Multipartite secret key distillation and bound entanglement

Remigiusz Augusiak
Faculty of Applied Physics and Mathematics, Gdańsk University of Technology,
Narutowicza 11/12, 80–952 Gdańsk, Poland
ICFO–Institute Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Pawel Horodecki
Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Narutowicza 11/12, 80–952 Gdańsk, Poland

Recently it has been shown that quantum cryptography beyond pure entanglement distillation is possible and a paradigm for the associated protocols has been established. Here we systematically generalize the whole paradigm to the multipartite scenario. We provide constructions of new classes of multipartite bound entangled states, i.e., those with underlying twisted GHZ structure and nonzero distillable cryptographic key. We quantitatively estimate the key from below with help of the privacy squeezing technique.

PACS numbers:

I. INTRODUCTION

Quantum cryptography is one of the most successful applications of quantum physics in information theory. The original pioneering BB84 scheme [1] was based on sending nonorthogonal states through an insecure quantum channel. Then the alternative approach (E91) [2] based on generating key from pure entangled quantum state have been proposed and later extended to the case of mixed states in quantum privacy amplification scheme [3] which exploited the idea of distillation of pure entangled quantum states from more copies of noisy entangled (mixed) states [4]. Much later it was realized that actually existence of (may be noisy) initial entanglement in the state is necessary for any type of protocols distilling secret key from quantum states [5, 6]. In a meantime the problem of unconditional security (security in the most unfriendly scenario when the eavesdropper may apply arbitrarily correlated measurements on the sent particles or, in the entanglement distillation scheme, distribute many particles in a single entangled quantum state) was further solved in Ref. [7] in terms of entanglement distillation showing equivalence between the two (BB84 and E91) ideas (see Ref. [8] for an alternative proof). However, still the protocol worked only for entanglement that could be distilled. Also, other protocols [9, 10] that exploited a modern approach to secrecy (based on classical notions) also were used in cases when pure entanglement was distillable. It was known, however, for a relatively long time that there are states (called bound entangled) that can not be distilled to pure form [11]. In the above context it was quite natural to expect that bound entangled states cannot lead to private key. However, it happens not to be true [12]: one can extend the entanglement distillation idea from distillation of pure states to distillation of private states (in general mixed states that contain a private bit) and further show that there are examples of bound entangled states from which secure key can be distilled. A general paradigm has been systematically worked out in Refs. [13, 14] with further examples of bound entangled states with secure key [15, 16] and interesting applications [17, 18, 19]. From the quantum channels perspective the extended scheme [12] represents secure key distillation with help of a quantum channel with vanishing quantum capacity (i.e., it is impossible to transmit qubit states faithfully). Those channels [12, 16] were later used in the discovery [20] of the drastically non intuitive, fully nonclassical effect of mutual activation of zero capacity channels, which "unlock" each other allowing to transmit quantum information faithfully if encoded into entanglement across two channels inputs. On the other hand with help of the seminal machinery exploiting the notion of almost productness in unconditionally secure quantum key distillation [21] it has been shown that unconditional security under channels that do not convey quantum information is possible [22]. Here we would like to stress that we focus on the approach to quantum cryptography based on private states rather than the, to some extent, complementary information–theoretic approach which has also been proven very fruitful (see Refs. [6, 21, 22, 24, 25]).

The results discussed above concern bipartite states. The aim of the present paper, which, among others, concludes part of the analysis of [26], is to develop the general approach to distillation of secure key from multipartite states. Basically the content of the paper can be divided into two parts. In the first part we systematically and in a consistent way generalize the approach from Ref. [13]. Here the basic notion of multipartite p–dits that has been introduced and analyzed already in the previous paper [27].

It should be stressed here that, as extensively discussed in [13], other modifications of the paradigm are possible as far as the so–called notion of "direct accessibility of cryptographic key" is considered. The p–dit approach is

---

*Electronic address: remigiusz.augusiak@icfo.es
†Electronic address: pawel@mif.pg.gda.pl
based on local von Neumann measurements, while it is possible also to consider local POVM–s \[17\]. Both approaches (and additional one) were proved to be equivalent in terms of the amount of distillable key contained in a given bipartite state in Ref. \[13\]. While we leave this issue for further analysis we strongly believe that the abstract proofs of the latter work naturally extend to our multipartite case.

The first part of the present paper contains qualitatively new elements like conditions for closeness to a p–dit state which were not known so far, and a derivation of a lower bound for multipartite key where an additional analysis of distance to so–called cq states was needed. The second part of the paper contains constructions of novel states i.e. multipartite states that contain secure key though are bound entangled. The states are based on the underlying (twisted) N–partite GHZ structure and are PPT under any N – 1 versus one system partial transpose. The secret key content is bounded from below quantitatively with help of the technique adopted form \[16\].

More specifically after basic definitions and a generalization of the modern definition (that has already become standard) of secure key distillation from quantum state in Sec. II we pass to Sec. III where the notion of multipartite private–dit state (in short p–dit) and its properties are discussed including especially the condition for ε–closeness to a p–dit. Distillable cryptographic key in terms of p-dits is analyzed in section IV. Here an upper bound in terms of relative entropy is proved in analogy to the bipartite case. A lower bound on the key based on a modification of the one–way Devetak–Winter protocol \[10\] to the multipartite case is provided with help of a natural lemma with a somewhat involved proof. Also the application \[16\] of privacy squeezing \[12\] is naturally extended and applied here.

The next section is the longest one since it contains all the constructions of multipartite bound entanglement with cryptographic key. Note that the first construction, being an extension and modification of bipartite examples from Ref. \[13\], requires nontrivial coincidence of several conditions that are contained in Lemma V.3. They ensure that, on the one hand the state is PPT, but on the other it allows to be modified by the LOCC recurrence protocol to a state that is close to a multipartite p–dit. This is equivalent to distillability. Independently, a quantitative analysis is performed illustrating how the lower bound for distillable key becomes positive. The second class of bound entangled states (to some extent inspired by bipartite four–qubit states from \[16\]) involves hermitian unitary block elements of the density matrix. Here the construction is different and, in comparison to the first one, the observed secure key is much stronger. Finally we shortly recall the limitations of quantum cryptography \[33,35\]. Section VI contains conclusions.

II. BASIC NOTIONS AND THE STANDARD DEFINITION OF SECURE KEY

In what follows we shall be concerned with the scenario in which N parties \(A_1, \ldots, A_N\) wish to obtain perfectly correlated strings of bits (or in general dits) that are completely uncorrelated to the eavesdropper Eve by means of local operations and public communication (LOPC). Let us recall that the difference between the standard local operations and classical communication (LOCC) and LOPC lies in the fact that in the latter we need to remember that any classical message announced by the involved parties may be registered by Eve. Therefore in comparison to the LOCC paradigm in the LOPC paradigm one also includes the map (see e.g. Refs. \[13, 19\])

\[
\varrho_{ABE} = \sum_i \varrho_{ABE}^{(i)} \otimes |i\rangle \langle i|^{A'}, \quad \text{distillability. Independently,}
\]

\[
\varrho_{ABE}^{(i)} = \sum_{j=0}^{d-1} |e_i^{(1)} \cdots e_i^{(N)}\rangle \langle e_i^{(1)} \cdots e_i^{(N)}| \otimes \varrho^E,
\]

From the quantum cryptographic point of view the common aim of all the parties \(A_1, \ldots, A_N\) is to distill the following state

\[
\varrho_{ABE}^{(N, \text{id})} = \frac{1}{d} \sum_{i=0}^{d-1} |e_i^{(1)} \cdots e_i^{(N)}\rangle \langle e_i^{(1)} \cdots e_i^{(N)}| \otimes \varrho^E
\]

called hereafter \textit{ideal} c...cq (cq) state, by means of LOPC. Here \(A \equiv A_1 \cdots A_N\) and \(|e_i^{(j)}\rangle\text{ }|_{i=0}^{d-1}\) is some orthonormal basis in the Hilbert space corresponding to the \(j\)th party (denoted hereafter by \(H_j\)). Their tensor product constitutes the product basis in \(H_1 \otimes \cdots \otimes H_N\), which we shall denote as

\[
B_{N}^{\text{prod}} = \{ |e_i^{(1)} \rangle \otimes \cdots \otimes |e_i^{(N)}\rangle \}_{i_1, \ldots, i_N = 0}^{d-1}.
\]

(In what follows we will be often assuming \(|e_i^{(j)}\rangle\text{ }|_{i=0}^{d-1}\) to be the standard basis in \(H_j\).) One sees that the ideal cq states represent perfect classical correlations with respect to the product basis \(B_{N}^{\text{prod}}\) that uncorrelated to the eavesdropper’s degrees of freedom.

We may also define a general cq state to be

\[
\varrho_{ABE}^{(N, \text{cq})} = \sum_{i_1, \ldots, i_N = 0}^{d-1} p_{i_1, \ldots, i_N} \langle e_i^{(1)} \cdots e_i^{(N)}| \langle e_i^{(1)} \cdots e_i^{(N)}| \otimes \varrho^E
\]

In the above considerations formula we could take different dimensions on each side, however, for simplicity we restrict to the case of equal dimensions. All the parties should have strings of the same length at the end of the protocol to make a key.

It should be also emphasized that in what follows the \(j\)th party is assumed to have an additional ‘garbage’ quantum system defined on some Hilbert space \(H_j\). Thus we will be assuming that usually the states shared by the
parties are defined on the Hilbert space $\mathcal{H} \otimes \mathcal{H}'$, where $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_N$ and $\mathcal{H}' = \mathcal{H}'_1 \otimes \ldots \otimes \mathcal{H}'_N$. $B_{N}^{\text{prod}}$ constitutes the product basis in $\mathcal{H}$. Also, following Ref. [13], the part of a given state corresponding to $\mathcal{H}'$ ($\mathcal{H}'$) will be sometimes called the key part (the shield part). This terminology comes from the fact that the key part is the one from which the parties obtain the cryptographic key, while the shield part protects secret correlation from the eavesdropper.

Following e.g. Refs. [12, 13], using the notion of cq states, we may define the distillable cryptographic key in the multipartite scenario as follows.

**Definition II.1.** Let $\varrho_{AE}$ be a state acting on $\mathbb{C}^{d_1} \otimes \ldots \otimes \mathbb{C}^{d_N} \otimes \mathbb{C}^{d_E}$ and $(P_n)_{n=1}^{\infty}$ be a sequence of LOPC operations such that $P_n(\varrho_{AE}) = \varrho_{AE}^{(q,n)}$, where $\varrho_{AE}^{(q,n)}$ is a cq state with A part defined on $(\mathbb{C}^{d_n}) \otimes H$. The set of operations $P = (A_n)_{n=1}^{\infty}$ is said to be a cryptographic key distillation protocol if

$$\lim_{n \to \infty} \left\| \varrho_{AE}^{(q,n)} - \varrho_{AE}^{(d,n)} \right\|_1 = 0, \quad (5)$$

where $\varrho_{AE}^{(d,n)}$ is the ideal cq state defined on the same Hilbert space as $\varrho_{AE}^{(q,n)}$. We define the rate of the protocol $P = (P_n)_{n=1}^{\infty}$ as

$$R_P(\varrho_{AE}) = \lim sup_{n \to \infty} \frac{\log d_n}{n}, \quad (6)$$

and the distillable classical key as

$$C_D(\varrho_{AE}) = \sup_{P} R_P(\varrho_{AE}). \quad (7)$$

If instead of $\varrho_{AE}$ one has the purification $|\psi_{AE}\rangle$ we write $C_D(\varrho_A)$.

Let us also mention that a good indicator of the secrecy of our correlations as well as the uniformity of the probability distribution $p_{i_1,\ldots,i_N}$ is the trace norm distance $\left\| \varrho_{AE}^{(d)} - \varrho_{AE}^{(q)} \right\|_1$.

### III. PRIVATE STATES

#### A. Definition and properties

Here we discuss the multipartite generalizations of two important concepts of the scheme from Refs. [12, 13]. Firstly we introduce the notion of twisting and then the notion of multipartite private states.

