Quantum privacy witness

Konrad Banaszek
Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski, Hoża 69, PL-00-681 Warszawa, Poland

Karol Horodecki
Instytut Informatyki, Universytet Gdański, PL-80-952 Gdańsk, Poland

Paweł Horodecki
Wydział Fizyki Technicznej i Matematyki Stosowanej, Politechnika Gdańska, PL-80-952 Gdańsk, Poland

(Received 20 September 2011; published 27 January 2012)

While it is usually known that the mean value of a single observable is enough to detect entanglement or its distillability, the counterpart of such an approach in the case of quantum privacy has been missing. Here we develop the concept of a privacy witness, i.e., a single observable that may detect the presence of the secure key even in the case of bound entanglement. Then we develop the notion of secret-key estimation based on few observables and discuss the witness decomposition into local measurements. The surprising property of the witness is that with the help of a low number of product measurements involved it may still report the key values that are *strictly above* distillable entanglement of the state. For an exemplary four-qubit state studied in a recent experiment [K. Dobek *et al.*, Phys. Rev. Lett. **106**, 030501 (2011)] this means 6 Pauli operator product measurements versus 81 needed to carry out the complete quantum state tomography. The present approach may be viewed as a paradigm for the general program of experimentally friendly detection and estimation of task-dedicated quantum entanglement.

DOI: 10.1103/PhysRevA.85.012330 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

Entanglement-based cryptography [1], equivalent formally to the Bennett-Brassard 1984 protocol (BB84) scheme [2], uses the power of quantum entanglement monogamy obeyed by a maximally entangled pure quantum state. If the state is noisy, then in some cases it is possible to run an entanglement distillation process [3], which may be interpreted as quantum privacy amplification [4]. Since the final output is maximally entangled, it may be used directly for secret-key generation. The efficiency of this procedure is quantified with distillable entanglement E_D, which defines how many singlet states can be obtained in the asymptotic regime per one input.

Still, it was known that certain states that cannot be prepared by local operations and classical communication (LOCC) are not distillable, exhibiting the phenomenon of bound entanglement [5]. For a long time, bound entanglement was believed to be useless for cryptography, but several years ago it was shown [6,7] that at least some bound entangled states may be useful in quantum cryptography. This is one extreme instance of the general fact that the amount of distillable secure key K_D may exceed the amount of distillable singlets E_D. The latter effect has been verified in a recent experiment [8].

The key ingredient in the complete theory of distilling a secret key from quantum states [6,7] is the notion of a *private bit* (pbit), or, more generally, a *private dit* (pdit), which is a delocalized maximally entangled state that still retains some entanglement monogamy result. A quantum pdit is composed from a $d \otimes d$ key part AB and the shield part $A'B'$ shared between Alice (subsystems AA') and Bob (subsystems BB') in such a way that the local von Neumann measurements on the key part in a *particular* basis will make the results completely statistically uncorrelated from the results of any measurement of an eavesdropper Eve on her subsystem E, which is a part of the purification $|\Psi\rangle_{ABA'B'E}$ of the pdit state $\hat{\varrho}_{ABA'B'}$. There is a nice explanation of how the shield part protects the statistics of the measurement on A and B to be correlated to Eve: it just makes it impossible to distinguish the results of the measurement by an external observer.

An obvious way to determine privacy properties is to reconstruct tomographically the complete pdit state $\hat{\varrho}_{ABA'B'}$. This, however, is a very time-consuming process, especially if the system under investigation is high-dimensional. The aim of the present paper is to give bounds on the distillable secure key based on just a few observables. This advances further the study presented in Ref. [9], where it was proposed to carry out a tomography of the so-called privacy-squeezed state of the state of merit. We demonstrate that a single observable suffices to provide a nontrivial bound. We also provide more accurate estimates based on two observables. These results provide tools for application-specific detection of entanglement, refining the fundamental concept of the entanglement witness proposed in Refs. [10,11], which can be also subjected to optimization with respect to local measurements [12,13] and used to quantify the amount of entanglement [14,15].

The present results can be viewed as an outcome of a more general research program: experimentally friendly detection or estimation of task-dedicated quantum entanglement and/or correlations. In fact it is quite usual that we are interested in that aspect of entanglement which is useful for specific quantum information task. The quantity characterizing this aspect may be a monotone, but we believe that it need not be in general. For instance, it is known that there are cases when specific Bell inequalities that are important for device independent cryptography are better violated by nonmaximally entangled states. In this context we believe that the present paradigm will lead to systematic development of experimentally friendly detection or estimation of resources for quantum information tasks.

This paper is organized as follows. In Sec. II we elaborate on lower bounds on distillable entanglement and the distillable key. In Sec. III we present a lower bound on the distillable key in terms of a single parameter, i.e., a single privacy witness. An approximate version of this bound is presented in the Appendix. In Sec. IV we discuss how to infer privacy of a noisy state from the expectation values of two observables. Finally, Sec. V concludes the paper.

II. KEY BOUNDS

Let us start by reviewing how an individual observable can be used to estimate distillable entanglement E_D. The most natural observable in this context is a projector

$$\hat{W}_{\text{ent}} = |\Psi_{\max}\rangle\langle\Psi_{\max}| \tag{1}$$

onto a maximally entangled state $|\Psi_{\max}\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|\phi_i\rangle_A \otimes |\psi_i\rangle_B$ of two d-level systems, where $\{|\phi_i\rangle_A\}$ and $\{|\psi_i\rangle_B\}$ are any two orthonormal bases. Following the idea of Ref. [3] dealing with the case $d = 2$, there is a protocol for an arbitrary d such that if $F(\hat{\varrho}_{AB}) = \text{Tr}(\hat{W}_{\text{ent}}\hat{\varrho}_{AB}) = \langle\Psi_{\max}|\hat{\varrho}_{AB}|\Psi_{\max}\rangle$ satisfies $F(\hat{\varrho}_{AB}) > \frac{1}{d}$, then the state $\hat{\varrho}_{AB}$ is distillable [16].

