak–Winter protocol.

Remark 3. Note that the right-hand side of equation (68) can also be written as $\frac{1}{2}\sqrt{p_e(1 - p_e)}$ where p_e is the probability of error (i.e. anticorrelation) when the key part is measured in standard basis.

Proof of proposition 2. Alice and Bob first apply twirling $\Lambda'_{XX} \circ \Lambda_{ZZ}$ (an LOCC operation) and obtain the following state:

$$\Lambda'_{XX} \circ \Lambda_{ZZ}(\varrho) = \begin{bmatrix} A \oplus J & & & D \oplus D^\dagger \\ & E \oplus H & F \oplus F^\dagger & \\ & F \oplus F^\dagger & E \oplus H & \\ D \oplus D^\dagger & & & A \oplus J \end{bmatrix}. \tag{69}$$

This state is now of the spider form and, thanks to flags, we have direct sums within the blocks. Now, the privacy-squeezed state has the following Bell diagonal form:

$$\sigma = \begin{bmatrix} \|A\| + \|J\| & & & \|D\| + \|D^\dagger\| \\ & \|E\| + \|H\| & \|F\| + \|F^\dagger\| & \\ & \|F\| + \|F^\dagger\| & \|E\| + \|H\| & \\ \|D\| + \|D^\dagger\| & & & \|A\| + \|J\| \end{bmatrix}. \tag{70}$$

Then the proof follows from proposition 1. □

Note that in the proof above we use Λ'_{XX}, a twirling with flags. If Λ_{XX}, a twirling without flags, was used instead, we would have to replace $\|D\|$ with $\|D + D^\dagger\|$ in (68) (analogously for $\|F\|$) which can be much smaller than $\|D\|$, and even equal to zero in the extreme case of anti-Hermitian D, i.e. $D^\dagger = -D$, so in this case no key can be distilled from $\Lambda_{XX}(\varrho)$ even if ϱ is a private state, i.e. $\varrho = \gamma(D)$.

Note also that in the proof, we have first applied twirling with flags to the original state, and then the privacy-squeezing operation. Actually, the same state would be obtained if we first apply the privacy squeezing and then apply (standard) twirling. This is illustrated by the following diagram:

$$\begin{tikzcd}
\varrho \arrow[r, "\Lambda'_{XX}\circ\Lambda_{ZZ}"] \arrow[d, "P_{sq}"'] & \varrho' \arrow[d, "P_{sq}"] \\
\sigma \arrow[r, "\Lambda_{XX}\circ\Lambda_{ZZ}"] & \sigma'
\end{tikzcd} \tag{71}$$

where P_{sq} stands for privacy squeezing. As explained above, this diagram would not commute if we used solely twirling without flags. Thus, to seek key-distillable states, one can go the alternative route, i.e. first compute the privacy-squeezed state, and then, by twirling, obtain a Bell diagonal state. Now, if $\Lambda_{XX} \circ \Lambda_{ZZ}(\sigma)$ satisfies the necessary security condition for realistic QKD on a Pauli channel from [11], i.e. its eigenvalues λ_i satisfy (32), then ϱ is key distillable using proposition 2.

Acknowledgments

The work is supported by the Polish Ministry of Science and Higher Education grant no. 3582/B/H03/2009/36 and by the European Commission through the Integrated Project FET/QIPC QESSENCE. This work was done at the National Quantum Information Centre of Gdańsk.

Appendix

The parametrization of a single-qubit unitary [26]

$$U = \mathrm{e}^{\mathrm{i}\alpha}\begin{bmatrix} \mathrm{e}^{\mathrm{i}\left(-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\left(\frac{\gamma}{2}\right) & -\mathrm{e}^{\mathrm{i}\left(-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\left(\frac{\gamma}{2}\right) \\ \mathrm{e}^{\mathrm{i}\left(\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\left(\frac{\gamma}{2}\right) & \mathrm{e}^{\mathrm{i}\left(\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\left(\frac{\gamma}{2}\right) \end{bmatrix}. \tag{A.1}$$

References

[1] Horodecki K, Pankowski Ł, Horodecki M and Horodecki P 2008 Low dimensional bound entanglement with one-way distillable cryptographic key *IEEE Trans. Inf. Theory* **54** 2621–5 (arXiv:quant-ph/0506203)

[2] Wiesner S 1983 Conjugate coding *Sigact News* **15** 78–88

[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing (Bangalore, India, December 1984)* (New York: IEEE Computer Society Press) pp 175–9

