Quantum privacy witness

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

Karol Horodecki
Instytut Informatyki, Uniwersytet Gdański, 80-952 Gdańsk, Poland

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

(Dated: September 13, 2011)

The present results can be viewed as an outcome of a more general research program: experimentally friendly detection/estimation of task-dedicated quantum entangle-
ment 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 to be in general. For instance it is known that there are cases when specific Bell inequalities which 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/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 distillable key. In Sec. III we present a lower bound on distillable key in terms of single parameter, i.e., single privacy version. An approximate version of this bound is presented in 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 an individual observable can be used to estimate distillable entanglement $E_D$. The most natural observable in this context is a projector

$$W_{\text{ent}} = |\Psi_{\text{max}}\rangle \langle \Psi_{\text{max}}|$$

onto a maximally entangled state $|\Psi_{\text{max}}\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |\phi_i\rangle_A \otimes |\psi_i\rangle_B$ 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 $F(\hat{\rho}_{AB}) = \text{Tr}(W_{\text{ent}} \hat{\rho}_{AB}) = \langle \Psi_{\text{max}} | \hat{\rho}_{AB} |\Psi_{\text{max}}\rangle$, satisfies $F(\hat{\rho}_{AB}) > \frac{1}{4}$ then the state $\hat{\rho}_{AB}$ is distillable [10].

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

$$E_D(\hat{\rho}_{AB}) \geq S(\hat{\rho}_{B}) - S(\hat{\rho}_{AB})$$

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 $\hat{\rho}_{AB}$ in order to bring it to a highly symmetric form and then apply the hashing inequality [2] which eventually gives:

$$E_D(\hat{\rho}_{AB}) \geq \log_2 d - H \left( F, \frac{1 - F}{d^2 - 1}, ..., \frac{1 - F}{d^2 - 1} \right),$$

where $F = F(\hat{\rho}_{AB})$ 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 $\hat{\rho}_{AB}$. 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:

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

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

$$E_D(\hat{\rho}_{AB}) \geq 1 - H(p_1, p_2, p_3, p_4).$$

Eqs. (5) and (6) provide bounds on the key rate for $\hat{\rho}_{AB}$, as distilled singlet states can be used for the standard Ekert protocol. In general however, this may be not the most efficient way to generate the key.

As pointed out in the introduction, a straightforward way to verify that we have a p-bit or a state close to p-bit enough that the secret key may be distilled. It is based on the so-called quantum state tomography which allows 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 $K_{D\text{W}}$, which quantifies the secret key distillable through a specific one-way secret key distillation protocol:

$$K_D(\hat{\rho}_{ABA'B'}) \geq K_{D\text{W}}(\hat{\rho}_{ABA'B'}).$$

The Devetak-Winter function is given explicitly by the difference of two Holevo quantities $\chi_{AB}$ and $\chi_{AE}$ 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 the subsystem $A$ in the secure basis $\{ \langle i | A \rangle \}$:

$$K_{D\text{W}}(\hat{\rho}_{ABA'B'}) = \chi_{AB} \left( \text{Tr}_E \hat{\rho}_{\text{ABE}}^{\text{eq}} \right) - \chi_{AE} \left( \text{Tr}_B \hat{\rho}_{\text{ABE}}^{\text{eq}} \right).$$

The state $\hat{\rho}_{\text{ABE}}^{\text{eq}}$ is given by:

$$\hat{\rho}_{\text{ABE}}^{\text{eq}} = \text{Tr}_{A'B'} \left( \sum_i \langle \langle i | A \rangle | \hat{\rho}_{AA'B'B'}^{\text{ABE}} \langle i | A \rangle \otimes \hat{\rho}_{A'B'B'E} \right) \right).$$

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 $\hat{\rho}_{ABA'B'}$ can be written as a $4 \times 4$ array of blocks $\hat{A}_{ij,kl} = \hat{\rho}_{AB}(ij) |\hat{\rho}_{ABA'B'}(kl)_{AB}|$