**Definition III.1.** Let $(U_{i_1,\ldots,i_N})_{i_1,\ldots,i_N}$ be some family of unitary operations acting on $\mathcal{H}'$. Given the N–partite product basis $B_{N}^{\text{prod}}$ we define **multipartite twisting** to be the unitary operation given by the following formula

$$U_t = \sum_{i_1,\ldots,i_N=0}^{d-1} |e^{(1)}_{i_1} \ldots e^{(N)}_{i_N}\rangle \langle e^{(1)}_{i_1} \ldots e^{(N)}_{i_N}| \otimes U_{i_1,\ldots,i_N}. \quad (8)$$

This is an important notion since, as shown in the bipartite case in Ref. [13] (Theorem 1) and as it holds also for multipartite states, application of twisting (taken with respect to the product basis $B_{N}^{\text{prod}}$) to a given state $\varrho_{AA'}$ does not have any effect on the cq state obtained upon a measurement of the A part of the purification of $\varrho_{AA'}$ in the product basis $B_{N}^{\text{prod}}$. More precisely states $\varrho_{AA'}$ and $U_t \varrho_{AA'} U_t^\dagger$ have the same cq state with respect to $B_{N}^{\text{prod}}$ for any twisting that is constructed using $B_{N}^{\text{prod}}$.

We can now pass to the notion of multipartite private states. These are straightforward generalization of private states from Refs. [12, 13] and were defined already in Ref. [21].

**Definition III.2.** Let $U_i$ be some unitary operations for every $i$ and let $\varrho_{A'}$ be a density matrix acting on $\mathcal{H}'$. By **multipartite private state** or **multipartite pdt** we mean the following

$$\Gamma_{AA'}^{(d)} = \frac{1}{d} \sum_{i,j=0}^{d-1} |e_i^{(1)} \ldots e_i^{(N)}(N)\rangle \langle e_j^{(1)} \ldots e_j^{(N)}(N)| \otimes U_i \varrho_{A'} U_j^\dagger. \quad (9)$$

Naturally, for $N = 2$ the above reproduces the bipartite private states $\gamma_{A_1A_2A_1'A_2'}^{(d)}$ introduced in Ref. [13]. It follows from the definition that any multipartite private state may be written as $\Gamma_{AA'}^{(d)} = U_i (P_{d,N}^{(i)} \otimes \varrho_{A'}) U_i^\dagger$ with $\varrho_{A'}$ and $U_i$ denoting some density matrix acting on $\mathcal{H}'$ and some twisting, respectively. Moreover, $P_{d,N}^{(i)}$ stands for the projector onto the so–called GHZ state $|\psi_{d,N}^{(+)}\rangle$ given by

$$|\psi_{d,N}^{(+)}\rangle = \sum_{i=0}^{d-1} |i\rangle \otimes N. \quad (10)$$

In other words we say that multipartite private states are twisted GHZ states tensored with an arbitrary density matrix $\varrho_{A'}$.

As a simple but illustrative example of a multipartite pdt one may consider the following $(2D)^N \times (2D)^N$ state (with $\mathcal{H} = (\mathbb{C}^2)^{\otimes N}$ and $\mathcal{H}' = (\mathbb{C}^D)^{\otimes N}$)

$$\Gamma_{ex}^{(2)} = \frac{1}{2D^N} \left[ \begin{array}{ccc} 1_{D^N} & 0 & \cdots & V_{\pi}^{(D)} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ V_{\pi}^{(D)\dagger} & 0 & \cdots & 1_{D^N} \end{array} \right],$$

$$= \frac{1}{2D^N} \left[ \begin{array}{cc} |0\rangle \langle 0|^{\otimes N} + |1\rangle \langle 1|^{\otimes N} \otimes 1_{D^N} \\ \cdots \end{array} \right] + \left( |0\rangle \langle 0|^{\otimes N} + |1\rangle \langle 1|^{\otimes N} \otimes V_{\pi}^{(D)} \right). \quad (11)$$

where $V_{\pi}^{(D)}$ is a permutation operator defined as

$$V_{\pi}^{(D)} = \sum_{i_1,\ldots,i_N=0}^{D-1} |i_1\rangle \langle i_{\pi(1)}| \otimes |i_2\rangle \langle i_{\pi(2)}| \otimes \cdots \otimes |i_N\rangle \langle i_{\pi(N)}|.$$
with $\pi$ being an arbitrary permutation of $N$-element set. Clearly $V_\pi^{(D)}$ is unitary matrix for any permutation $\pi$ and thus $|V_\pi^{(D)}| = I_{D^N}$ ($|A|$ is defined as $\sqrt{A A^\dagger}$).

This, in view of the Lemma A.1 (Appendix), means that $\mathcal{M}_2(I_{D^N}, V_\pi^{(D)}) \geq 0$ (for the definition of $\mathcal{M}_2$ see Appendix) for any $\pi$ and hence $\Gamma_{ex}^{(2)}$ represents quantum state. Moreover, $\Gamma_{ex}^{(2)}$ may be derived from the general form (9) by substituting $\varrho_{AA'} = I_{D^N}/D^N$, i.e., maximally mixed state acting on $(C^D)^{\otimes N}$. Finally, both unitary operations in Eq. (9) may be taken to be $U_0 = V_\pi^{(D)}$ and $U_1 = I_{D^N}$.

As multipartite private state constitute a central notion of our cryptographic scheme, below we shortly characterize multipartite private states. Firstly, we notice that any state of which eq state is the ideal one with respect to some basis $B_N$ must be of the form (6) and vice versa.

Theorem III.1. Let $\varrho_{AA'}$ be a state defined on $\mathcal{H} \otimes \mathcal{H}'$ with $\mathcal{H} = (C^d)^{\otimes N}$ and arbitrary but finite-dimensional $\mathcal{H}'$. Let also $\varrho_{AA'}^{(eq)}$ denote the eq state obtained from the purification of $\varrho_{AA'}$ upon the measurement of the $A$ part in $B_N^{\text{prod}}$ and tracing out the $A'$ part. Then $\varrho_{AA'}^{(eq)}$ is of the form (6) if and only if $\varrho_{AA'}$ is of the form (9), both with respect to $B_N^{\text{prod}}$.

This fact may be proved in exactly the same way as its bipartite version from Ref. 13.

Secondly, it was shown in Ref. 27 that any multipartite private state is distillable providing also a lower bound on distillable entanglement. For completeness it is desirable to briefly recall this result, which can be stated as follows. For any multipartite private state $\Gamma_{AA'}^{(d)}$ its distillable entanglement is bounded as

$$E_D(\Gamma_{AA'}^{(d)}) \geq \max_{i,j=0,\ldots,d-1} \left\{ \eta_{ij} \max \left[ \frac{1}{2} - H \left( \frac{1}{2} + \frac{\eta_{ij}}{2 \sqrt{a_{ij}^{(1)} a_{ij}^{(2)}}} \right) \right] \right\}$$

(13)

where $\eta_{ij}$, $a_{ij}^{(1)}$, $a_{ij}^{(2)}$, and finally $a_{ij}^{(d)}$ are parameters characterizing the given private state $\Gamma_{AA'}^{(d)}$. They are defined as follows

$$\eta_{ij} = \max \left| \langle f_1 | \ldots | f_N | U_i \varrho_{A} U_i^\dagger | g_1 \rangle \ldots | g_N \rangle \right|,$$

(14)

where maximum is taken over a pair of pure product vectors $|f_1 \rangle \ldots |f_N \rangle$ and $|g_1 \rangle \ldots |g_N \rangle$ belonging to $\mathcal{H}'$. The parameters $a_{ij}^{(1)}$ and $a_{ij}^{(2)}$ are given by

$$a_{ij}^{(1)} = \langle \tilde{f}_1^{(ij)} | \ldots | \tilde{f}_N^{(ij)} | U_i \varrho_{A} U_i^\dagger | \tilde{f}_1^{(ij)} \rangle \ldots | \tilde{f}_N^{(ij)} \rangle$$

(15)

and

$$a_{ij}^{(2)} = \langle \tilde{g}_1^{(ij)} | \ldots | \tilde{g}_N^{(ij)} | U_j \varrho_{A} U_j^\dagger | \tilde{g}_1^{(ij)} \rangle \ldots | \tilde{g}_N^{(ij)} \rangle,$$

(16)

where $\tilde{f}_1^{(ij)} \ldots \tilde{f}_N^{(ij)}$ and $\tilde{g}_1^{(ij)} \ldots \tilde{g}_N^{(ij)}$ are the vectors realizing the maximum in Eq. (14). Finally $a_{ij}^{(d)}$ denotes the larger of two numbers $a_{ij}^{(1)}$ and $a_{ij}^{(2)}$.

It follows from Eqs. (14), (15), and (16) that $\eta_{ij}$ is always positive and on the other hand $\eta_{ij} \leq \sqrt{a_{ij}^{(1)} a_{ij}^{(2)}}$. This means that $a_{ij}^{(d)} > 0$ and consequently for any pair $(i < j)$ the expression under the maximum in Eq. (13) is positive proving that $E_D$ of any multipartite private state is nonzero.

Finally, we notice following Ref. 27 that for bipartite private states also other entanglement measures were bounded from below. Namely, it was shown that

$$E_C\left(\gamma^{(d)}_{A_1A_2A'_3A'_4} \right) \geq \log d$$

(17)

and, due to the fact that entanglement of formation is not smaller than the entanglement cost, $E_F\left(\gamma^{(d)}_{A_1A_2A'_3A'_4} \right) \geq \log d$.

B. Conditions for closeness to multipartite private states

Here we provide necessary and sufficient conditions allowing for judging how close to some multipartite private state is some given state $\varrho_{AA'}$ defined on $\mathcal{H} \otimes \mathcal{H}'$.

Let us firstly notice that any state acting on $\mathcal{H} \otimes \mathcal{H}'$ may be written in the following block form

$$\varrho_{AA'} = \sum_{i_1,\ldots,i_N=0}^{d-1} \sum_{j_1,\ldots,j_N=0}^{d-1} |i_1 \ldots i_N, j_1 \ldots j_N, \Omega_{i_1 \ldots i_N}^{j_1 \ldots j_N} \rangle \langle \Omega_{i_1 \ldots i_N}^{j_1 \ldots j_N}|,$$

(18)

where $\Omega_{i_1 \ldots i_N}^{j_1 \ldots j_N}$ are assumed to be square matrices defined on $\mathcal{H}'$. Also by $\varrho_{AA'}$ we denote the state $\varrho_{AA'} = \text{Tr}_{A'}(U_i \varrho_{AA'} U_i^\dagger)$ with some twisting $U_i$, and by $(\varrho_{AA'}^{j_1 \ldots j_N})$ its entries in the standard basis. Then we can prove the following useful lemma.

Lemma III.1. Let $\varrho_{AA'}$ be some density matrix acting on $\mathcal{H} \otimes \mathcal{H}'$ with $\mathcal{H} = (C^d)^{\otimes N}$ and arbitrary finite-dimensional $\mathcal{H}'$. Then there exists such twisting $U_t$ that for a fixed index $i$ all the elements $(\varrho_{AA'}^{i_1 \ldots i_N})$ and $(\varrho_{AA'}^{j_1 \ldots j_N})$ $(j = 0, \ldots, d-1)$ of the $i$-th row and column of $\varrho_{AA'}$ are $\text{Tr}_{A'}(U_t \varrho_{AA'} U_t^\dagger)$ equal $\|\Omega_{i_1 \ldots i_N}^{j_1 \ldots j_N} \|$ and $\|\Omega_{j_1 \ldots j_N}^{i_1 \ldots i_N} \|$, respectively.