[4] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3

[5] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4 (arXiv:quant-ph/0003004)

[6] Gisin N and Wolf S 2000 Linking classical and quantum key agreement: Is there 'bound information'? *CRYPTO 2000: Advances in Cryptology* (Berlin: Springer) pp 482–500 (arXiv:quant-ph/0005042)

[7] Horodecki M, Horodecki P and Horodecki R 1998 Mixed-state entanglement and distillation: Is there a 'bound' entanglement in nature? *Phys. Rev. Lett.* **80** 5239–42 (arXiv:quant-ph/9801069)

[8] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Secure key from bound entanglement *Phys. Rev. Lett.* **94** 160502 (arXiv:quant-ph/0309110)

[9] Augusiak R and Horodecki P 2009 Multipartite secret key distillation and bound entanglement *Phys. Rev.* A **80** 042307 (arXiv:0811.3603 [quant-ph])

[10] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2009 General paradigm for distilling classical key from quantum states *IEEE Trans. Inf. Theory* **55** 1898–929 (arXiv:quant-ph/0506189)

[11] Acín A, Bae J, Bagan E, Baig M, Masanes Ll and Muñoz-Tapia R 2006 Secrecy content of two-qubit states *Phys. Rev.* A **73** 012327 (arXiv:quant-ph/0411092)

[12] Bae J 2010 Secret key distillation from shielded two-qubit states *Phys. Rev.* A **81** 052320 (arXiv:0803.0345 [quant-ph])

[13] Chi D P, Choi J W, Kim J S, Kim T and Lee S 2007 Bound entangled states with a nonzero distillable key rate *Phys. Rev.* A **75** 032306 (arXiv:quant-ph/0612225v4)

[14] Amselem E and Bourennane M 2009 Experimental four-qubit bound entanglement *Nature Phys.* **5** 748–52

[15] Lavoie J, Kaltenbaek R, Piani M and Resch K J 2010 Experimental bound entanglement in a four-photon state arXiv:1005.1258v2 [quant-ph]

[16] Kampermann H, Bruß D, Peng X and Suter D 2010 Experimental generation of pseudo bound-entanglement *Phys. Rev.* A **81** 040304 (arXiv:0909.2743 [quant-ph])

[17] Barreiro J T, Schindler P, Gühne O, Monz T, Chwalla M, Roos C F, Hennrich M and Blatt R 2010 Experimental multiparticle entanglement dynamics induced by decoherence arXiv:1005.1965 [quant-ph]

[18] DiGuglielmo J, Samblowski A, Hage B, Pineda C, Eisert J and Schnabel R 2010 Preparing the bound instance of entanglement arXiv:1006.4651 [quant-ph]

[19] Smith G and Yard J 2008 Quantum communication with zero-capacity channels *Science* **321** 1812–5 (arXiv:0807.4935 [quant-ph])

[20] Gottesman D and Hoi-Kwong L 2003 Proof of security of quantum key distribution with two-way classical communications *IEEE Trans. Inf. Theory* **49** 457–75 (arXiv:quant-ph/0105121)

[21] Renner R 2005 Security of quantum key distribution arXiv:quant-ph/0512258

[22] Maurer U M 1993 Secret key agreement by public discussion from common information *IEEE Trans. Inf. Theory* **39** 733–42

[23] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction *Phys. Rev.* A **54** 3824–51 (arXiv:quant-ph/9604024)

[24] Devetak Igor and Winter Andreas 2005 Distillation of secret key and entanglement from quantum states *Proc. R. Soc.* A **461** 207–35 (arXiv:quant-ph/0306078)

[25] Oppenheim J 2008 For quantum information, two wrongs can make a right *Science* **321** 1783–4

[26] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[27] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942 (arXiv:quant-ph/0702225v2)

[28] Pankowski L, Piani M, Horodecki M and Horodecki P 2010 A few steps more towards NPT bound entanglement *IEEE Trans. Inf. Theory* **56** 4085–100 (arXiv:0711.2613 [quant-ph])

[29] Peres A 1996 Separability criterion for density matrices *Phys. Rev. Lett.* **77** 1413–5

[30] Horodecki M, Horodecki P and Horodecki R 1996 Separability of mixed states: necessary and sufficient conditions *Phys. Lett.* A **223** 1 (arXiv:quant-ph/9605038)