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

It can be transformed by LOCC (with respect to the partition $AA' : BB'$) to the form:
\[ \hat{\sigma} = \begin{pmatrix}
\frac{1}{2}(\hat{A}_{00,00} + \hat{A}_{11,11}) & 0 & 0 & \frac{1}{2}(\hat{A}_{00,11} + \hat{A}_{11,00}) \\
0 & \frac{1}{2}(\hat{A}_{01,01} + \hat{A}_{10,10}) & \frac{1}{2}(\hat{A}_{01,10} + \hat{A}_{10,01}) & 0 \\
0 & \frac{1}{2}(\hat{A}_{01,01} + \hat{A}_{10,10}) & \frac{1}{2}(\hat{A}_{01,10} + \hat{A}_{10,01}) & 0 \\
\frac{1}{2}(\hat{A}_{00,00} + \hat{A}_{11,11}) & 0 & 0 & \frac{1}{2}(\hat{A}_{00,11} + \hat{A}_{11,00})
\end{pmatrix} \] (10)

Which can be "unwisted" to Bell diagonal matrix which is directly related to privacy squeezed state (see [7, 9]):

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

where the norm \( || \cdot || \) stands for the trace norm.

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

\[ \hat{\sigma}_{AB} = \begin{pmatrix}
\frac{1}{2}(p_1 + p_2) & 0 & 0 & \frac{1}{2}(p_1 - p_2) \\
0 & \frac{1}{2}(p_3 + p_4) & \frac{1}{2}(p_3 - p_4) & 0 \\
0 & \frac{1}{2}(p_3 - p_4) & \frac{1}{2}(p_3 + p_4) & 0 \\
\frac{1}{2}(p_1 - p_2) & 0 & 0 & \frac{1}{2}(p_1 + p_2)
\end{pmatrix} \] (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:

\[ K_D(\hat{\sigma}_{ABA'B'}) \geq I_3(A : B) - S(\hat{\sigma}_{AB}) = 1 - h(p_1 + p_2) - H(p_1, p_2, p_3, p_4) \] (13)

Here \( I_3(A : B) \) is the classical mutual information for the outcomes of von Neumann measurements carried out by Alice and Bob in the secure basis \( \{00\}_{AB}, \{01\}_{AB}, \{10\}_{AB}, \{11\}_{AB} \). 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 \( I_3(A : B) = 1 - h(p_1 + p_2) \), where \( h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \) denotes the binary entropy.

Note that the bound given in Eq. (13) is weaker than that on distillable entanglement in Eq. (9). This is because 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 \( \hat{\sigma}_{ABA'B'} \) of the complete system \( ABA'B' \).

### III. SINGLE PRIVACY WITNESS

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

\[ \hat{W}_{key} = (11)_{AB} \langle 00 | + | 00 \rangle_{AB} (11) \otimes \hat{U}_{A'B'} \]

where \( \hat{U}_{A'B'} \) is any hermitian matrix satisfying \( \hat{U}^\dagger \hat{U} \leq \hat{1} \) acting on the shield subsystems \( A' \) and \( B' \).

We will use the expectation value of the secrecy witness \( \langle \hat{W}_{key} \rangle \) to approximate the value of \( p_1 - p_2 \). In fact we have:

\[ w := |\langle \hat{W}_{key} \rangle| = \text{Tr}([\hat{A}_{00,11} + \hat{A}_{11,00}] \hat{U}) \leq ||\hat{A}_{00,11} + \hat{A}_{11,00}|| = p_1 - p_2 \] (15)

since for any matrix satisfying \( \hat{U}^\dagger \hat{U} \leq \hat{1} \) one has \( \text{Tr}(\hat{A} \hat{U}) \leq ||\hat{A}|| \). Indeed, \( \hat{U}^\dagger \hat{U} \leq \hat{1} \) implies ||\( \hat{U} ||_\infty \leq 1 \) and consequently \( \text{Tr} \hat{A} \hat{U} \leq ||\hat{A}|| \cdot ||\hat{U} ||_\infty \). Sometimes the parameter \( w \) may give exactly the value of \( p_1 - p_2 \). We will give an instance of that at the end of this section. Let us also stress that the witness itself (13) is an observable which must be measured on the original state (9).