Proof. The proof is a simple extension of the one presented in Ref. 13. Acting on the state $\varrho_{AA'}$ with an unitary twisting $U_t$ and tracing out the $A'$ subsystem, one gets

$$\varrho_{AA'} = \sum_{i_1,\ldots,i_N=0}^{d-1} \sum_{j_1,\ldots,j_N=0}^{d-1} \text{Tr}_{A'}(U_{i_1 \ldots i_N} \Omega_{j_1 \ldots j_N}^{i_1 \ldots i_N}) \times |i_1 \ldots i_N, j_1 \ldots j_N \rangle \langle i_1 \ldots i_N|.$$  

(19)

First of all let us mention that from Eq. (19) it follows that we do not need to care about blocks lying on the
diagonal of $\varrho_{AA'}$ as the blocks $\Omega^i_{i...iN}$ must be positive and the following holds
\[
\text{Tr} \left( U_{i...iN} \Omega^i_{i...iN} U_{i...iN}^\dagger \right) = \|\Omega^i_{i...iN}\|_1. \tag{20}
\]

Now, let us focus now on the matrices $\Omega^j_{i...i}$ for some fixed $i$ and any $j \neq i$ (as the case of $i = j$ has just been discussed). For simplicity and without any loss of generality we can choose $i = 0$ and thus we need to prove the theorem for $i = 1, \ldots, d - 1$. At the beginning let us concentrate on the matrix $\Omega^0_{0...0}$. We express it with the singular-value decomposition as $\Omega^0_{0...0} = V_i D_i W_i^\dagger$, where $V_i$ and $W_i$ are unitary matrices and $D_i$ stands for a diagonal matrix containing singular values of $\Omega^0_{0...0}$, i.e., eigenvalues of $|\Omega^0_{0...0}|^{1/2}$. Then from Eq. [19] one infers that if it suffices to take $U_{0...0} = V_i^\dagger$ and $U_{1...1} = W$ in the twisting $U_i$ to get
\[
\text{Tr} \left( U_{0...0} \Omega^0_{0...0} U_{1...1}^\dagger \right) = \text{Tr} (V_i^\dagger V_i D_i W_i^\dagger W) = \text{Tr} D_i = \|\Omega^0_{0...0}\|_1. \tag{21}
\]

Now we may proceed with the remaining matrices $\Omega^j_{0...0}$ ($j = 2, \ldots, d - 1$). We need to find such matrices in the twisting $U_i$ that Eq. [21] holds also for the remaining $\Omega^j_{0...0}$. Notice that unitary matrices $U_{0...0}$ and $U_{1...1}$ have just been fixed, however, we have still some freedom provided by $U_{j...j}$ ($j = 2, \ldots, d - 1$). Using the singular-value decomposition of all $\Omega^j_{0...0}$ ($j = 2, \ldots, d - 1$) we may write $\Omega^j_{0...0} = V_j D_j W_j^\dagger$. This leads to
\[
\text{Tr} \left( U_{0...0} \Omega^j_{0...0} U_{j...j}^\dagger \right) = \text{Tr} \left( V_i^\dagger \Omega^j_{0...0} U_{j...j}^\dagger \right) = \text{Tr} \left( V_i^\dagger V_j D_j W_j^\dagger U_{j...j}^\dagger \right) = \text{Tr} \left( D_j W_j^\dagger U_{j...j}^\dagger V_j V_j^\dagger \right). \tag{22}
\]

where we used the property of trace saying that $\text{Tr}AB = \text{Tr}BA$. It is clear from the above that to get the trace norm of $\Omega^j_{0...0}$ for any $j = 2, \ldots, d - 1$ it suffices to choose $U_{j...j}$ in such way that $W_j^\dagger U_{j...j} V_j = 1$. This means that $U_{j...j} = V_j^\dagger V_j W_j^\dagger$ ($j = 2, \ldots, d - 1$). The remaining $U_{1...iN}$ appearing in the definition of $U_i$ may be chosen at will. Concluding we showed that there exists such $U_i$ that for a fixed $i$ it holds that $(\tilde{\varrho}_A)_{i...i} = \|\Omega^j_{i...i}\|_1$ ($j = 0, \ldots, d - 1$). The fact that also $(\tilde{\varrho}_A)_{i...i} = \|\Omega^j_{i...i}\|_1$ follows obviously from hermiticity of $\varrho_A$.

This is a very useful lemma due to the fact that twistings do not change the cq state. It allows us to concentrate on a particular form of a given state $\varrho_{AA'}$. In other words, we can think about the state $\varrho_{AA'}$ as if it has such a reduction to a subsystem that some of its elements in fixed row or column are trace norms of respective blocks of $\varrho_{AA'}$ (obviously with respect to the same product basis $B_{NN}^{\text{red}}$). As an illustrative example we can consider $\varrho_{AA'}$ with $d = 2$. Then from Eq. [18] it can be written as
\[
\varrho_{AA'} = \begin{bmatrix}
\Omega^0_{0...0} & \Omega^0_{0...1} & \cdots & \Omega^0_{0...N} \\
\Omega^0_{0...1} & \Omega^0_{0...1} & \cdots & \Omega^0_{0...1} \\
\vdots & \vdots & \ddots & \vdots \\
\Omega^0_{0...N} & \Omega^0_{0...N} & \cdots & \Omega^0_{1...1}
\end{bmatrix}, \tag{23}
\]

where $\Omega^j_{i...iN} = (\Omega^j_{i...iN})^\dagger$ and $\Omega^j_{i...iN} \geq 0$ for any $i_k, j_k = 0, 1$. In view of Lemma 3.2 the above may be brought to the following state
\[
\tilde{\varrho}_A \equiv \text{Tr}_A(U_i \varrho_{AA'} U_i^\dagger) = \begin{bmatrix}
\|\Omega^0_{0...0}\|_1 & (\tilde{\varrho}_A)^0_{0...0} & \cdots & (\tilde{\varrho}_A)^0_{0...N} \\
(\tilde{\varrho}_A)^0_{0...1} & \|\Omega^0_{0...1}\|_1 & \cdots & (\tilde{\varrho}_A)^0_{0...1} \\
\vdots & \vdots & \ddots & \vdots \\
(\tilde{\varrho}_A)^0_{0...N} & (\tilde{\varrho}_A)^0_{0...N} & \cdots & \|\Omega^0_{1...1}\|_1
\end{bmatrix}. \tag{24}
\]

Now we are prepared to provide the aforementioned conditions for closeness to multipartite private states (the bipartite case was discussed in Ref. [18]). Firstly we show that if a given $\varrho_{AA'}$ is close to some multipartite pdit then (due to the above lemma) there exist such $U_i$ that the A subsystem has all the elements $(\text{Tr}_A U_i \varrho_{AA'} U_i^\dagger)_{j...j} = \Omega^j_{j...j}$ for $j = 0, \ldots, d - 1$ close to $1/d$.

**Theorem III.2.** Let $\Omega^j_{i...iN}$ be some matrices and $\varrho_{AA'}$ be an $N$-partite state of the form [13] such that $\|\varrho_{AA'} - \Gamma^{(d)}_{AA'}\|_1 \leq \epsilon$ for some multipartite private state $\Gamma^{(d)}_{AA'}$ for some $\epsilon > 0$. Then for a fixed index $i$ one has $\|\Omega^j_{i...i} - (1/d)\|_1 \leq \epsilon$ and $\|\Omega^j_{i...i}\|_1 - (1/d) \leq \epsilon$ for any $j = 0, \ldots, d - 1$.

**Proof.** The proof is a modification of the one given in Ref. [13] (Proposition 3). Let $\Gamma^{(d)}_{AA'}$ be a such private state that $\|\varrho_{AA'} - \Gamma^{(d)}_{AA'}\|_1 \leq \epsilon$ and $U_i$ be such twisting that $\Gamma^{(d)}_{AA'} = U_i (P_{d...N}^{\sigma_A}) U_i^\dagger$ with $\sigma_A$ denoting some state on $\mathcal{H}^C$. Then, due to the invariance of the trace norm under unitary operations, we have
\[
\|U_i^\dagger \varrho_{AA'} U_i - P_{d...N}^{\sigma_A} \|_1 \leq \epsilon. \tag{25}
\]

Now, utilizing the fact that the trace norm can only decrease under the partial trace, we get
\[
\|\tilde{\varrho}_A - P_{d...N}^{\sigma_A} \|_1 \leq \epsilon, \tag{26}
\]

where $\tilde{\varrho}_A$ is of the form [19]. Notice that in general $U_i$ does not have to be the one bringing $\tilde{\varrho}_A$ to the form discussed in Lemma III.1. After application of the exact form of $P_{d...N}^{(+)}$ and $\tilde{\varrho}_A$ given by Eq. [19] one can rewrite
the above as
\[
\left| \sum_{i_1, \ldots, i_N = 0}^{d-1} |i_1 \cdots i_N \rangle \langle j_1 \cdots j_N| \text{Tr} \left( U_{i_1 \cdots i_N \Omega_{i_1 \cdots i_N}^{j_1 \cdots j_N} U_{j_1 \cdots j_N}^\dagger \right) \right|
\]
\[
- \frac{1}{d} \sum_{i, j = 0}^{d-1} |i \rangle \langle j|^{\otimes N} \leq \epsilon.
\] (27)

Now we may utilize the fact that for any \( A = \sum_{ij} a_{ij} |i \rangle \langle j| \) square of its Hilbert–Schmidt norm is given by \( \| A \|_2^2 = \sum_{ij} |a_{ij}|^2 \) and that \( \| A \|_2 \leq \| A \|_1 \). Therefore, if \( \| A \|_2 \leq \epsilon \) for some \( \epsilon > 0 \) then one infers that any of its elements obeys \( |a_{ij}| \leq \epsilon \) \((i, j = 0, \ldots, d - 1)\). This reasoning, after application to the matrix \( \tilde{\varrho}_A - P_{d,N}^{(+)} \), leads us to the conclusion that for any \( i, j = 0, \ldots, d - 1 \) it holds
\[
\left| \text{Tr} \left( U_{i \cdots i} \Omega_{i \cdots i}^{j \cdots j} U_{j \cdots j}^\dagger \right) - \frac{1}{d} \right| \leq \epsilon,
\] (28)
which eventually gives \( |\text{Tr}(U_{i \cdots i} \Omega_{i \cdots i}^{j \cdots j} U_{j \cdots j}^\dagger)| \geq 1/d - \epsilon \). This, after application of the polar decomposition of \( \Omega_{i \cdots i}^{j \cdots j} \) and properties of trace can be rewritten as \( |\text{Tr}(W_{ij} |\Omega_{i \cdots i}^{j \cdots j})| \geq 1/d - \epsilon \) with \( W_{ij} \) being some unitary matrix. Now, applying the Cauchy–Schwarz inequality to the Hilbert–Schmidt scalar product we can infer that for any positive \( A \) and unitary \( W \) the following chain of inequalities holds
\[
|\text{Tr} (WA)| = |\text{Tr} (WVA^\dagger)| \leq \sqrt{\text{Tr}(W^\dagger W)\text{Tr}(V^\dagger V)} = \text{Tr} A = \| A \|_1.
\] (29)

Thus we have that \( \| \Omega_{i \cdots i}^{j \cdots j} \|_1 \geq 1/d - \epsilon \) for any \((i, j = 0, \ldots, d - 1)\).

On the other hand we can apply such twisting \( \tilde{U}_i \) that after application to \( \tilde{\varrho}_A \) and tracing out the \( A \) subsystem we get \( \tilde{\varrho}_A \) such that in its \( i \)th row (or column) \( \langle \tilde{\varrho}_A \rangle_{i \cdots i}^{j \cdots j} = \| \Omega_{i \cdots j} \|_1 \) for \( j = 1, \ldots, d - 1 \). Then, one easily concludes that
\[
\left| \tilde{\varrho}_{A'} \right| \leq \frac{1}{d} \sum_{i,j} |\tilde{\varrho}_{A_{i \cdots i}^{j \cdots j}}| \leq \epsilon
\] (30)
with \( \tilde{\varrho}_{A'} = \tilde{U}_i \tilde{\varrho}_{A \tilde{U}_i^\dagger} \). After the analogous reasoning as in the previous case we get
\[
\left| \| \Omega_{i \cdots i}^{j \cdots j} \|_1 - \frac{1}{d} \text{Tr}(\tilde{W}_{ij} \sigma_{A'}) \right| \leq \epsilon
\] (31)
for some chosen \( i \) and \( j = 0, \ldots, d - 1 \). Here by \( \tilde{W}_{ij} \) we denoted all product of the respective unitary matrices following from product of \( \tilde{U}_i \) and \( U_j \). Using the fact that \(|z_1 - z_2| \geq |z_1| - |z_2|\), we infer from the above inequality that
\[
\left| \| \Omega_{i \cdots i}^{j \cdots j} \|_1 \right| \leq \epsilon + \frac{1}{d} \left| \text{Tr} \left( \tilde{W}_{ij} \sigma_{A'} \right) \right|.
\] (32)

It follows from the Cauchy–Schwarz inequality that the absolute value on the right–hand side is not greater than one. Thus we get the inequalities
\[
\left| \| \Omega_{i \cdots i}^{j \cdots j} \|_1 \right| \leq \epsilon + \frac{1}{d}
\] (33)
for the chosen \( i \) and \( j = 0, \ldots, d - 1 \). Joining this facts together we get the desired result.