The corresponding rate of the distillation protocol can be easily estimated from below by the hashing protocol [17,18], which gives a lower bound for the distillable entanglement as

$$E_D(\hat{\varrho}_{AB}) \geqslant S(\hat{\varrho}_B) - S(\hat{\varrho}_{AB}), \tag{2}$$

where $S(\cdot)$ denotes the von Neumann entropy.

Since an application of the so-called $U \otimes U^*$ twirling [16] can only decrease distillable entanglement E_D, we may twirl the state $\hat{\varrho}_{AB}$ in order to bring it to a highly symmetric form and then apply the hashing inequality (2), which eventually gives

$$E_D(\hat{\varrho}_{AB}) \geqslant \log_2 d - H\left(F, \frac{1-F}{d^2-1}, \ldots, \frac{1-F}{d^2-1}\right), \tag{3}$$

where $F = F(\hat{\varrho}_{AB})$ and $H(\{p_i\}) = -\sum_i p_i \log_2 p_i$ is the Shannon entropy.

The above formula is valid for any bipartite quantum state $\hat{\varrho}_{AB}$. There are more sophisticated twirling protocols. For instance, for two qubits there is a protocol [19] utilizing selected random Pauli operations that brings the state to a form diagonal in the Bell basis:

$$\hat{\varrho}_{AB}^{\text{Bell}} = \sum_{i=1}^{4} p_i |\Psi_i\rangle\langle\Psi_i|, \tag{4}$$

where $|\Psi_i\rangle$ are Bell states. Applying the hashing protocol to $\hat{\varrho}_{AB}^{\text{Bell}}$ leads to

$$E_D(\hat{\varrho}_{AB}) \geqslant 1 - H(p_1, p_2, p_3, p_4). \tag{5}$$

Equations (3) and (5) provide bounds on the key rate for $\hat{\varrho}_{AB}$, as distilled singlet states can be used for the standard Ekert protocol. In general, however, this may not be the most efficient way to generate the key.

As pointed out in the Introduction, there exists a straightforward way to verify that we have a pdit, or a state sufficiently close to a pdit, from which the secret key may be distilled. It is based on the so-called quantum state tomography, which allows us to calculate specific entropic functions that can be used to estimate the amount of the secret key from below. A useful quantity is the Devetak-Winter function $K_{DW}^{\rightarrow}$, which quantifies the secret key distillable through a specific one-way secret-key distillation protocol:

$$K_D(\hat{\varrho}_{ABA'B'}) \geqslant K_{DW}^{\rightarrow}(\hat{\varrho}_{ABA'B'}). \tag{6}$$

The Devetak-Winter function is given explicitly by the difference of two Holevo quantities χ_{AB} and χ_{AE}, which characterize the amount of information that can be recovered, respectively, by Bob and Eve from subsystems B and E after Alice carried out a von Neumann measurement of subsystem A in the secure basis $\{|i\rangle_A\}$:

$$K_{DW}^{\rightarrow}(\hat{\varrho}_{ABA'B'}) = \chi_{AB}\left(\text{Tr}_E\hat{\varrho}_{ABE}^{\text{cqq}}\right) - \chi_{AE}\left(\text{Tr}_B\hat{\varrho}_{ABE}^{\text{cqq}}\right). \tag{7}$$

The state $\hat{\varrho}_{ABE}^{\text{cqq}}$ is given by

$$\hat{\varrho}_{ABE}^{\text{cqq}} = \text{Tr}_{A'B'}\Bigg(\sum_i (|i\rangle_A\langle i| \otimes \hat{\mathbb{1}}_{A'BB'E}) \times |\Psi\rangle_{AA'BB'E}\langle\Psi|(|i\rangle_A\langle i| \otimes \hat{\mathbb{1}}_{A'BB'E})\Bigg). \tag{8}$$

Let us now restrict our attention to a situation when the key part is composed of two qubits, A and B. The complete density matrix $\hat{\varrho}_{ABA'B'}$ can be written as a 4×4 array of blocks $\hat{A}_{ij,kl} = {}_{AB}\langle ij|\hat{\varrho}_{ABA'B'}|kl\rangle_{AB}$:

$$\hat{\varrho}_{ABA'B'} = \begin{pmatrix} \hat{A}_{00,00} & \hat{A}_{00,01} & \hat{A}_{00,10} & \hat{A}_{00,11} \\ \hat{A}_{01,00} & \hat{A}_{01,01} & \hat{A}_{01,10} & \hat{A}_{01,11} \\ \hat{A}_{10,00} & \hat{A}_{10,01} & \hat{A}_{10,10} & \hat{A}_{10,11} \\ \hat{A}_{11,00} & \hat{A}_{11,01} & \hat{A}_{11,10} & \hat{A}_{11,11} \end{pmatrix}. \tag{9}$$

It can be transformed by LOCC (with respect to the partition $AA' : BB'$) to the form

$$\hat{\hat{\varrho}} = \begin{pmatrix} \frac{1}{2}(\hat{A}_{00,00} + \hat{A}_{11,11}) & 0 & 0 & \frac{1}{2}(\hat{A}_{00,11} + \hat{A}_{11,00}) \\ 0 & \frac{1}{2}(\hat{A}_{01,01} + \hat{A}_{10,10}) & \frac{1}{2}(\hat{A}_{01,10} + \hat{A}_{10,01}) & 0 \\ 0 & \frac{1}{2}(\hat{A}_{01,10} + \hat{A}_{10,01}) & \frac{1}{2}(\hat{A}_{01,01} + \hat{A}_{10,10}) & 0 \\ \frac{1}{2}(\hat{A}_{00,11} + \hat{A}_{11,00}) & 0 & 0 & \frac{1}{2}(\hat{A}_{00,00} + \hat{A}_{11,11}). \end{pmatrix}. \tag{10}$$

This state can be "untwisted" to a Bell diagonal matrix that is directly related to the privacy-squeezed state (see [7,9]):

$$\hat{\sigma}_{AB} = \begin{pmatrix} \frac{1}{2}||\hat{A}_{00,00}+\hat{A}_{11,11}|| & 0 & 0 & \frac{1}{2}||\hat{A}_{00,11}+\hat{A}_{11,00}|| \\ 0 & \frac{1}{2}||\hat{A}_{01,01}+\hat{A}_{10,10}|| & \frac{1}{2}||\hat{A}_{01,10}+\hat{A}_{10,01}|| & 0 \\ 0 & \frac{1}{2}||\hat{A}_{01,10}+\hat{A}_{10,01}|| & \frac{1}{2}||\hat{A}_{01,01}+\hat{A}_{10,10}|| & 0 \\ \frac{1}{2}||\hat{A}_{00,11}+\hat{A}_{11,00}|| & 0 & 0 & \frac{1}{2}||\hat{A}_{00,00}+\hat{A}_{11,11}|| \end{pmatrix}, \tag{11}$$

where the norm $||\cdot||$ stands for the trace norm.