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

\[ H(p_1, p_2, p_3, p_4) \leq H \left( p_1, p_2, \frac{1}{2}(1 - p_1 - p_2), \frac{1}{2}(1 - p_1 - p_2) \right) \] (16)

applied to Eq. (11), which yields:

\[ K_D \geq 1 - h(p_1 + p_2) - H \left( p_1, p_2, \frac{1}{2}(1 - p_1 - p_2), \frac{1}{2}(1 - p_1 - p_2) \right) \] (17)

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:

\[ K_D \geq 1 - \sup_{p_1, p_2 \geq 0, p_1 + p_2 \leq 1} \left[ h(p_1 + p_2) + H \left( p_1, p_2, \frac{1}{2}(1 - p_1 - p_2), \frac{1}{2}(1 - p_1 - p_2) \right) \right] \] (18)

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

We can simplify the optimization in Eq. (18) 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:

\[ K_D \geq \inf_{w \leq p_\pm \leq 1} \left( p_+ - 2h(p_+) - p_+ h(\xi_+) \right). \tag{19} \]

Because the lower limit for \( \xi_+ \) is greater or equal to 1/2, optimization over \( \xi_+ \) for a fixed value of \( p_+ \) yields \( h(\xi_+) \leq h((w + p_+)/2p_+) \). Consequently, the minimization in Eq. (19) needs to be carried out over a single parameter \( p_+ \):

\[ K_D \geq \inf_{w \leq p_+ \leq 1} \left[ p_+ - 2h(p_+) - p_+ h((w + p_+)/2p_+) \right]. \tag{20} \]

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

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

\[ K_D \geq 1 - h(w) - H \left( w, \frac{1}{3}(1 - w), \frac{1}{3}(1 - w), \frac{1}{3}(1 - w) \right) \tag{21} \]

In the last inequality we have used the fact that both \( p_1 + p_2 \geq w \) and \( p_1 \geq w \).

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

\[ K_D \geq 1 - 2h(w) - h \left( \frac{1}{2}(1 + w) \right) \tag{22} \]

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

![Graph of lower bounds on the distillable key as a function of w = |\langle \hat{W}_{\text{priv}} \rangle| derived in Eqs. (15) (solid line), (21) (dashed line), and (22) (dotted line).](image)

The above considerations are based on the ccq scenario, when Alice and Bob measure their qubits in the secure key basis \{0\}, \{1\}. However if the shield part is not affected by local unitary the optimal \( \hat{U} \) remains unchanged. For instance, in the case of the four-qubit state whose approximate version was realized experimentally in Ref. [8], a two-qubit swap operator \( \hat{V}_{AB'} = \hat{1}_{AB'} - 2|\Psi-\rangle_{AB'}\langle\Psi-| \) 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 \( \hat{W}^R_{\text{key}} = \langle 11 \rangle_{AB}(00) + |00\rangle_{AB}(11) \otimes \hat{U}_R \) and \( \hat{W}^I_{\text{key}} = \langle 11 \rangle_{AB}(00) + |00\rangle_{AB}(11) \otimes \hat{U}_I \).

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 \( \hat{\sigma}^A \otimes \hat{\sigma}^B \otimes \hat{U}_{AB'} \), characterizes correlations between measurements performed on the subsystems \( A \) and \( B \) in the key basis. The security of the key will be inferred using the expectation value of an observable \( \hat{\sigma}^A \otimes \hat{\sigma}^B \otimes \hat{U}_{AB'} \).

We derive the following parameterization of \( \hat{\sigma}_{AB} \):

\[ \hat{\sigma}_{AB} = \left( \begin{array}{ccc} \frac{1}{2}p_+ & 0 & 0 \\ 0 & p_-(\xi_+ - \frac{1}{2}) & \frac{1}{2}p_- \\ 0 & \frac{1}{2}p_- & 0 \end{array} \right) \right)^*. \tag{23} \]

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) a sentence has been cut off here. The parameters \( \xi_- \), \( \xi_+ \) satisfy the inequality:

\[ \frac{1}{2} \leq \xi_+, \xi_- \leq 1, \tag{24} \]