Notice that in the particular case of \( d = 2 \), discussed already in Ref. [13] (Proposition 3), the only condition for \( \| \Omega_{0 \cdots 0}^{1 \cdots 1} \|_1 \) (and equivalently for \( \| \Omega_{1 \cdots 1}^{0 \cdots 0} \|_1 \)) is that \( \| \Omega_{0 \cdots 0}^{1 \cdots 1} \|_1 \geq 1/2 - \epsilon \). This is because, due to the fact that \( \text{Tr} \tilde{\varrho}_A = 1 \) and the positivity of \( \tilde{\varrho}_A \geq 0 \) (and thus also of the \( 2 \times 2 \) matrix containing the elements \( \| \Omega_{i \cdots j} \|_1 \)), with \( i, j = 0, 1 \) \( \| \Omega_{0 \cdots 0}^{1 \cdots 1} \|_1 \leq 1/2 \).

Interestingly, one may prove also a converse statement, namely if after applying respective twisting \( U_i \), for some fixed row, say the \( i \)th one, all \( \| \Omega_{i \cdots j} \|_1 \) are close to \( 1/d \), then there exists some multipartite private state close to a given state \( \varrho_{AA'} \).

\textbf{Theorem III.3.} Let \( \varrho_{AA'} \) given by Eq. (32) be such that for a fixed \( i \) the blocks \( \Omega_{i \cdots j} \) obey \( \| \Omega_{i \cdots j} \|_1 \geq 1/d - \epsilon \) for any \((j = 0, \ldots, d - 1)\) and \( \| \varrho_{AA'} \|_1 \leq 1/2 \). Thus there exists such a multipartite private state \( \varrho_{AA'}^{(d)} \) that
\[
\| \varrho_{AA'} - \Gamma_{\tilde{\varrho}_A}^{(d)} \|_1 \leq \sqrt{\log 2 \left[ 2N \sqrt{d \eta(c)} \log d + H(2 \sqrt{d \eta(c)}) \right] + 2 \sqrt{d \eta(c)}}
\] (34)
where \( \eta(c) \rightarrow 0 \) if \( c \rightarrow 0 \) and consequently the function on the right–hand side tends to zero whenever \( \epsilon \rightarrow 0 \). Here \( H \) denotes the binary entropy.

\textbf{Proof.} The proof is based on the one given in Ref. [13]. Let \( U_i \) be such twisting that for fixed \( i \) it holds of \( \langle \tilde{\varrho}_A \rangle_{i \cdots i}^{j \cdots j} = \| \Omega_{i \cdots i}^{j \cdots j} \|_1 \) \((j = 0, \ldots, d - 1)\). Then since \( \langle \tilde{\varrho}_A \rangle_{i \cdots i}^{j \cdots j} = [(\tilde{\varrho}_A)_{i \cdots i}^{j \cdots j}]^* \) with asterisk denoting complex conjugation, the Hilbert–Schmidt scalar product of \( \tilde{\varrho}_A \) and \( P_{d,N}^{(+)} \) may be expressed as
\[
\text{Tr} \tilde{\varrho}_A P_{d,N}^{(+)} = \frac{1}{d} \sum_{i,j=0}^{d-1} (\tilde{\varrho}_A)_{i \cdots i}^{j \cdots j} + \frac{2}{d} \sum_{i,j=0}^{d-1} \text{Re}(\tilde{\varrho}_A)_{i \cdots i}^{j \cdots j}.
\] (35)

On the other hand from the positivity of \( \tilde{\varrho}_A \) one may prove the following inequality
\[
\sum_{i=0}^{d-1} (\tilde{\varrho}_A)_{i \cdots j}^{i \cdots i} \geq \frac{2}{d-1} \sum_{i=0}^{d-1} \text{Re}(\tilde{\varrho}_A)_{i \cdots j}^{i \cdots i}.
\] (36)

which after substitution to Eq. (35) gives
\[
\text{Tr} \tilde{\varrho}_A P_{d,N}^{(+)} \geq \frac{2}{d-1} \sum_{i,j=0}^{d-1} \text{Re}(\tilde{\varrho}_A)_{i \cdots i}^{j \cdots j}.
\] (37)
Now we can utilize Lemma A.2 (see Appendix) to the $d \times d$ matrix with entries $(\tilde{\rho}_{a})_{i,j}^{\perp}$ ($i,j = 0, \ldots, d - 1$). Namely, due to the assumption that for some fixed $i$ the elements $(\tilde{\rho}_{a})_{i,j}^{\perp}$ satisfy $| (\tilde{\rho}_{a})_{i,j}^{\perp} - 1/d | \leq \epsilon$, we have from Lemma A.2 that $| (\tilde{\rho}_{a})_{i,j}^{\perp} - 1/d | \leq \eta(\epsilon)$ for any $i,j = 0, \ldots, d - 1$ with $\eta(\epsilon) \to 0$ for $\epsilon \to 0$. This means that the real parts of any $(\tilde{\rho}_{a})_{i,j}^{\perp}$ also satisfies the above condition. In this light we get from Eq. (37) that

\[
\text{Tr} \tilde{\rho}_{a} P^{(+)}_{d,N} \geq \frac{2}{d - 1} \sum_{i,j=0}^{d-1} \text{Re}(\tilde{\rho}_{a})_{i,j}^{\perp} \geq \frac{2}{d - 1} \sum_{i,j=0}^{d-1} \left( \frac{1}{d} - \eta(\epsilon) \right) = \frac{d(d-1)}{2} \left( \frac{1}{d} - \eta(\epsilon) \right) = 1 - d\eta(\epsilon),
\]

(38)

where the first equality follows from the fact that the respective sum contains $d(d - 1)/2$ elements. The remainder of the proof goes along the same line as its bipartite version from Ref. [13] leading to the claimed inequality.

Notice that to prove the theorem for the particular case of $d = 2$ it suffices to assume that $\| \Omega^{0}_{i=1} \|_{1} \geq 1/2 - \epsilon$.

Concluding we obtained necessary and sufficient conditions for a given state $\rho_{A^{n}}$ to be close to some multipartite private state expressed in terms of the trace norm of some blocks of $\rho_{A^{n}}$ (see Eq. (18)).

\section{DISTILLABLE CRYPTOGRAPHIC KEY}

\subsection{Definition}

Having introduced the concept of multipartite private states we may pass to the definition of multipartite cryptographic key. The seminal fact behind the notion of multipartite private states is that as shown in Refs. [12, 13], one can think about quantum cryptography as a distillation of private states by means of LOCC. In other words, we have a standard distillation scheme (as entanglement distillation) in which we can forget about the eavesdropper.

\textit{Definition IV.1.} Let $\rho_{A}$ denote a given multipartite state acting on $\mathbb{C}^{d_{1}} \otimes \ldots \otimes \mathbb{C}^{d_{N}}$ and $(\Lambda_{n})_{n=1}^{\infty}$ a sequence of LOCC operations giving $\Lambda_{n} (\rho^{(n)}_{A}) = \rho^{(n)}_{A^{n}}$ with $\rho^{(n)}_{A^{n}}$ being a state acting on $(\mathbb{C}^{d_{1}})^{\otimes n} \otimes \mathcal{H}_{n}^{n}$, where $\mathcal{H}_{n}$ stands for a finite-dimensional Hilbert space corresponding to the $A'$ part of $\rho^{(n)}_{A^{n}}$. Then we say that $\Lambda = (\Lambda_{n})_{n=1}^{\infty}$ is a multipartite private state distillation protocol if there exists such a family of multipartite private states $(\Gamma^{(a_{n})}_{A^{n}})_{n=1}^{\infty}$ that the condition

\[
\lim_{n \to \infty} \| \rho^{(n)}_{A^{n}} - \Gamma^{(a_{n})}_{A^{n}} \|_{1} = 0
\]

(39)

holds. A rate of the protocol $\Lambda$ is defined as $R_{\Lambda} (\rho_{A}) = \limsup_{n \to \infty} [(1/n) \log d_{n}]$ and the distillable key as

\[
K_{D} (\rho_{A}) = \sup_{\Lambda} R_{\Lambda} (\rho_{A}).
\]

(40)

As shown in the bipartite case in Ref. [13], both the Definition II.1 and Definition IV.1 are equivalent in the sense that if there exists LOCC protocol distilling some multipartite private state there also exists LOPC protocol distilling the ideal ccq state (when purification is considered) with the same rate. As the proof from Ref. [13] may also be applied to the multipartite case, we provide the generalized version of the above fact below.

\textit{Theorem IV.1.} The following two implications hold. Assume that from a given state $\sigma_{A}$ such that Eve has its purification $| \psi_{A \bar{E}} \rangle$ one may create by LOPC some ccq state $\rho^{(eq)}_{A \bar{E}}$ (see Eq. (1)) obeying $\| \rho^{(eq)}_{A \bar{E}} - \rho^{(id)}_{A \bar{E}} \|_{1} \leq \epsilon$ for some $\epsilon > 0$ (recall that $\rho^{(id)}_{A \bar{E}}$ denotes the ideal ccq state given by Eq. (2)). Then there exists such LOCC protocol that can distill a state $\rho^{(eq)}_{A^{n}A^{n}'}$ from $\sigma_{A}$ that satisfies $\| \rho^{(eq)}_{A^{n}A^{n}'} - \Gamma^{(d_{n})}_{A^{n}A^{n}'} \|_{1} \leq 2\sqrt{\epsilon}$ for some multipartite private state $\Gamma^{(d_{n})}_{A^{n}A^{n}'}$. On the other hand if from $\sigma_{A}$ one can distill a state $\rho^{(eq)}_{A}$ close to some pdt $\Gamma^{(d_{n})}_{A^{n}A^{n}'}$, i.e., such that $\| \rho^{(eq)}_{A} - \Gamma^{(d_{n})}_{A^{n}A^{n}'} \|_{1} \leq \epsilon$ then there exists a LOPC protocol distilling from $\rho_{A}$ a ccq state such that $\| \rho^{(eq)}_{A} - \rho^{(id)}_{A} \|_{1} \leq 2\sqrt{\epsilon}$. Each subsystem of the $A$ part of $\rho^{(eq)}_{A}$ and of the key part of $\Gamma^{(d_{n})}_{A^{n}A^{n}'}$ is defined on $\mathbb{C}^{d_{n}}$.

\textit{Proof.} The proof goes directly along the same lines as the one from Ref. [13].

Interestingly, the distillable key $K_{D}$ may be used to quantify entanglement among multipartite states. More precisely, from the definition it follows that $K_{D}$ is monotonic under the action of LOCC operations (see e.g. [29]). Moreover, it vanishes on multipartite states that have at least one separable cut, which is a consequence of the straightforward multipartite generalization of the results from Ref. [2] provided in Ref. [30]. Finally, as we shall show the distillable key is normalized on GHZ states $P^{(+)}_{d,N}$ in the sense that $K_{D} (P^{(+)}_{d,N}) = \log d$. However, firstly we need to provide two bounds on $K_{D}$.

\subsection{Bounds on the distillable key}

The first bound is a simple multipartite generalization of the upper bound provided in Ref. [13], while the second bound is a consequence of a multipartite adaptation of the Devetak–Winter protocol [12]. Let us start from the upper bound.

\textit{Theorem IV.2.} Let $\rho_{A}$ be some $N$-partite state. Then

\[
K_{D} (\rho_{A}) \leq F_{r}^{\infty} (\rho_{A}).
\]

(41)

where $F_{r}^{\infty} (\rho_{A})$ is a regularized version of the relative entropy, i.e.,

\[
F_{r}^{\infty} (\rho_{A}) = \lim_{n \to \infty} \frac{1}{n} \inf_{\sigma_{A}^{e} \in \mathcal{D}} S (\rho^{(n)}_{A} \| \sigma_{A}^{e}).
\]

(42)
and $\mathcal{D}$ denotes the set of all $N$–partite fully separable states, i.e., states of the form

$$\varrho_{\text{sep}} = \sum_{i} p_{i} \varrho_{A_{i}}^{(i)} \otimes \cdots \otimes \varrho_{A_{N}}^{(i)}.$$  \hfill (43)

**Proof.** The proof is a generalization of the one from Ref. 1.3.

Interestingly, we may also bound $K_{D}$ from below. For this purpose we need to prove the following theorem.