It will be convenient to write $\hat{\sigma}_{AB}$ in the form

$$\hat{\sigma}_{AB} = \begin{pmatrix} \frac{1}{2}(p_1+p_2) & 0 & 0 & \frac{1}{2}(p_1-p_2) \\ 0 & \frac{1}{2}(p_3+p_4) & \frac{1}{2}(p_3-p_4) & 0 \\ 0 & \frac{1}{2}(p_3-p_4) & \frac{1}{2}(p_3+p_4) & 0 \\ \frac{1}{2}(p_1-p_2) & 0 & 0 & \frac{1}{2}(p_1+p_2) \end{pmatrix}. \tag{12}$$

It is easy to see that $\hat{\sigma}_{AB}$ is diagonal in the Bell basis and the parameters p_i are occupation probabilities of the corresponding Bell states.

There is a useful bound on the secret key, which is [9]

$$\begin{aligned} K_D(\hat{\varrho}_{ABA'B'}) &\geqslant I_{\text{cl}}(A:B) - S(\hat{\sigma}_{AB}) \\ &= 1 - h(p_1+p_2) - H(p_1,p_2,p_3,p_4). \end{aligned} \tag{13}$$

Here $I_{\text{cl}}(A:B)$ is the classical mutual information for the outcomes of von Neumann measurements carried out by Alice and Bob in the secure basis $|00\rangle_{AB}, |01\rangle_{AB}, |10\rangle_{AB}, |11\rangle_{AB}$. As the joint probability distribution for these outcomes is $\{\frac{1}{2}(p_1+p_2), \frac{1}{2}(p_3+p_4), \frac{1}{2}(p_3+p_4), \frac{1}{2}(p_1+p_2)\}$, we have $I_{\text{cl}}(A:B) = 1 - h(p_1+p_2)$, where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ denotes the binary entropy. For other bounds, see [20].

Note that the bound given in Eq. (13) is weaker than that on distillable entanglement in Eq. (5), but the physical meaning of the probability distribution $p_1,\ldots,p_4$ is different. In the present case the state $\hat{\sigma}_{AB}$ does not actually describe the physical system at any stage of the protocol but is rather a formal construct characterizing privacy properties of the state $\hat{\varrho}_{ABA'B'}$ of the complete system $ABA'B'$.

III. SINGLE PRIVACY WITNESS

The class of secrecy witnesses we shall consider here is defined formally as

$$\begin{aligned} \hat{W}_{\text{priv}} &= (|11\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11|) \otimes \hat{U}_{A'B'} \\ &= \tfrac{1}{2}\left(\hat{\sigma}_A^x \otimes \hat{\sigma}_B^x - \hat{\sigma}_A^y \otimes \hat{\sigma}_B^y\right) \otimes \hat{U}_{A'B'}, \end{aligned} \tag{14}$$

where $\hat{U}_{A'B'} \equiv \hat{U}$ is any Hermitian matrix satisfying $\hat{U}\hat{U}^\dagger \leqslant \hat{\mathbb{1}}$ acting on the shield subsystems A' and B'.

We will use the expectation value of the privacy witness $\langle \hat{W}_{\text{priv}} \rangle$ to approximate the value of $p_1 - p_2$. In fact we have

$$\begin{aligned} w := |\langle \hat{W}_{\text{priv}} \rangle| &= |\text{Tr}[(\hat{A}_{00,11} + \hat{A}_{11,00})\hat{U}]| \\ &\leqslant ||\hat{A}_{00,11} + \hat{A}_{11,00}|| = p_1 - p_2 \end{aligned} \tag{15}$$

since, for any matrix satisfying $\hat{U}\hat{U}^\dagger \leqslant \hat{\mathbb{1}}$ and any $\hat{A}$, one has $\text{Tr}(\hat{A}\hat{U}) \leqslant ||\hat{A}||$. The most straightforward way to verify this fact is to resort to the definition of the trace norm:

$$\text{Tr}\hat{A}\hat{U} \leqslant ||\hat{A}\hat{U}|| = \sqrt{\text{Tr}\hat{U}\hat{U}^\dagger\hat{A}^\dagger\hat{A}} \leqslant \sqrt{\text{Tr}\hat{A}^\dagger\hat{A}} = ||\hat{A}||. \tag{16}$$

Sometimes the parameter w may give exactly the value of $p_1 - p_2$, and then we shall call $\hat{W}_{\text{priv}}$ optimal. The unitary operation $\hat{U}$ defining such an optimal witness is just a Hermitian conjugate of the unitary operation diagonalizing the operator $(\hat{A}_{00,11} + \hat{A}_{11,00})^\dagger(\hat{A}_{00,11} + \hat{A}_{11,00})$. We will give an instance of the optimal witness and the corresponding $\hat{U}$ at the end of this section. Let us also stress that the witness itself (14) is an observable, which must be measured on the original state (9).