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

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

\[ K_D \geq 1 - 2h(p_+) - p_+ h(\xi_+) - p_- h(\xi_-). \tag{25} \]

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 \( 0 \leq p_+ < 1 - p^* \) or \( p^* < p_+ \leq 1 \), where \( p^* \approx 0.89 \) is the bigger of two solutions of a transcendental equation \( h(p^*) = \frac{1}{2} \) on the interval \( 0 \leq p^* \leq 1 \). We will restrict our further discussion only to the case \( p^* < p_+ \leq 1 \), as the analysis of the second case \( 0 \leq p_+ < 1 - p^* \) is completely analogous.

Let us now discuss 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 \( p_{\pm} = \frac{1}{2} (1 \pm \langle \hat{\sigma}^A \otimes \hat{\sigma}^B \otimes \hat{U}_{AB'} \rangle) \). Following discussion after Eq. (23), 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 antico\-related subspaces. These two possibilities can be analyzed jointly by defining
\[ w_z := \left| \langle \hat{\sigma}_A^z \otimes \hat{\sigma}_B^z \otimes \hat{\mathbb{1}}_{A'B'} \rangle \right| \] (26)
and using in further discussion
\[ p_{\pm} = \frac{1}{2}(1 \pm w_z). \] (27)
The condition \( p_+ > p^* \) can be equivalently written as
\[ w_z > 2p^* - 1 \approx 0.78 \] (28)
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
\[ w_z := \left| \langle \hat{\sigma}_A \otimes \hat{\sigma}_B \otimes \hat{U}_{A'B'} \rangle \right|. \] (29)
It allows us to bound the parameters \( \xi_- \) and \( \xi_+ \) according to the following inequality which will be at the heart of our reasoning:
\[ w_x = \left| \text{Tr}[\hat{U}(\hat{A}_{00,11} + \hat{A}_{01,10} + \hat{A}_{10,01} + \hat{A}_{11,00})] \right| \leq \| \hat{A}_{00,11} + \hat{A}_{11,00} \| + \| \hat{A}_{01,10} + \hat{A}_{10,01} \| = p_+(2\xi_+ - 1) + p_-(2\xi_- - 1). \] (30)
For fixed \( p_{\pm} \), this inequality determines the allowed region of \( (\xi_-, \xi_+) \) in the square defined by Eq. (24) as
\[ p_-\xi_- + p_+\xi_+ \geq \frac{1}{2}(1 + w_x). \] (31)

When evaluating the lower bound on the key rate \( K_D \) according to Eq. (25) 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. (25) under constraints given by Eqs. (24) and (31). This is equivalent to maximizing under the same constraints a concave function
\[ f(\xi_-, \xi_+) = p_-h(\xi_-) + p_+h(\xi_+). \] (32)
The lower bound on the key can be written as
\[ K_D \geq 1 - 2h(p_+) - f_{\text{max}}, \] (33)
where \( f_{\text{max}} \) 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. (24) decreasing either of the arguments \( \xi_- \) or \( \xi_+ \) will always increase the value of \( f(\xi_-, \xi_+) \). This in turn implies that \( f_{\text{max}} \) is reached on the line
\[ p_-\xi_- + p_+\xi_+ = \frac{1}{2}(1 + w_x). \] (34)
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. (25). This follows from a straightforward fact that the expression \( 1 - 2h(p_+) - p_+ \) is nonpositive for \( p^* < p_+ \leq 1 \). Therefore no point with \( \xi_+ = \frac{1}{2} \) should satisfy Eq. (31). Because the slope of the line \( \xi_+ = \frac{1}{2} \) 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:
\[ w_x + w_z > 1. \] (35)