**Theorem IV.3.** Let $\varrho_{AE}^{(\text{eq})}$ be some multipartite cq state acting on $(\mathbb{C}^{d})^{\otimes N} \otimes \mathbb{C}^{d_{E}}$ and given by

$$\varrho_{AE}^{(\text{eq})} = \sum_{i_{1}, \ldots, i_{N} = 0}^{d-1} p_{i_{1} \ldots i_{N}} \ket{i_{1} \ldots i_{N}} \bra{i_{1} \ldots i_{N}}.$$  \hfill (44)

Then it is arbitrarily close to the ideal cq state if and only if for a chosen party $A_{i}$ all the reductions to three–partite systems $A_{i}A_{j}E$ with $j \neq i$ are arbitrarily close to the bipartite ideal cq state. More precisely, if $\| \varrho_{AE}^{(\text{eq})} - \varrho_{AE}^{(N,\text{id})} \| \leq \epsilon$ holds for $\epsilon > 0$, then for the fixed party $A_{i}$ the following inequalities

$$\left\| \sum_{i_{1}, \ldots, i_{N} = 0}^{d-1} p_{i_{1} \ldots i_{N}} \ket{i_{i_{i} i_{j}} \bra{i_{i_{i} i_{j}}} \otimes \varrho_{AE}^{E} - \varrho_{AE}^{(2,\text{id})} \right\|_{1} \leq \epsilon$$

are satisfied for $j = 1, \ldots, i-1, i+1, \ldots, N$. Conversely, assuming that for fixed $A_{i}$ the inequalities \hfill (45) hold for $\epsilon > 0$ and $j \neq i$, one has

$$\left\| \varrho_{AE}^{(\text{eq})} - \varrho_{AE}^{(N,\text{id})} \right\|_{1} \leq (4N-3) \epsilon$$  \hfill (46)

**Proof.** We proceed in two steps. In the first step we show that if the trace norm distance between some multipartite cq state $\varrho_{AE}^{(\text{eq})}$ and the ideal one is bounded by some $\epsilon > 0$ then any bipartite state arising by tracing out $N-2$ parties from the cq state is close to the bipartite ideal cq state. This part of the proof is relatively easy since it suffices to utilize the fact that the trace norm distance does not increase under the partial trace. The proof of the converse statement is much more sophisticated.

Let us assume that the following

$$\left\| \varrho_{AE}^{(\text{eq})} - \varrho_{AE}^{(N,\text{id})} \right\|_{1} \leq \epsilon$$  \hfill (47)

holds for some small $\epsilon > 0$. Then since the trace norm does not increase under the partial trace we have immediately the following set of inequalities

$$\left\| \sum_{i_{1}, \ldots, i_{N} = 0}^{d-1} p_{i_{1} \ldots i_{N}} \ket{i_{k_{i} i_{i}} \bra{i_{k_{i} i_{i}}} \otimes \varrho_{AE}^{E} - \varrho_{AE}^{(2,\text{id})} \right\|_{1} \leq \epsilon$$

for any pair of indices $k, l = 1, \ldots, N$. To end the first part of the proof it suffices to substitute $\sum_{i \neq \{k, l\}} p_{i_{1} \ldots i_{N}} \varrho_{AE}^{E} - \varrho_{AE}^{(2,\text{id})}$, where summation over $I \setminus \{k, l\}$ means that we sum over all $ij$ but $ik$ and $i_{l}$.

To proceed with the second part of the proof we assume that one chosen party, say $A_{1}$, shares with the remaining $N-1$ parties a state that is close to the bipartite ideal cq state. In other words we assume that for any $J = 2, \ldots, N$ the following inequalities

$$\left\| \sum_{i_{1}, \ldots, i_{N} = 0}^{d-1} p_{i_{1} \ldots i_{N}} \ket{i_{i_{1} i_{j}} \bra{i_{i_{1} i_{j}}} \otimes \varrho_{AE}^{E} - \varrho_{AE}^{(2,\text{id})} \right\|_{1} \leq \epsilon$$

are satisfied. Basing on this set of inequalities we will show that the left–hand side of Eq. \hfill (47) is bounded from above by some linear function of $\epsilon$ vanishing for $\epsilon \to 0$. For this purpose let us denote the left–hand side of Eq. \hfill (47) by LHS and notice that it can be split into two sums (see Eqs. \hfill (2) and \hfill (4)), namely the one containing the elements for $i_{1} = \ldots = i_{N}$ and the rest ones. In this light, denoting by $I$ the set of sequences $(i_{1}, \ldots, i_{N})$ obtained by removing all those with $i_{1} = \ldots = i_{N}$ from the set of all possible sequences, we can write

$$\text{LHS} = \sum_{(i_{1}, \ldots, i_{N}) \in I} p_{i_{1} \ldots i_{N}} + \sum_{i_{1} \neq i_{2}} \sum_{i_{1} = 0}^{d-1} p_{i_{1} \ldots i_{N}} \left\| \varrho_{AE}^{E} - \varrho_{AE}^{(2,\text{id})} \right\|_{1}$$

$$+ \sum_{i_{1} \neq i_{2}} \left| p_{i_{1} \ldots i_{N}} - \frac{1}{d} \right|| = 1 \right|,$$

where the inequality comes from the fact that the term $p_{i_{1} \ldots i_{N}} \varrho_{AE}^{E}$ was added and subtracted in the second term in the first line and from the inequality $\| A + B \|_{1} \leq \| A \|_{1} + \| B \|_{1}$. The last equality is a simple consequence of the fact that the trace norm of any density matrix is just one. In what follows, using the inequalities \hfill (49), we show that all the three terms appearing in the above are bounded by linear functions of $\epsilon$ vanishing for $\epsilon \to 0$. With this aim, utilizing once more the fact that the trace norm does not increase under the partial trace, we can infer from Eq. \hfill (47) that

$$\left\| \sum_{i_{1}, \ldots, i_{N} = 0}^{d-1} p_{i_{1} \ldots i_{N}} \ket{i_{i_{1} i_{j}}} \bra{i_{i_{1} i_{j}}} \otimes \varrho_{AE}^{E} - \varrho_{AE}^{(2,\text{id})} \right\|_{1} \leq \epsilon$$

for $j = 2, \ldots, N$. Now we can divide all the terms appearing in the first sum into two groups, namely, the one for $i_{1} = i_{j}$ and the remaining terms. This, after calculating
the respective norms, leads to the following inequality
\[
\sum_{i_0 = 0}^{d-1} \sum_{i_2, i_3 = 0}^{i_1, \ldots, i_{j-1}, i_{j+1}, \ldots, i_N = 0} p_{ii_2i_3} - \frac{1}{d} \leq \epsilon.
\] (53)

From the sum appearing under the sign of an absolute value in (53), we can extract the probability \(p_{i_1 \ldots i_N}\), obtaining
\[
\sum_{i_0 = 0}^{d-1} \sum_{i_2, i_3 = 0}^{i_1, \ldots, i_{j-1}, i_{j+1}, \ldots, i_N = 0} p_{ii_2i_3} - \frac{1}{d} \leq \epsilon,
\] (55)

where \(I_i\) denotes the strings of \(N - 2\) indices \((i_2, \ldots, i_{j-1}, i_{j+1}, \ldots, i_N)\) such that at least one of them is different from \(i\). Utilizing a simple inequality \(|z_1 - z_2| \geq |z_1| - |z_2|\) satisfied by all \(z_1, z_2 \in \mathbb{C}\), we get
\[
\sum_{i_0 = 0}^{d-1} p_{i_1 \ldots i_N} - \frac{1}{d} \leq \epsilon + \sum_{i_0 = 0}^{d-1} \sum_{(i_2, \ldots, i_{j-1}, i_{j+1}, \ldots, i_N) \in \bar{I}_j} p_{ii_2i_3} - \frac{1}{d} \leq \epsilon + \sum_{(i_1, \ldots, i_N) \in \bar{I}_j} p_{i_1 \ldots i_N},
\] (56)

where \(\bar{I}_j\) denotes the string of \(N\) indices such that the first and \(j\)th ones are equal \((i_1 = i_j)\) and at least one of the remaining ones is different from \(i_1\). One sees that the second term on the right–hand side of Eq. (56) may be bounded from above in the following way
\[
\sum_{(i_1, \ldots, i_N) \in \bar{I}_j} p_{i_1 \ldots i_N} \leq \sum_{k=2}^{j-1} \sum_{i_k \neq i_1, i_k \neq i_j} p_{i_1 \ldots i_N}
\]
\[
+ \sum_{k=j+1}^{N} \sum_{i_k \neq i_1, i_k \neq i_j} p_{i_1 \ldots i_N}
\]
\[
\leq \sum_{k=2}^{j-1} \epsilon + \sum_{k=j+1}^{N} \epsilon
\]
\[
= (N - 2) \epsilon,
\] (57)

where the second inequality is a consequence of the inequality given in Eq. (54). Finally, application of Eq. (57) to Eq. (56), gives
\[
\sum_{i_0 = 0}^{d-1} p_{i_1 \ldots i_N} - \frac{1}{d} \leq (N - 1) \epsilon.
\] (58)

This is a quite natural conclusion saying that if the measurement outcomes between fixed party (here \(A_1\)) and each of the remaining ones are almost perfectly correlated, then the measurement outcomes are almost perfectly correlated among all the parties.

We have still two terms in Eq. (50) unbounded. Using once again the inequality \(|z_1 - z_2| \geq |z_1| - |z_2|\) \((z_1, z_2 \in \mathbb{C})\) and the fact that \(p_{i_1 \ldots i_N}\) represents some probability distribution we may write
\[
\sum_{(i_1, \ldots, i_N) \in I} p_{i_1 \ldots i_N} = 1 - \sum_{i_0 = 0}^{d-1} p_{i_1 \ldots i_N}
\]
\[
\leq 1 - \left[1 - (N - 1) \epsilon\right]
\]
\[
= (N - 1) \epsilon.
\] (59)

Thus, the only thing we need is to bound from above the last term in Eq. (50). Remarkably, to achieve this aim it suffices to utilize a single inequality from the whole set (49), say the one for \(j = 2\). The we can write
\[
\left\| \sum_{i_1, \ldots, i_N = 0}^{d-1} p_{i_1 \ldots i_N} |i_1 i_2| i_1 i_2 \right\|_1 - \frac{1}{d} \sum_{i = 0}^{d-1} |i\rangle \langle i| \otimes g^E
\]
\[
= \left\| \sum_{i = 0}^{d-1} p_{i \ldots i} |i\rangle \langle i| \otimes g_{i \ldots i}^E - \frac{1}{d} \sum_{i = 0}^{d-1} |i\rangle \langle i| \otimes g^E + \sum_{(i_1, \ldots, i_N) \in \mathcal{E}_2} p_{i_1 \ldots i_N} |i_1 i_1\rangle i_1 i_1 \otimes g_{i_1 i_1}^E + \sum_{i_1 \ldots i_N = 0} p_{i_1 \ldots i_N} |i_1 i_2\rangle i_1 i_2 \otimes g_{i_1 i_2}^E \right\|_1.
\]

Then, due to the fact that \(\|A - B\|_1 \geq \|A\|_1 - \|B\|_1\), we may rewrite the above as
\[
\left\| \sum_{i = 0}^{d-1} p_{i \ldots i} |i\rangle \langle i| \otimes g_{i \ldots i}^E - \frac{1}{d} \sum_{i = 0}^{d-1} |i\rangle \langle i| \otimes g^E + \sum_{(i_1, \ldots, i_N) \in \mathcal{E}_2} p_{i_1 \ldots i_N} |i_1 i_1\rangle i_1 i_1 \otimes g_{i_1 i_1}^E + \sum_{i_1 \ldots i_N = 0} p_{i_1 \ldots i_N} |i_1 i_2\rangle i_1 i_2 \otimes g_{i_1 i_2}^E \right\|_1 \leq \epsilon + \sum_{(i_1, \ldots, i_N) \in \mathcal{E}_2} p_{i_1 \ldots i_N} + \sum_{i_1 \ldots i_N = 0} p_{i_1 \ldots i_N}
\]
\[
\leq \epsilon + (N - 2)\epsilon + \epsilon = N\epsilon,
\]
where the second inequality follows from Eqs. 62 and 67 (with \(j = 2\)). On the other hand, we can easily show that
\[
\left\| \sum_{i = 0}^{d-1} p_{i \ldots i} |i\rangle \langle i| \otimes g_{i \ldots i}^E - \frac{1}{d} \sum_{i = 0}^{d-1} |i\rangle \langle i| \otimes g^E - \epsilon + (N - 2)\epsilon + \epsilon = N\epsilon,
\]
\[
\left\| \sum_{i = 0}^{d-1} p_{i \ldots i} |i\rangle \langle i| \otimes g_{i \ldots i}^E - \frac{1}{d} \sum_{i = 0}^{d-1} |i\rangle \langle i| \otimes g^E \right\|_1 \geq \sum_{i = 0}^{d-1} p_{i \ldots i} \|g_{i \ldots i}^E - g^E\|_1 - \sum_{i = 0}^{d-1} p_{i \ldots i} - \frac{1}{d}.
\]

Comparison of Eqs. 65, 61 and 62 allows us to write
\[
\sum_{i = 0}^{d-1} p_{i \ldots i} \|g_{i \ldots i}^E - g^E\|_1 \leq N\epsilon + \sum_{i = 0}^{d-1} p_{i \ldots i} - \frac{1}{d}
\]
\[
\leq N\epsilon + (N - 1)\epsilon = (2N - 1)\epsilon.
\]

Putting now all the pieces together, that is, substituting Eqs. 65, 59, and 63 to Eq. 60, we finally have
\[
\left\| \sum_{i_1 \ldots i_N = 0}^{d-1} p_{i_1 \ldots i_N} |i_1 \ldots i_N\rangle i_1 \ldots i_N \otimes g_{i_1 \ldots i_N}^E - \frac{1}{d} \sum_{i = 0}^{d-1} |i\rangle \langle i| \otimes g^E \right\|_1 \leq (4N - 3)\epsilon.
\]

Noting that for fixed \(N\) it holds that \((4N - 3)\epsilon \rightarrow 0\) whenever \(\epsilon \rightarrow 0\) we finish the proof.