Quantitative estimation of the distillable key will be based on the inequality

$$H(p_1,p_2,p_3,p_4) \leqslant H\big(p_1,p_2,\tfrac{1}{2}(1-p_1-p_2),\tfrac{1}{2}(1-p_1-p_2)\big) \tag{17}$$

applied to Eq. (13), which yields

$$\begin{aligned} K_D \geqslant 1 - h(p_1+p_2) - H\big(&p_1,p_2,\tfrac{1}{2}(1-p_1-p_2), \\ &\tfrac{1}{2}(1-p_1-p_2)\big). \end{aligned} \tag{18}$$

As we are interested in the most pessimistic scenario, we need to minimize the right-hand side over pairs (p_1,p_2) that satisfy all the constraints. This gives the *central formula*:

$$\begin{aligned} K_D \geqslant 1 - \sup_{\substack{p_1-p_2\geqslant w \\ p_1,p_2\geqslant 0,\, p_1+p_2\leqslant 1}} &\big[h(p_1+p_2) \\ &+ H\big(p_1,p_2,\tfrac{1}{2}(1-p_1-p_2),\tfrac{1}{2}(1-p_1-p_2)\big)\big]. \end{aligned} \tag{19}$$

We found numerically the boundary value w^* at which the above bound becomes strictly positive, i.e., the witness condition $w = |\langle \hat{W}_{\text{priv}} \rangle| > w^*$, to be equal to $w^* \approx 0.907$.

We can simplify the optimization in Eq. (19) by introducing a new pair of variables, $p_+ = p_1 + p_2$ and $\xi_+ = p_1/(p_1+p_2)$.

A straightforward calculation shows that the bound for the key expressed in the new variables takes the form

$$K_D \geqslant \inf_{\substack{w\leqslant p_+\leqslant 1\\ (w+p_+)/2p_+\leqslant \xi_+\leqslant 1}} [p_+ - 2h(p_+) - p_+ h(\xi_+)]. \tag{20}$$

Because the lower limit for ξ_+ is greater or equal to 1/2, optimization over ξ_+ for a fixed value of p_+ yields $h(\xi_+) \leqslant h((w+p_+)/2p_+)$. Consequently, the minimization in Eq. (20) needs to be carried out over a single parameter p_+:

$$K_D \geqslant \inf_{w\leqslant p_+\leqslant 1} [p_+ - 2h(p_+) - p_+ h((w+p_+)/2p_+)]. \tag{21}$$

The absolute minimum of this expression is analyzed in the Appendix. However, we can simplify the bound in two ways, leading to weaker but more compact formulas.

Weaker bound 1. Suppose that $w \geqslant (1-w)/3$, which is equivalent to $w \geqslant 1/4$. Then we have the following estimate:

$$K_D \geqslant 1 - h(w) - H\big(w, \tfrac{1}{3}(1-w), \tfrac{1}{3}(1-w), \tfrac{1}{3}(1-w)\big). \tag{22}$$

In the last inequality we have used the fact that both $p_1 + p_2 \geqslant w$ and $p_1 \geqslant w$.

Weaker bound 2. There is a possibility of having another bound with the help of subadditivity of the entropy $H[p_1,p_2,p_3,p_4] \leqslant h(p_1+p_2) + h(p_1+p_3)$, which yields

$$K_D \geqslant 1 - 2h(w) - h\big(\tfrac{1}{2}(1+w)\big). \tag{23}$$

For a graphic comparison of the derived formulas, see Fig. 1.

The above considerations are based on the so-called ccq scenario, i.e. such that Alice and Bob measure their qubits in the secure key basis $|0\rangle, |1\rangle$. However, the optimal $\hat{U}$ [i.e., the one that saturates (15)] remains unchanged if we transform the key part of the given state by local unitary transformation. More specifically, if we rotate the state $\hat{\varrho}_{ABA'B'}$, given in Eq. (9) with optimal witness of the form (14), by the operation $\hat{U}_A \otimes \hat{U}_B \otimes \hat{I}_{A'} \otimes \hat{I}_{B'}$, where $\hat{U}_A \otimes \hat{U}_B |ij\rangle = |e_i f_j\rangle$, then the optimal witness $\hat{W}'$ for a new state ρ' is $\hat{W}' = (|e_0 f_0\rangle\langle e_1 f_1| + |e_1 f_1\rangle\langle e_0 f_0|) \otimes \hat{U}_{A'B'}$, where $\hat{U}_{A'B'}$ is the same as in $\hat{W}_{\text{priv}}$. Let us give here an example of when we know the optimal $\hat{U}$. In the case of the four-qubit state whose approximate version was realized experimentally in Ref. [8], a two-qubit swap operator $\hat{V}_{A'B'} = \hat{\mathbb{1}}_{A'B'} - 2|\Psi_-\rangle_{A'B'}\langle\Psi_-|$ used in the privacy witness would give *exactly* the value $|\langle\hat{W}_{\text{priv}}\rangle| = p_1 - p_2$. Note also that if $\hat{U}$ were not Hermitian, we could decompose $\hat{U} = \hat{U}_R + i\hat{U}_I$ and measure two observables $\hat{W}^R_{\text{priv}} = (|11\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11|) \otimes \hat{U}_R$ and $\hat{W}^I_{\text{priv}} = (|11\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11|) \otimes \hat{U}_I$.

IV. TWO-OBSERVABLE PRIVACY ESTIMATION

In this section we will show how to characterize the privacy properties of a noisy entangled state from expectation values of two observables. The first one, given by $\hat{\sigma}^z_A \otimes \hat{\sigma}^z_B \otimes \hat{\mathbb{1}}_{A'B'}$, characterizes correlations between measurements performed on the subsystems A and B in the key basis. The security of the key will be inferred by combining its expectation value with that of an observable $\hat{\sigma}^x_A \otimes \hat{\sigma}^x_B \otimes \hat{U}_{A'B'}$, which probes off-diagonal blocks of the density matrix $\hat{\varrho}_{ABA'B'}$.