Further analysis depends on whether the point \( (\xi_-=1, \xi_+ = \frac{1}{2}) \) 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. (31) and the allowed region of parameters has the shape of a trapezoid, as shown in Fig. 2(a). Consequently, all values \( \frac{1}{2} \leq \xi_- \leq 1 \) are allowed. On the other hand, when \( p_+ \leq w_x \), the allowed region is a triangle, as depicted in Fig. 2(b). The minimum allowed value of \( \xi_- \) is then \( w_x - w_z/(1 - w_z) \). We can combine these two cases by defining
\[ \xi_- = \max \left\{ \frac{1}{2} \left( \frac{w_x - w_z}{1 - w_z} \right) \right\} \] (36)
The maximization of \( f(\xi_-, \xi_+) \) over the line defined in Eq. (34) can now be written as a supremum over a single parameter:
\[ f_{\text{max}} = \sup_{\xi_- \leq \xi \leq 1} f \left( \frac{1 + w_x}{1 + w_x} - \frac{1 - w_z}{1 + w_z} \right) \] (37)
which inserted into Eq. (33) yields the final form of the bound:
\[ K_D \geq 1 - 2h(p_+) - \sup_{\xi_- \leq \xi \leq 1} \left[ (1 - p_+)h(\xi) + p_+h \left( \frac{1 + w_x}{1 + w_x} - \frac{1 - w_z}{1 + w_z} \right) \right] \] (38)
where \( p_+ = (1 + w_x)/2 \). The results of a numerical evaluation of the supremum are shown in Fig. 2(a).

It is also possible to derive a slightly weaker bound that requires no numerical maximization, which we will denote as \( f_{\text{max}} \). Because the function \( f(\xi_-, \xi_+) \) is monotonic in each one of its two arguments, as discussed after Eq. (33), we have
\[ f_{\text{max}} \leq f_{\text{max}} = f(\xi_-^\text{min}, \xi_+^\text{min}). \] (39)
where \( \xi_-^\text{min} \) and \( \xi_+^\text{min} \) are the smallest possible values of \( \xi_- \) and \( \xi_+ \) within the allowed region defined by Eqs. (24) and (31). The value \( \xi_-^\text{min} \) has been given explicitly in Eq. (36), while it is easy to verify that
\[ \xi_+^\text{min} = \frac{w_x + w_z}{1 + w_z}. \] (40)
The simplified bound therefore takes the following explicit form:
\[ K_D \geq 1 - 2h(p_+) - (1 - p_+)h(\xi_-^\text{min}) - p_+h \left( \frac{w_x + w_z}{1 + w_z} \right) \] (41)
FIG. 2: The permitted region of the parameters \((\xi_-, \xi_+)\) used to maximize the function \(f(\xi_-, \xi_+)\) defined in Eq. (32).

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. (38) and (b) a weaker estimate according to Eq. (41). The bound is positive in the shaded area, with solid contours drawn at steps 0.1 starting from 0.

FIG. 4: The lower bound on the key given in Eq. (43) obtained from observables \(w\) and \(w_z\). The physical region is restricted to points \((w, w_z)\) satisfying the condition \((1 + w_z)/2 \geq w\). The coding of the bound value is the same as in Fig. 3(b).

Finally, let us note that the observable \(w\) defined in Eq. (15) can be combined with \(w_z\) to yield a stronger bound on the distillable key. To derive this bound, let us return to Eq. (25) 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 \(\xi_+\):

\[
\xi_+ \geq \frac{1}{2} + \frac{w}{2p_+}. \tag{42}
\]

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

\[
K_D \geq p_+ [1 - h(1/2 + w/2p_+)] - 2h(p_+). \tag{43}
\]

Let us note that physical values of \(w\) and \(w_z\) must satisfy the condition \((1 + w_z)/2 \geq w\), otherwise we would have \(p_1 + p_2 = p_+ = (1 + w_z)/2 < w \leq p_1 - p_2\) and consequently \(p_2 < 0\). In Fig. 4 we depict the bound (43) in the physical region of \(w\) and \(w_z\).

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 amount of 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 p-bit state \( \rho_{ABA'B'} \) in the form \([6]\)

\[
\hat{\rho}_{ABA'B'} = \frac{1}{2d^2} \left[ \langle 00 \rangle_{AB} |00\rangle + |11\rangle_{AB} \langle 11 | \otimes \hat{I}_{A'B'} + \langle 00 \rangle_{AB} \langle 11 | + |11\rangle_{AB} \langle 00 | \otimes \hat{V}_{A'B'} \right]
\]

where \( \hat{I}_{A'B'} \) and \( \hat{V}_{A'B'} \) stand respectively for bipartite identity and swap operator on the subsystems \( A'B' \).