It should be mentioned that as it follows from the second part of the proof, we do not need to assume the whole set of inequalities given in 49. Actually it suffices to assume that a single inequality from the set 49 holds and the remaining ones from the set given in Eq. 51. In other words it suffices to assume that the measurement outcomes between a fixed party and any from the other parties are almost perfectly correlated and that Eve is almost completely uncorrelated from the measurement outcomes of a single pair. This is in full agreement with our intuition. Namely, if the measurement outcomes of any pair \(A_i A_j\) (with fixed \(i\) and arbitrary \(j \neq i\)) are perfectly correlated and Eve has full knowledge about the measurement outcomes of just a single party, she actually has the knowledge about measurement outcomes of all parties. Therefore if all the parties have perfect correlations and Eve is completely uncorrelated from a single party, she must be completely uncorrelated from all the parties. Consequently, it is sufficient to assume that a single pair shares state that is close to a ccq state and other chosen pairs have almost perfect correlations.

Now we are prepared to provide a lower bound on the multipartite distillable key in the LOPC paradigm. We achieve this by extending of the Devetak–Winter protocol to the multipartite case. We do this by applying the bipartite Devetak–Winter protocol to \(N - 1\) pairs of parties in some state \(g_{AE}\) such that each of them consist of one chosen party, say \(A_1\), and one of the remaining ones. Everything works as in the standard Devetak–Winter protocol, i.e., the party \(A_1\) performs the measurement in some
basis, e.g. the standard one obtaining the so-called cq state (classical–quantum...–quantum)
\[ \varrho_{AE}^{(cq)} = \sum_i p_i |i\rangle\langle i|_{A_1} \otimes \varrho_{A_2...A_N E}^{(i)}. \tag{65} \]

Then, roughly speaking, the party \( A_1 \) performs the Devetak–Winter protocol with the remaining parties simultaneously. One knows that the correlation between \( A_1 \) and the remaining parties \( A_j \) \((j = 2, \ldots, N)\) are described by the mutual information \( I(A_1 : A_j)(\varrho_{A_1 A_j E}^{(cq)}) \). However, the establish common multipartite key we need to consider the worst case, i.e., \( \min_{j=2,\ldots,N} I(A_1 : A_j)(\varrho_{A_1 A_j E}^{(cq)}) \). On the other hand, the correlation between \( A_1 \) and \( E \) are given by \( I(A_1 : E) \) and this amount of bits has to be subtracted at the privacy amplification stage of the process.

Consequently, the rate of the protocol is
\[ \min_{j=2,\ldots,N} I(A_1 : A_j)(\varrho_{A_1 A_j E}^{(cq)}) - I(A_1 : E)(\varrho_{A_1 A_j E}^{(cq)}) \tag{66} \]
and therefore, the multipartite distillable key satisfies
\[ C_D(\varrho_{AE}) \geq \min_{j=2,\ldots,N} I(A_1 : A_j)(\varrho_{A_1 A_j E}^{(cq)}) - I(A_1 : E)(\varrho_{A_1 A_j E}^{(cq)}). \tag{67} \]

Here, \( \varrho_{A_1 A_j E}^{(cq)} \) denotes the cq state, which arises from \( (65) \) by tracing out all the parties but the first and \( j \)th one and Eve. Moreover, by \( I(X : Y)(\varrho_{XY}) \) we denoted the mutual information defined as \( I(X : Y)(\varrho_{XY}) = S(\varrho_X) + S(\varrho_Y) - S(\varrho_{XY}) \) with \( S \) denoting the von Neumann entropy.

We have still some freedom in choosing the distributing party and therefore we can always choose the one for which the rate of the extended Devetak–Winter protocol is highest. In this way we get the lower bound on \( C_D \) of the form
\[ C_D(\varrho_{AE}) \geq \max_{i=1,\ldots,N} \frac{1}{d} \sum_{i=0}^{d-1} |i\rangle\langle i| \otimes |i\rangle\langle i| \tag{68} \]

Let us finally mention that due to the Theorem IV.1 we can also bound \( K_D \) from below using \( (65) \). Namely, since \( K_D(\varrho_{AE}) = C_D(\psi_{AE}) \), we have the following
\[ K_D(\varrho_{AE}) \geq \max_{i=1,\ldots,N} \left[ \min_{j=1,\ldots,N} I(A_1 : A_j) - I(A_1 : E) \right] \tag{69} \]

where the respective quantities are calculated from e.g., the cq state following the purification of \( \varrho_{AE} \).

Now we can go back to the definition of \( K_D \). As previously mentioned, it holds that \( K_D(P_{d,N}^{(+)}(E)) = \log d \). To show it explicitly, on the one hand we can utilize the above bound. We know from Theorem IV.1 that \( K_D(P_{d,N}^{(+)}(E)) = C_D(\psi_{AE}) \), where \( \psi_{AE} \) is a purification of \( P_{d,N}^{(+)}(E) \) and obviously has the form \( \psi_{AE}(E) \) with \( |E\rangle \) being some state kept by Eve. Measurement of the A subsystem of \( \psi_{AE} \) with respect to the standard basis leads us to the ideal cq state \( \varrho_{AE}^{(eq)} = \omega_{d,N} \otimes |E\rangle\langle E| \), where
\[ \omega_{d,N} = \frac{1}{d} \sum_{i=0}^{d-1} |i\rangle\langle i| \otimes |i\rangle\langle i| \tag{70} \]
which has the quantities \( I(A_1 : A_j) = \log d \) \((i, j = 1, \ldots, N)\) and \( I(A_1 : E) = \log d \) \((i = 1, \ldots, N)\). Substituting both these facts into Eq. \( (68) \) gives us \( K_D(P_{d,N}^{(+)}(E)) \geq \log d \).

On the other hand we can utilize the bound given in Eq. \( (11) \). Firstly, notice that \( S(\rho_{d,n}^{(n)}(\sigma_{d,n}^{(n)}) = n S(\rho_{d,n}^{(n)} \| \sigma_{d,n}^{(n)}) \) for two an arbitrary natural number \( n \) and arbitrary density matrices \( \rho \) and \( \sigma \). Secondly, one easily finds that (see e.g. Ref. \( [31] \))
\[ S(P_{d,N}^{(+)} \| \omega_{d,N}) = \log d \tag{71} \]
and consequently the following estimate holds
\[ K_D(P_{d,N}^{(+)}(E)) = \lim_{n \to \infty} \frac{1}{n} \inf_{\varrho_{d,n}^{(n)} \in D} S(P_{d,N}^{(+)} \| \varrho_{d,n}^{(n)}) \leq \lim_{n \to \infty} \frac{1}{n} n S(P_{d,N}^{(+)} \| \omega_{d,N}) \]
\[ = \lim_{n \to \infty} \frac{1}{n} n S(P_{d,N}^{(+)} \| \omega_{d,N}) \]
\[ = \log d. \tag{72} \]

Thus \( K_D(P_{d,N}^{(+)}(E)) \leq \log d \) and taking into account the previously obtained inequality \( K_D(P_{d,N}^{(+)}(E)) \leq \log d \) we infer \( K_D(P_{d,N}^{(+)}(E)) = \log d \). Thus, as stated previously, the multipartite distillable key may be considered as an entanglement measure.

Let us discuss the last issue of this section. To apply the extended Devetak–Winter protocol successfully, that is to get a nonzero rate, one obviously has to have the right-hand side of Eq. \( (68) \) positive. One knows from Theorem IV.1 that distillation of some multipartite private state by means of LOCC is equivalent to the distillation of an ideal cq state by means of LOPC. This in turn means that the closer some particular state \( \varrho_{AE} \) is to some multipartite private state, the closer it is to the ideal state. Then, from Theorem IV.3 it follows that the closer some cq state is to the ideal cq state the closer are its bipartite reductions to the bipartite ideal cq state. Both these facts mean that by distilling some multipartite private state from copies of a given state we can make the right-hand side of Eq. \( (68) \) (equivalently Eq. \( [31] \)) positive. Consequently, concatenating some LOCC protocol distilling multipartite private states (an example of such a protocol is given in the following subsection) and the extended
Devetak–Winter protocol introduces a subtle effect here. Namely, on the one hand, using more copies in the LOCC protocol producing a state that is closer to some multipartite private state makes the right-hand side of Eq. (65) larger. On the other hand spending more copies decreases the success probability which needs to be included in the overall rate of the protocol. This issue will become more clear when some particular classes of states will be investigated in the next section.

C. Recursive LOCC protocol distilling multipartite private states

Here we provide an illustrative example of a recursive LOCC protocol allowing for distillation of multipartite private states from some classes of states. This protocol is a generalization of the LOCC protocol discussed in Ref. [12, 13] to the case of an arbitrary number of parties. Assume then that \( N \) parties \( A_1, \ldots, A_N \) have \( k \) copies of some state \( \rho_{AA} \) in their possession. In ith step each party performs the following operations.

- Take the state \( \rho_{AA}^{(i-1)} \) (where \( \rho_{AA}^{(0)} = \rho_{AA} \)) and one of the remaining \( k - i \) copies of \( \rho_{AA} \).
- Treating A part of \( \rho_{AA}^{(i-1)} \) (\( \rho_{AA} \)) as source (target) qubits, perform CNOT operations.
- Finally, the parties perform the measurement in computational basis on the target qubits and compare the results: in the case of equal results (all zeros or all ones) the parties keep the state, otherwise they get rid of it.

In this way, spending \( k \) copies of some state \( \rho_{AA} \), all the parties can distill a state \( \rho_{AA}^{(k)} \) that is closer to some multipartite private state than the initial one, i.e., \( \rho_{AA} \). Quantitative analysis concerning this protocol after application to two different constructions of states may be found in Sections V.A and V.B.

D. Multpartite privacy squeezing

Concluding the discussion concerning the distillable key we need to mention the multipartite version of the so-called privacy squeezing [12, 13] together with its application in the recent important method [16] of bounding the secret key from below. Following Lemma III.1 we know that having some state \( \rho_{AA} \) expressed in the form (13), there always exists a twisting \( U_t \) that the state \( \overline{\rho}_A = \text{Tr}_{A'}(U_t \rho_{AA} U_t^\dagger) \) has some special form. Namely, in some chosen row (column) some of its entries are trace norms of respective blocks of \( \rho_{AA} \). We will call the state \( \overline{\rho}_A \) obtained in this way privacy squeezed state. Furthermore, we already know that twistings do not change the cq state with respect to some basis \( B_{N}^{\text{prod}} \).

Let us now proceed by stating some of the conclusion following both the above facts. As previously mentioned we have that \( K_D(\overline{\rho}_A) = C_D(\psi_{AE}) \), where \( |\psi_{AE} \rangle \) denotes the purification of \( \overline{\rho}_A \). Assuming that all the parties share some state \( \rho_{AA} \) defined on \( H \otimes H' \) and denoting by \( |\psi_{AA'E} \rangle \) the purification of \( \rho_{AA} \), we have

\[
K_D(\rho_{AA'}) = C_D(|\psi_{AA'E} \rangle) \geq C_D(\rho_{AE}) \geq C_D(\rho_{AE}^{(\text{eq})}).
\]

Here \( \rho_{AE} = \text{Tr}_A(\psi_{AA'E}) \) and \( \rho_{AE}^{(\text{eq})} \) stands for a cq state obtained upon the measurement of the A subsystem in \( B_{N}^{\text{prod}} \). The first inequality follows from the fact that throwing out the A’ subsystem one can only lower the key as it could be treated ‘virtually’ as giving it to Eve. The second inequality is a consequence of the fact that measurement in some product basis leads to classical state on the A part of the state (notice that such measurement is LOPC operation which due to the definition of \( C_D \) can only lower its value).