In further discussion it will be convenient to use the following parametrization of $\hat{\sigma}_{AB}$:

$$\hat{\sigma}_{AB} = \begin{pmatrix} \frac{1}{2}p_+ & 0 & 0 & p_+\big(\xi_+ - \frac{1}{2}\big) \\ 0 & \frac{1}{2}p_- & p_-\big(\xi_- - \frac{1}{2}\big) & 0 \\ 0 & p_-\big(\xi_- - \frac{1}{2}\big) & \frac{1}{2}p_- & 0 \\ p_+\big(\xi_+ - \frac{1}{2}\big) & 0 & 0 & \frac{1}{2}p_+ \end{pmatrix}. \tag{24}$$

The nonnegative parameters $p_+ = p_1 + p_2$ and $p_- = 1 - p_+ = p_3 + p_4$ can be interpreted as occupation probabilities of the correlated and the anticorrelated subspaces, spanned respectively by pairs or vectors $|00\rangle_{AB}$, $|11\rangle_{AB}$ and $|01\rangle_{AB}$,$|10\rangle_{AB}$. The other two parameters, given explicitly by $\xi_+ = p_1/p_+$ and $\xi_- = p_3/p_-$, characterize the off-diagonal elements of $\hat{\sigma}_{AB}$, respectively, in the correlated and the anticorrelated sectors and therefore contain information about the privacy properties. Because the off-diagonal elements of $\hat{\sigma}_{AB}$ are nonnegative due to the definition given in Eq. (11) and must ensure positive definiteness of $\hat{\sigma}_{AB}$, the parameters ξ_-,ξ_+ satisfy the inequality

$$\tfrac{1}{2} \leqslant \xi_+,\xi_- \leqslant 1, \tag{25}$$

i.e., the relevant region for pairs (ξ_-,ξ_+) has the geometric shape of a square.

In the new parametrization, the lower bound on the key takes the following form:

$$K_D \geqslant 1 - 2h(p_+) - p_+ h(\xi_+) - p_- h(\xi_-). \tag{26}$$

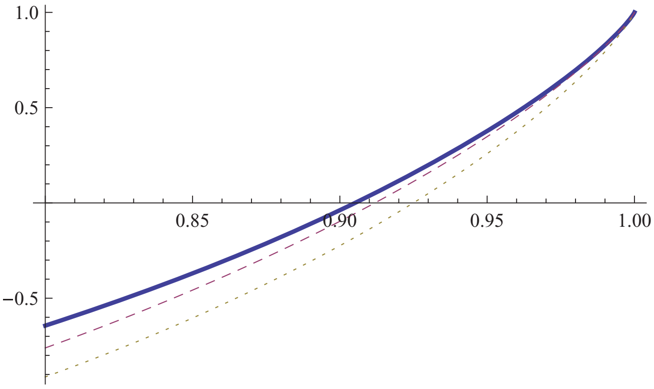


FIG. 1. (Color online) Graphs of lower bounds on the distillable key as a function of $w = |\langle\hat{W}_{\text{priv}}\rangle|$ derived in Eqs. (19) (solid line), (22) (dashed line), and (23) (dotted line).

Because the binary entropies $h(\xi_+)$ and $h(\xi_-)$ are nonnegative, a necessary condition for this bound to be nontrivial is $h(p_+) < \frac{1}{2}$; otherwise, the right-hand side is not positive. This means that p_+ must satisfy either $0 \leqslant p_+ < 1 - p^*$ or $p^* < p_+ \leqslant 1$, where $p^* \approx 0.89$ is the bigger of two solutions of a transcendental equation $h(p^*) = \frac{1}{2}$ on the interval $0 \leqslant p^* \leqslant 1$. We will restrict our further discussion to the case $p^* < p_+ \leqslant 1$, as the analysis of the second case $0 \leqslant p_+ < 1 - p^*$ is completely analogous.

Let us now analyze how the parameters of $\hat{\sigma}_{AB}$ are related to measured observables. The parameters $p_\pm$ can be evaluated directly from the measured observables as $p_\pm = \frac{1}{2}(1 \pm \langle \hat{\sigma}_A^z \otimes \hat{\sigma}_B^z \otimes \hat{\mathbb{1}}_{A'B'} \rangle)$. Following the discussion after Eq. (26), we will be interested in the regime when $p_+ > p^*$. Considering the other regime when $p_+ < 1 - p^*$ effectively boils down to swapping the roles of the correlated and the anticorrelated subspaces. These two possibilities can be analyzed jointly by defining

$$w_z := \left| \langle \hat{\sigma}_A^z \otimes \hat{\sigma}_B^z \otimes \hat{\mathbb{1}}_{A'B'} \rangle \right| \tag{27}$$

and using in further discussion

$$p_\pm = \tfrac{1}{2}(1 \pm w_z). \tag{28}$$

The condition $p_+ > p^*$ can be equivalently written as

$$w_z > 2p^* - 1 \approx 0.78, \tag{29}$$

which defines the minimum value of w_z above which the bound on the key can become nontrivial.

The second quantity we will use in our analysis will be

$$w_x := \left| \langle \hat{\sigma}_A^x \otimes \hat{\sigma}_B^x \otimes \hat{U}_{A'B'} \rangle \right|. \tag{30}$$

It allows us to bound the parameters ξ_- and ξ_+ according to the following inequality, which is at the heart of our reasoning:

$$\begin{aligned} w_x &= |\mathrm{Tr}[\hat{U}(\hat{A}_{00,11} + \hat{A}_{01,10} + \hat{A}_{10,01} + \hat{A}_{11,00})]| \\ &\leqslant ||\hat{A}_{00,11} + \hat{A}_{11,00}|| + ||\hat{A}_{01,10} + \hat{A}_{10,01}|| \\ &= p_+(2\xi_+ - 1) + p_-(2\xi_- - 1). \end{aligned} \tag{31}$$