In the limit of large \( d \) the distillable entanglement is bounded by vanishing log-negativity \( E_D \leq \log_2 (1 + \frac{1}{d^2}) \rightarrow 0 \), while the privacy witness \( W = (\hat{\sigma}_A^x \otimes \hat{\sigma}_B^x + \hat{\sigma}_A^y \otimes \hat{\sigma}_B^y) \otimes \hat{V}_{A'B'} \) gives us the value of lower bound \( K_D \geq 1 \) since \( w = Tr(W \hat{\rho}_{ABA'B'}) = 1 \) and then just either of the weaker bounds given in Eqs. \([21]\) or \([22]\) 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 experiment reported in Ref. \([8]\) the operator in question is the swap operator which is composed of three terms involving products of Pauli matrices:

\[
\hat{V}_{A'B'} = \frac{1}{2} (\hat{I}_{A'B'} + \hat{\sigma}_A^x \otimes \hat{\sigma}_B^x + \hat{\sigma}_A^y \otimes \hat{\sigma}_B^y + \hat{\sigma}_A^z \otimes \hat{\sigma}_B^z).
\]

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 less than the full tomography which requires \( 81 \) products of four Pauli matrices. Note that in some cases, like the p-bit 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 \( E_D(\rho) \leq \log_2 (1 + \frac{1}{d^2}) \approx 0.585 \).

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 p-bit he 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.

Acknowledgments

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

Appendix A: Single witness bound

Let us denote

\[
\kappa(p_\pm) = p_+ - 2h(p_+) - p_+ h((p_+ + w)/2p_+) - \frac{1}{2} \log_2 \left( \frac{p_+^2 - w^2}{(1 - p_+)^2} \right).
\]

The derivative with respect to \( p_+ \) reads:

\[
\frac{d\kappa}{dp_+} = \frac{1}{2} \log_2 \left( \frac{p_+^2 - w^2}{(1 - p_+)^2} \right).
\]

It is easy to see that on the interval \( w \leq p_+ \leq 1 \) 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 which 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 \( \delta \approx (1 - w)^3/2w^3 \) and consequently the bound on the key in the approximate form

\[
K_D \geq \kappa \left( w + \frac{(1 - w)^4}{2w^3} \right).
\]

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. \([19]\).

![FIG. 5: The difference between the bounds from Eqs. \([19]\) and \([A3]\) as a function of the parameter \( w \).](image-url)
[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, Bangalore, India, December 1984, 1984), pp. 175–179.
[3] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A 53, 2046 (1996), quant-ph/9511030.
[4] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. 77, 2818 (1996), quant-ph/9604039.
[5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. 80, 5239 (1998), quant-ph/9801069.
[6] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. 94, 160502 (2005), quant-ph/0309110.
[7] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory 55, 1898 (2009), quant-ph/0506189.
[8] K. Dobek, M. Karpinski, R. Demkowicz-Dobrzanski, K. Banaszek, and P. Horodecki, Phys. Rev. Lett. 106, 030501 (2011), arXiv:1010.4575.
[9] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE 54, 2621 (2008), quant-ph/0506203.
[10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A 223, 1 (1996), quant-ph/9605038.
[11] B. M. Terhal, Phys. Lett. A 271, 319 (2000), quant-ph/9911057.
[12] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A 66, 062305 (2002), quant-ph/0205089.
[13] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, J. Mod. Opt. 50, 1079 (2003), quant-ph/0210134.
[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), quant-ph/0503152.
[16] M. Horodecki and P. Horodecki, Phys. Rev. A 59, 4206 (1999), quant-ph/9708015.
[17] I. Devetak and A. Winter, Phys. Rev. Lett. 93, 080501 (2004), quant-ph/0307053.
[18] I. Devetak and A. Winter, Proc. R. Soc. Lond. A 461, 207 (2005), quant-ph/0306078.
[19] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996), quant-ph/9511027.