Now we can formulate and prove the following theorem as a multipartite generalization of the bipartite considerations from Ref. [16] (cf. [14]) which exploit privacy squeezing to bound the secure key from below.

Theorem IV.4. Let \( \rho_{AA'} \) be some \( N \)-partite state defined on \( H \otimes H' \). Then

\[
K_D(\rho_{AA'}) \geq C_D(\rho_{AE}^{(\text{eq})}), \tag{74}
\]

where \( \rho_{AE}^{(\text{eq})} \) is a cq state derived from purification \( |\overline{\rho}_{AE} \rangle \) of privacy squeezed state \( \overline{\rho}_A = \text{Tr}_{A'}(U_t \rho_{AA} U_t^\dagger) \).

Proof. Denoting by \( |\psi_{AA'E} \rangle \) the purification of \( \rho_{AA} \), we have immediately from Eq. (73) that \( K_D(\rho_{AA'}) \geq C_D(\rho_{AE}^{(\text{eq})}) \) with \( \rho_{AE}^{(\text{eq})} \) standing for a cq state being a result of the measurement of A part in \( B_{N}^{\text{prod}} \) and tracing A’ part of \( |\psi_{AA'E} \rangle \). Then, as already stated, for any twisting \( U_t \) (in \( B_{N}^{\text{prod}} \)) the states \( \rho_{AA} \) and \( \overline{\rho}_{AA} = \text{Tr}_{A'}(U_t \rho_{AA} U_t^\dagger) \) have the same cq states with respect to the basis \( B_{N}^{\text{prod}} \). Consequently, \( C_D(\rho_{AE}^{(\text{eq})}) = C_D(\rho_{AE}^{(\text{eq})}) \) with \( \rho_{AE}^{(\text{eq})} \) being a cq state derived from the twisted state \( U_t \rho_{AA} U_t^\dagger \) (obviously via its purification). Now, we can consider the situation in which the A’ subsystem is given to Eve. This means that instead of taking ‘huge’ purification \( |\psi_{AA'E} \rangle \) of the privacy squeezed state \( \overline{\rho}_A = \text{Tr}_{A'}(U_t \rho_{AA} U_t^\dagger) \) we can take ‘smaller’ version denoted by \( |\overline{\rho}_{AE} \rangle \) (more precisely to purify some density matrix acting on H it suffices to use a Hilbert space of lower dimensionality than to purify a state acting on \( H \otimes H' \)). The new purification obviously must obey \( \overline{\rho}_A = \text{Tr}_{E}(|\overline{\rho}_{AE} \rangle \langle \overline{\rho}_{AE}|) \). Now comparing these two situations we infer that \( C_D(\rho_{AE}^{(\text{eq})}) \geq C_D(\rho_{AE}^{(\text{eq})}) \) holds, where \( \rho_{AE}^{(\text{eq})} \) is cq state appearing upon measurement of A subsystem in \( |\overline{\rho}_{AE} \rangle \) in \( B_{N}^{\text{prod}} \). The inequality is a consequence of the fact that in the case of the first cq state the A’ part unused, however, kept by the parties. In turn, in the second situation the A’ subsystem is treated as it would be given to Eve when deriving \( \rho_{AE}^{(\text{eq})} \). Giving some part of state can only lower the secrecy as in
this case, roughly speaking, she gains some information about what is shared by the parties. This concludes the proof. □

V. CONSTRUCTIONS

In this section we present two constructions of multipartite bound entangled states with nonzero distillable cryptographic key. Both are based on the structure exhibited by the GHZ states and therefore the scheme of secure key distillation presented above easily applies here.

The first construction is a straightforward generalization of the bipartite construction presented in Ref. [13]. Therefore, for comparative purposes, we present also a plot containing a lower bound on distillable key in the bipartite case. The second construction is completely new and in comparison to the first one allows to get a higher lower bounds on distillable key than the first one.

Before we start it is desirable to establish the notation that we will use extensively below. By $\mathcal{P}^{(N)}_0$ we shall denote a projector onto the $N$–partite pure state $|\psi_0^{(N)}\rangle = |0\rangle^\otimes N$ and $\mathcal{P}^{(N)}_i$ (for $i = 1, \ldots, N$) is a projector onto the $N$–partite state $|\psi_i^{(N)}\rangle$, in which the $i$th party possesses $|1\rangle$, while other parties are in the $|0\rangle$ state. For instance $\mathcal{P}^{(4)}_2$ projects onto the four–partite pure state $|\psi_2^{(4)}\rangle = |0100\rangle$. Moreover, let $\overline{\mathcal{P}}^{(N)}_0$ and $\overline{\mathcal{P}}^{(N)}_i$ denote projectors obtained from $\mathcal{P}^{(N)}_0$ and $\mathcal{P}^{(N)}_i$, respectively, by exchanging all zeros and ones. Thus, for example $\overline{\mathcal{P}}^{(4)}_2$ is the projector onto $|\overline{\psi}_2^{(4)}\rangle = |1011\rangle$. We will denote in an analogous way by $|\overline{\psi}_{ij}^{(N)}\rangle$ (or $|\overline{\psi}_{ij}^{(N)}\rangle$) a $N$–qubit pure state, in which $i$th and $j$th qubits are in the $|1\rangle$ ($|0\rangle$) state and the remaining ones are in the $|0\rangle$ ($|1\rangle$) state. Then by $\overline{\mathcal{P}}^{(N)}_{ij}$ and $\overline{\mathcal{P}}^{(N)}_{ij}$ we denote projectors onto $|\overline{\psi}_{ij}^{(N)}\rangle$ and $|\overline{\psi}_{ij}^{(N)}\rangle$, respectively.

Let also $T_i$ denote the partial transposition with respect to $i$th party (with the exception that $T_0$ denotes the identity map). Here we usually assume that each party has two subsystems of a given state $\rho_{AA'}$ and sometimes $T_i$ will be denoting the partial transposition with respect to one or both subsystems. It will be, however, clear from the context which of the subsystems are partially transposed. Concatenation of partial transpositions with respect to some subset of parties, say $A_1, \ldots, A_k$ will be denoted by $T_{A_1 \ldots A_k}$.

A. The first construction

Here we assume that the key part on each site is of qubit structure, while the shield part has arbitrary dimension, however, with the same dimension on each site. More precisely, we have $\mathcal{H}_i = \mathbb{C}^2$ and $\mathcal{H}_i' = \mathbb{C}^D$ (for $i = 1, \ldots, N$).

Now, let us introduce the following matrix

$$X^{(N)}_D = \frac{1}{D^N + 2D - 4} \left[ (D - 2)P_{D,N}^{(+) - 2P_D^{(N)} + Q_D^{(N)}} \right],$$

(75)

where, as previously, $P_{D,N}^{(+)\, (N)}$ denotes a projector onto the $N$–partite $D$–dimensional GHZ state (see Eq. (10)), and $P_D^{(N)}$ and $Q_D^{(N)}$ are projectors defined as

$$P_D^{(N)} = R_D^{(N)} - P_D^{(+)\, (N)}, \quad Q_D^{(N)} = 1_{D^N} - R_D^{(N)},$$

(76)

where

$$R_D^{(N)} = \sum_{i=0}^{D-1} |i\rangle\langle i|^\otimes N.$$

(77)

The projectors $P_D^{(N)}$ and $Q_D^{(N)}$ are chosen in such a way that each operator from the triple $P_D^{(+)\, (N)}, P_D^{(N)}$, and $Q_D^{(N)}$ is defined on orthogonal support. Furthermore, the denominator in Eq. (75) is chosen such that the matrix $X^{(N)}_D$ is normalized in the trace norm.

The states under consideration are of the form

$$\theta_{AA'}^{(D,N)} = \frac{1}{\mathcal{N}^{(N)}_D} \left[ \sum_{i=0}^{N} \left( \mathcal{P}^{(N)}_i \mathcal{P}^{(N)}_i \right) \otimes \left( |X^{(N)}_{D,T_i}^{(N)}\rangle \langle X^{(N)}_{D,T_i}^{(N)}| \right)_{A'} \right.$$

$$\left. + \left( |0\rangle\langle 0|^\otimes N + |1\rangle\langle 1|^\otimes N \right) \otimes \left( |X^{(N)}_D|^{(N)} \right)_{A'} \right],$$

(78)

where the subscripts $A$ and $A'$ are indicated to distinguish their key and shield parts, respectively. However, for the sake of clarity, in further considerations these subscripts will be omitted.

The normalization factor $\mathcal{N}^{(N)}_D$ appearing in Eq. (78) is given by

$$\mathcal{N}^{(N)}_D = 2^{N(N+1)D(N+1) + 2D - 4}. \quad \frac{D^N}{D^N + 2D - 4}.$$

(79)

At the beginning we need to show that the matrices $\theta^{(D,N)}_{AA'}$ really represent quantum states, i.e., they are positive (the normalization condition is already satisfied). Firstly, let us notice that the blocks corresponding to $\mathcal{P}_0$ and $\overline{\mathcal{P}}_0$ and the two off–diagonal blocks in Eq. (78) constitute a matrix of the form $\mathcal{M}_{12}(|X^{(N)}_{D,T_i}^{(N)}\rangle, |X^{(N)}_{D,T_i}^{(N)}\rangle)$ (see Lemma A.1 for the definition of $\mathcal{M}_{12}$), positivity of which is guaranteed by Lemma A.1. Thus the only thing we need to deal with is to show that the remaining blocks lying on the diagonal of $\theta^{(D,N)}_{AA'}$ are positive. To achieve this goal, below we prove a more general lemma.

Lemma V.1. Let $X^{(N)}_{D,T_i}$ be defined by Eq. (75). Then the matrices $|X^{(N)}_{D,T_i}\rangle \langle X^{(N)}_{D,T_i}|$ are positive semi–define for all $k, l = 1, \ldots, N$.

Proof. Noticing that $R_D^{(N)}$ is diagonal for arbitrary $D$ and $N$, the partial transposition of $X^{(N)}_{D,T_i}$ with respect to the $k$–th subsystem may be written as $X^{(N)}_{D,T_k}$
As we will see below, the absolute value of the sign before the projector $R_D^{(N)}$ may be obtained by simple changing the sign before the projector $R_D^{(N)}$. To prove positivity of $S_D^{(N)T_k}$ let $|\psi\rangle = \sum_{i_1,\ldots,i_N} \alpha_{i_1\ldots i_N} |i_1\ldots i_N\rangle$ denote an arbitrary vector from $(\mathbb{C}^D)^\otimes N$ written in the standard basis of $(\mathbb{C}^D)^\otimes N$. Then we have

$$\langle \psi | S_D^{(N)T_k} | \psi \rangle = \sum_{i\neq j} \alpha_{i\ldots j\ldots i}^* \alpha_{i\ldots j\ldots i} + \sum_{(i_1,\ldots,i_N) \in I_k} |\alpha_{i_1\ldots i_N}|^2 \geq 0.$$  

Here the notation $\alpha_{i\ldots j\ldots i}$ means that all indices of $\alpha$ excluding the $k$-th one ($k$ stands for the number of subsystem being partially transposed) are equal. Moreover, as previously $I$ denotes the set of all sequences $(i_1,\ldots,i_N)$ except the cases when $i_1 = \ldots = i_N$, while $I_k$ is the set $I$ minus all sequences in which all indices but the one on $k$-th position are equal.

As the value of $k$ is not specified, the above considerations holds for any $k=1,\ldots,N$. Furthermore, using the same reasoning one can also prove positivity of $S_D^{(N)}$ being transposed with respect to any subset of different subsystems (besides the full transposition). This fact will be utilized below.