For fixed $p_\pm$, this inequality determines the allowed region of (ξ_-,ξ_+) within the square defined by Eq. (25) as

$$p_-\xi_- + p_+\xi_+ \geqslant \tfrac{1}{2}(1 + w_x). \tag{32}$$

When evaluating the lower bound on the key rate K_D according to Eq. (26), we are interested in the worst-case scenario that is consistent with the measurement results. Therefore our task is to minimize the right-hand side of Eq. (26) under constraints given by Eqs. (25) and (32). This is equivalent to maximizing under the same constraints a concave function

$$f(\xi_-,\xi_+) = p_- h(\xi_-) + p_+ h(\xi_+). \tag{33}$$

The lower bound on the key can be written as

$$K_D \geqslant 1 - 2h(p_+) - f^{\max}, \tag{34}$$

where $f^{\max}$ is the maximum of $f(\xi_-,\xi_+)$ over the allowed region of parameters. It is useful to note that because $f(\xi_-,\xi_+)$ is a convex linear combination of binary entropies $h(\xi_-)$ and $h(\xi_+)$, within the square given by Eq. (25), decreasing either of the arguments ξ_- or ξ_+ will always increase the value of $f(\xi_-,\xi_+)$. This in turn implies that $f^{\max}$ is reached on the line

$$p_-\xi_- + p_+\xi_+ = \tfrac{1}{2}(1 + w_x). \tag{35}$$

To proceed with the maximization, let us start from an observation that if $\xi_+ = \frac{1}{2}$, i.e., the correlated sector of the density matrix has zero off-diagonal elements, no positive key rate can be guaranteed by Eq. (26). This follows from the straightforward fact that the expression $1 - 2h(p_+) - p_+$ is nonpositive for $p^* < p_+ \leqslant 1$. Therefore no point with $\xi_+ = \frac{1}{2}$ should satisfy Eq. (32). Because the slope of the line (35) is negative, it is sufficient to require that the point $(\xi_- = 1, \xi_+ = \frac{1}{2})$ is outside the allowed region. This is equivalent to the inequality

$$2w_x + w_z > 1. \tag{36}$$

Further analysis depends on whether the point $(\xi_- = \frac{1}{2}, \xi_+ = 1)$ is located within the allowed region of parameters. It is easy to verify that this is determined by the relation between p_+ and w_x. If $p_+ > w_x$, this point satisfies Eq. (32), and the allowed region of parameters has the shape of a trapezoid, as shown in Fig. 2(a). Consequently, all values $\frac{1}{2} \leqslant \xi_- \leqslant 1$ are allowed. On the other hand, when $p_+ \leqslant w_x$, the allowed region is a triangle, as depicted in Fig. 2(b). The minimum allowed value of ξ_- is then $(w_x - w_z)/(1 - w_z)$. We can combine these two cases by defining

$$\xi_-^{\min} = \max\left\{ \frac{1}{2}, \frac{w_x - w_z}{1 - w_z} \right\}. \tag{37}$$

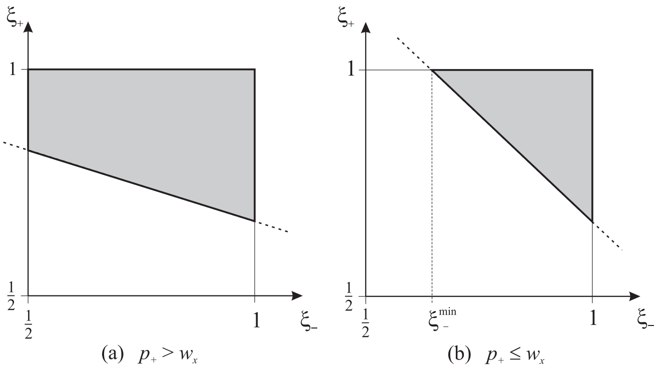
The maximization of $f(\xi_-,\xi_+)$ over the line defined in Eq. (35) can now be written as a supremum over a single parameter:

$$f^{\max} = \sup_{\xi_-^{\min} \leqslant \xi \leqslant 1} f\left(\xi, \frac{1 + w_x}{1 + w_z} - \xi \frac{1 - w_z}{1 + w_z} \right), \tag{38}$$

which, inserted into Eq. (34), yields the final form of the bound:

$$\begin{aligned} K_D \geqslant 1 - 2h(p_+) - \sup_{\xi_-^{\min} \leqslant \xi \leqslant 1} \Bigg[&(1 - p_+) h(\xi) \\ &+ p_+ h\left(\frac{1 + w_x}{1 + w_z} - \xi \frac{1 - w_z}{1 + w_z} \right) \Bigg], \end{aligned} \tag{39}$$

where $p_+ = (1 + w_z)/2$. The results of a numerical evaluation of the supremum are shown in Fig. 3(a).



(a) $p_+ > w_x$ (b) $p_+ \leq w_x$

FIG. 2. The permitted region of the parameters (ξ_-,ξ_+) used to maximize the function $f(\xi_-,\xi_+)$ defined in Eq. (33).

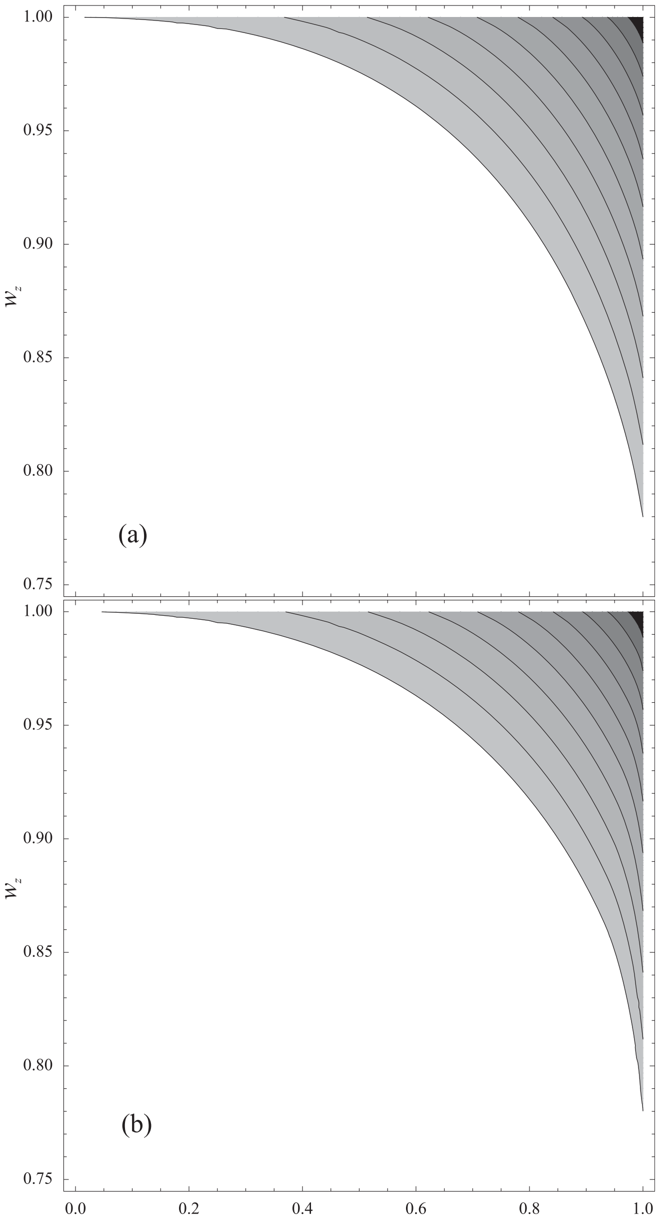


FIG. 3. The lower bound on the key as a function of w_x and w_z obtained from (a) full optimization over the free parameters specified in Eq. (39) and (b) a weaker estimate according to Eq. (42). The bound is positive in the shaded area, with solid contours drawn at steps of 0.1 starting from 0.

It is also possible to derive a slightly weaker bound that requires no numerical optimization. Because the function $f(\xi_-,\xi_+)$ is monotonic in each one of its two arguments, as discussed after Eq. (34), we can estimate $f^{\max}$ by $\tilde{f}^{\max}$, defined as

$$f^{\max} \leqslant \tilde{f}^{\max} = f(\xi_-^{\min},\xi_+^{\min}), \tag{40}$$

where $\xi_-^{\min}$ and $\xi_+^{\min}$ are the smallest possible values of ξ_- and ξ_+ within the allowed region defined by Eqs. (25) and (32). The value $\xi_-^{\min}$ has been given explicitly in Eq. (37), and it is easy to verify that

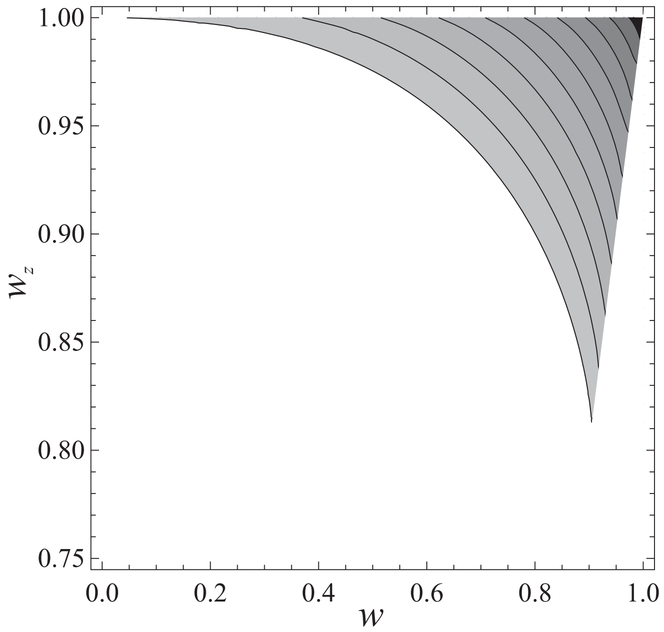


FIG. 4. The lower bound on the key given in Eq. (44) obtained from observables w and w_z. The physical region is restricted to points (w,w_z), satisfying the condition $(1+w_z)/2 \geqslant w$. The coding of the bound value is the same as in Fig. 3.

$$\xi_+^{\min} = \frac{w_x + w_z}{1+w_z}. \tag{41}$$

The simplified bound therefore takes the following explicit form:

$$K_D \geqslant 1 - 2h(p_+) - (1-p_+)h(\xi_-^{\min}) - p_+ h\left(\frac{w_x+w_z}{1+w_z}\right), \tag{42}$$

which is shown in Fig. 3(b).

Finally, let us note that the observable w defined in Eq. (15) can be combined with w_z to provide a stronger bound on the distillable key. To obtain this bound, let us return to Eq. (26) and estimate the last two terms on the right-hand side. The inequality shown in Eq. (15) rewritten in the new parametrization provides a lower bound on ξ_+:

$$\xi_+ \geqslant \frac{1}{2} + \frac{w}{2p_+}. \tag{43}$$

Because the right-hand side is greater than or equal to $1/2$, we have $h(\xi_+) \leqslant h(1/2 + w/2p_+)$. Further, we obviously have $h(\xi_-) \leqslant 1$. This yields

$$K_D \geqslant p_+[1 - h(1/2 + w/2p_+)] - 2h(p_+). \tag{44}$$

Let us note that physical values of w and w_z must satisfy the condition $(1+w_z)/2 \geqslant w$; otherwise, we would have $p_1 + p_2 = p_+ = (1+w_z)/2 < w \leqslant p_1 - p_2$ and, consequently, $p_2 < 0$. In Fig. 4 we depict the bound (44) in the physical region of w and w_z.

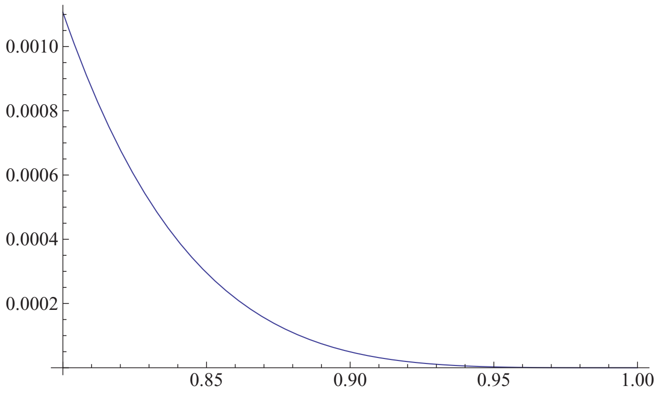


FIG. 5. (Color online) The difference between the bounds from Eqs. (20) and (A3) as a function of the parameter w.

V. DISCUSSION AND CONCLUSIONS

In this paper we have introduced a privacy witness, i.e., an observable, whose mean value allows one to estimate nontrivially from below the value of a secret key, even in the case when the resulting state exhibits the separation of the secret key and the distillable entanglement. In fact this separation may be quite drastic while the witness is working perfectly. To see this let us take $A'B'$ being $d \otimes d$-level systems and consider a pbit state $\varrho_{ABA'B'}$ in the form [6]

$$\hat{\varrho}_{ABA'B'} = \frac{1}{2d^2}[(|00\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|) \otimes \hat{\mathbb{1}}_{A'B'} + (|00\rangle_{AB}\langle 11| + |11\rangle_{AB}\langle 00|) \otimes \hat{V}_{A'B'}], \quad (45)$$

where $\hat{\mathbb{1}}_{A'B'}$ and $\hat{V}_{A'B'}$ stand, respectively, for the bipartite identity and the swap operator on the subsystems $A'B'$. In the limit of large d the distillable entanglement is bounded by vanishing log negativity $E_D \leqslant \log_2(1 + \frac{1}{d}) \to 0$, while the privacy witness $\hat{W}_{\text{priv}} = \frac{1}{2}(\hat{\sigma}_A^x \otimes \hat{\sigma}_B^x - \hat{\sigma}_A^y \otimes \hat{\sigma}_B^y) \otimes \hat{V}_{A'B'}$ gives us the value of lower bound $K_D \geqslant 1$ since $w = \text{Tr}(\hat{W}_{\text{priv}}\hat{\varrho}_{ABA'B'}) = 1$, and then just using either of the weaker bounds given in Eqs. (22) and (23) does the job. Note, in particular, that since the key part AB is a two-qubit part, the above estimate gives the maximum possible value of the secret key $K_D = \log_2 2 = 1$ despite the fact that the distillable entanglement of the state is almost zero.

In general the complexity of measuring the privacy witness is related to the Hilbert-Schmidt decomposition of the Hermitian operator $\hat{U}$ used to construct the witness [12]. In the case of the four-qubit state that was studied in the experiment reported in Ref. [8] the operator in question is the swap operator, which is composed of three terms involving products of Pauli matrices:

$$\hat{V}_{A'B'} = \tfrac{1}{2}\big(\hat{\mathbb{1}}_{A'B'} + \hat{\sigma}_{A'}^x \otimes \hat{\sigma}_{B'}^x + \hat{\sigma}_{A'}^y \otimes \hat{\sigma}_{B'}^y + \hat{\sigma}_{A'}^z \otimes \hat{\sigma}_{B'}^z\big). \quad (46)$$

Taking into account the necessary measurements on the key part, this gives in total $2 \times 3 = 6$ observables to be measured, each formed by a product of four Pauli matrices. This is dramatically fewer then the full tomography, which requires 81 products of four Pauli matrices. Note that in some cases, such as the pbit state discussed above, such an apparently poor measurement has no problem in reporting the key value that lies above the distillable entanglement, which is bounded for our example by the log negativity value $E_D(\varrho) \leqslant \log_2(1 + \frac{1}{2}) \approx 0.585$.

The above approach may be extended to higher dimensions, and other twirling techniques may be applied. It may be especially useful when the experimentalist has a good guess about the expected pbit state in the laboratory; then he or she may estimate the high key contents almost perfectly even if there is virtually no distillable entanglement in the system. Finally, let us note that the very difficult problem is to find the nonlinear entanglement witness that would capture collective behavior revealing the key in all the cases when any single-copy entropic function based on a one-way protocol fails. It seems that for this one needs quantum secrecy distillation protocols of new generation.

We believe that the present approach will lead to general and systematic development of experimentally friendly methods for detection and estimation of task-dedicated quantum entanglement and other resources.

ACKNOWLEDGMENT

This work was supported by 7th Framework Programme Future and Emerging Technologies projects CORNER (Grant No. 213681) and Q-ESSENCE (Grant No. 248095). K.H. is supported by Grant BW No. 538-5300-0637-1, and P.H. is supported by Grant No. NN 202-261-938. We acknowledge useful discussions with R. Demkowicz-Dobrzański.

APPENDIX: SINGLE-WITNESS BOUND

Let us denote

$$\kappa(p_+) = p_+ - 2h(p_+) - p_+ h((p_+ + w)/2p_+). \quad \text{(A1)}$$

The derivative with respect to p_+ reads

$$\frac{d\kappa}{dp_+} = \frac{1}{2}\log_2 \frac{p_+^2(p_+^2 - w^2)}{(1 - p_+)^4}. \quad \text{(A2)}$$

It is easy to see that on the interval $w \leqslant p_+ \leqslant 1$ the argument of the logarithm function runs from 0 to $+\infty$. Therefore $\kappa(p_+)$ reaches its minimum at a root of a polynomial equation $p_+^2(p_+^2 - w^2) = (1 - p_+)^4$. This is a cubic equation that can be solved exactly, but a simplified formula can be found by substituting $p_+ = w + \delta$ and assuming that $\delta \ll 1 - w$, which is motivated by numerical analysis. This yields $\delta \approx (1 - w)^4/2w^3$ and, consequently, the bound on the key in the approximate form

$$K_D \geqslant \kappa\left(w + \frac{(1 - w)^4}{2w^3}\right). \quad \text{(A3)}$$

This approximate expression turns out to reproduce the original bound quite tightly, as evidenced in Fig. 5, depicting the difference between Eq. (A3) and the bound given in Eq. (20).

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society Press, New York, 1984), pp. 175–179.

[3] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[4] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[6] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[7] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[8] K. Dobek, M. Karpinski, R. Demkowicz-Dobrzanski, K. Banaszek, and P. Horodecki, Phys. Rev. Lett. **106**, 030501 (2011).

[9] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).

[10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[11] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[12] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).

[13] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, J. Mod. Opt. **50**, 1079 (2003).

[14] R. Horodecki, M. Horodecki, and P. Horodecki, Phys. Rev. A **59**, 1799 (1999).

[15] F. G. S. L. Brandão, Phys. Rev. A **72**, 022310 (2005).

[16] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[17] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).

[18] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[19] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[20] D. P. Chi, J. W. Choi, J. S. Kim, T. Kim, and S. Lee, Phys. Rev. A **75**, 032306 (2007).