By virtue of the positivity of $S_D^{(N)T_k}$ we have that $|X_D^{(N)T_k}| = [1/(D^N + 2D - 4)](S_D^{(N)T_k} + R_D^{(N)})$ for any $k=1,\ldots,N$. Therefore the partial transposition of the latter with respect to the $l$-th subsystem gives

$$|X_D^{(N)T_k}|^{T_l} = \frac{1}{D^N + 2D - 4} (S_D^{(N)T_{k,l}} + R_D^{(N)}).$$

where $T_{k,l}$ denotes the partial transposition with respect to two single subsystems $A_k$ and $A_l$. Now we can distinguish two cases, namely, if $k = l$ and $k \neq l$. In the first one, double partial transpositions with respect to the same subsystem is just an identity map. Consequently from Eqs. (76), (77), and (80), one has

$$|X_D^{(N)T_k}|^{T_k} = \frac{1}{D^N + 2D - 4} (Q_D^{(N)} + D P_{D,N}^{(+)}).$$

Now the right-hand side of Eq. (83) is a linear combination of two positive operators and thus is positive. We have still left the second case, that is, when $k \neq l$. To resolve it we may use the remark made above, saying that the partial transposition of $S_D^{(N)}$ with respect to arbitrary non only one–partite subsystem is a positive matrix. This ends the proof.

Thus we have just proven that $\theta_{AA'}^{(D,N)}$ indeed represent quantum states. Now, our aim is to prove that on the one hand they are bound entangled and on the other hand they have nonzero distillable key. This purpose will be achieved in two steps. Firstly we show that partial transposition with respect to any elementary subsystem $(A_iA'_j)$ of $\theta_{AA'}^{(D,N)}$ is positive. Obviously, this does not confirm that the states are bound entangled since we do not even know they are entangled. However, the latter may be proven by showing that $K_D$ of these states is nonzero for $D \geq 3$.

Firstly, we concentrate on the positivity of all partial transpositions of $\theta_{AA'}^{(D,N)}$. To gain a better look on the problem let us consider a particular example of such a partial transposition, namely, $\theta_{AA'}^{(D,3)T_3}$. From Eq. (78) it follows that
As, due to Lemma A.1, the square matrix consisting of two diagonal and two off-diagonal blocks of $\varphi_{AA'}^{(D,N)}$, (cf. Eq. (51)) i.e., the matrix $M_2([X^{(N)T_i}_D, X^{(N)T_j}_D])$, is already positive, we need to prove positivity of $|X^{(N)T_i}_D|$ and $X^{(N)T_i}_D |T_j,k$ for any $i, j, k = 1, \ldots, N$. Let us therefore prove the following lemma.

Lemma V.2. Let $X^{(N)}_D$ be given by Eq. (72). Then for any $i, j, k = 1, \ldots, N$ it holds that

$$|X^{(N)T_i}_D| \geq 0, \quad |X^{(N)T_j}_D |T_j,k \geq 0. \quad (85)$$

Proof. Due to the definition of $X^{(N)}_D$ its absolute value may be calculated simply by changing a sign before $P^{(N)}_D$, giving

$$|X^{(N)}_D| = \frac{1}{D^N + 2D - 4} \left[ (D - 2)P^{(N)}_D + 2P^{(N)}_D + Q^{(N)}_D \right]. \quad (86)$$

Application of partial transposition with respect to the ith subsystem followed by substitution of Eq. (72) leads us to

$$|X^{(N)T_i}_D| = \frac{1}{D^N + 2D - 4} \left[ 1D + R^{(N)}_D + (D - 4)P^{(N)T_i}_D \right] \quad (87)$$

for any $i = 1, \ldots, N$. One may easily check that eigenvalues of $P^{(N)T_i}_D$ belong to the interval $[-1/D, 1/D]$ and therefore the matrix $1D + (D - 4)P^{(N)T_i}_D$ is always positive. This, together with the fact that $R^{(N)}_D \geq 0$, implies positivity of $|X^{(N)T_i}_D|$ for any $i = 1, \ldots, N$.

The second fact of the lemma may be proven just by noting that by virtue of Eq. (52) it holds

$$|X^{(N)T_j}_D |T_j,k = \frac{1}{D^N + 2D - 4} \left( S^{(N)T_j,k}_D + R^{(N)}_D \right). \quad (88)$$

As stated previously in the proof of Lemma V.1, the partial transposition of $S^{(N)}_D$ with respect to arbitrary subsystems is positive. This concludes the proof.

The above lemma proves actually that all the partial transpositions $\varphi_{AA'}^{(D,N)T_i}$ (i = 1, ..., N) are positive. Therefore, the states $\varphi_{AA'}^{(D,N)}$ are bound entangled, of course provided that they are entangled. This is because, due to the result of Ref. [11], positive partial transpositions with respect to any elementary subsystem makes it impossible to distill $k$-partite $(k = 2, \ldots, N)$ GHZ entanglement among any group of parties.

Let us now pass to the proof that any state $\varphi_{AA'}^{(D,N)}$ for $D \geq 3$ has nonzero $K_D$. For this purpose we show that using the protocol from Section IV C we can produce a state that is closer to some multipartite private state out of copies of $\varphi_{AA'}^{(D,N)}$. As we will show below we need to use as many copies as it is necessary to make the quantity appearing on the right-hand side of Eq. (92) strictly positive.

Application of the recursive LOCC protocol presented in Section IV C to $k$ copies of $\varphi_{AA'}^{(D,N)}$ gives with probability $p^{(k)}_{D,N} = 2^{k-1}N^{(k)}_{D,N}/\left(N^{(D)}_D\right)^k$ the following state

$$\Theta^{(N,k)}_{AA'} = \frac{1}{N^{(k)}_{D,N}} \sum_{i=0}^{N} (P^{(N)}_i + \overline{P}^{(N)}_i) \otimes \left( X^{(N)T_i}_D \otimes k \right) + \left( \langle 0| \otimes N + |1| \otimes N \otimes N \right) \otimes \left( X^{(N)}_D \otimes k \right), \quad (89)$$

where $N^{(k)}_{D,N}$ is a normalization factor given by

$$N^{(k)}_{D,N} = 2 \left[ 1 + N \left( \frac{D_N}{D_N + 2D - 4} \right)^k \right]. \quad (90)$$

Now, to simplify the considerations we can utilize the privacy squeezing (see Section IV D) to the obtained states $\Theta^{(N,k)}_{AA'}$. Namely, due to Lemma III.1 there exist such twistings $U_i^{(k)}$ that after application to $\Theta^{(N,k)}_{AA'}$ and tracing out the A subsystem one arrives at the following class of N-qubit states

$$\tilde{\Theta}^{(N,k)}_{AA'} = \frac{1}{N^{(k)}_{D,N}} \sum_{i=0}^{N} (P^{(N)}_i + \overline{P}^{(N)}_i) \left\| X^{(N)T_i}_D \otimes k \right\|_1 + \left( |0| \otimes N + |1| \otimes N \right) \left\| X^{(N)}_D \otimes k \right\|_1. \quad (91)$$

In other words, after ‘rotation’ with $U_i^{(k)}$ and throwing out the A subsystem we get a so-called privacy squeezed state, i.e., the one in which blocks are replaced with their norms. We also know from Theorem IV D that the distillable key of the cq state obtained from the privacy squeezed state $\tilde{\Theta}^{(N,k)}_{A}$ (measurement is performed in the same basis as twisting) cannot be greater than the distillable key of $\Theta^{(N,k)}_{AA'}$.

From Eq. (92) it follows that since $D^N + 2D - 4 > D^N$ for any $D \geq 3$ one has $N^{(k)}_{D,N} \rightarrow 2$, while for $D = 2$, $N^{(k)}_{2,N} \rightarrow 2(N + 1)$. In turn this means that for the off-diagonal elements of $\tilde{\Theta}^{(N,k)}_{A}$ one has that

$$\frac{1}{N^{(k)}_{D,N}} \left\| X^{(N)}_D \otimes k \right\|_1 = \frac{1}{N^{(k)}_{D,N}} \frac{k-\infty}{2} \quad (92)$$

with $D \geq 3$. By virtue of Theorem III.3 one infers that the more copies of $\varphi_{AA'}^{(D,N)}$ we put into the recurrence protocol, the closer we are to some multipartite private state. This also means that with $k \rightarrow \infty$ the sequence of states $\tilde{\Theta}^{(N,k)}_{A}$ goes to GHZ state $P^{(N)}_D$, however, for $D \geq 3$.

Now, to bound from below the distillable key of $\Theta^{(N,k)}_{AA'}$ according to the prescription given above we need to calculate a cq state of the privacy squeezed state $\tilde{\Theta}^{(N,k)}_{A}$. (The cq state is found here with respect to the basis in
which the original state is defined.) Simple algebra gives
\[
\Theta_{AE}^{(cq)} = \frac{1}{N_{D,N}^{(k)}} \left[ P_2^{(N)} \otimes |E_0\rangle\langle E_0| + \left( \frac{D^N}{D^N + 2D - 4} \right)^k \right.
\]
\[
\left. \sum_{j=1}^{N} \left( P_j^{(N)} \otimes |E_j\rangle\langle E_j| + \mathcal{T}_j^{(N)} \otimes |D_j\rangle\langle D_j| \right) \right],
\]
(93)

where \(|E_0\rangle\), \(|E_j\rangle\), and \(|D_j\rangle\) constitute a set of orthonormal states held by Eve. One notices immediately that \(\Theta_{AE}^{(cq)}\) tends to the multipartite ideal cq state (see Eq. (2)) for any integer \(D \geq 3\) whenever \(k \to \infty\).

To find a lower bound on distillable key of \(\Theta_{A}^{(N,k)}\) we utilize Eq. (68). However, according to Eq. (68) one needs to calculate the quantities \(I(A_i : A_j)\) for \(i \neq j\) and \(I(A_i : E)\) for the respective reductions of \(\Theta_{AE}^{(cq)}\). Fortunately, the initial states \(\theta_{AA'}^{(D,N)}\) have such symmetrical structure, preserved by the recurrence protocol and the privacy squeezing, that makes all the quantities \(I(A_i : A_j)\) \((i \neq j)\) equal (the same holds for \(I(A_i : E)\)). Consequently, in view of the above, using Eq. (68) and Theorem IV.4 (see Eq. (74)), we infer the following inequality
\[
K_D(\Theta_{AA'}^{(N,k)}) \geq I(A_1 : A_2)(\Theta_{AA'}^{(cq)})_1 - I(A_1 : E)(\Theta_{AA'}^{(cq)})_E.
\]
irrespectively of number of parties \(N\). Exemplary behaviour of the right–hand side of Eq. (94) (denoted by \(K_{DW}\)) in the function of \(k\) and \(D\) for \(N = 3\) is shown in Fig. 1a. It is clear from Figure 1a that it is possible to distill one secure bit of key from bound entangled states \(\Theta_{AA'}^{(N,k)}\) for sufficiently large \(k\). For comparison, Fig. 1b contains a lower bound of the distillable key in the case of \(N = 2\) discussed in Ref. [15].

We can also investigate the lower bound on \(K_D\) for the initial states \(\theta_{AA'}^{(D,N)}\). However, in this case we need to take into account the probability \(P_{D,N}^{(k)}\). In this way we arrive at
\[
K_D(\theta_{AA'}^{(D,N)}) \geq P_{D,N}^{(k)} \left[ I(A_1 : A_2)(\Theta_{AA'}^{(cq)})_1 - I(A_1 : E)(\Theta_{AA'}^{(cq)})_E \right].
\]
(95)

Figure 2 presents exemplary behaviour of the function appearing on the right–hand side of Eq. (95) (denoted by \(K_{DW}\)) for \(N = 3\). For comparison, in Figure 2 it is also plotted the same function in the case of \(N = 2\) (this case was discussed in Ref. [27]).

Let us conclude the first construction with discussion of some of its general properties. Above we used a particular class of matrices \(X_D^{(N)}\) (defined in Eq. (75)), however, it seems interesting to ask whether there are other matrices than \(X_D^{(N)}\) that could be used in the construction. In what follows we provide some constraints that the general matrix, hereafter denoted by \(Z_D^{(N)}\), must obey to be useful for purposes of the construction. The first important condition is that the trace norm of \(Z_D^{(N)}\) has to be strictly larger than the trace norm of \(\left|Z_D^{(N)}\right|_{max}^{T_i}\) for all \(i = 1, \ldots, N\). This guarantees convergence (in the trace norm) of the output states of the recursive LOCC protocol (given in Sec. IV.C) to some multipartite private states. Another crucial conditions are \(\left|Z_D^{(N)}\right|_{max}^{T_i} \geq 0\) and \(\left|Z_D^{(N)}\right|_{max}^{T_i} \geq 0\) for all \(i = 1, \ldots, N\). The first one is necessary for \(\theta_{AA'}^{(D,N)}\) (when constructed with the matrix \(Z_D^{(N)}\)) to be positive, while the second one allows to prove that \(\theta_{AA'}^{(D,N)}\) have positive partial transposition with respect to any elementary subsystem.

**Lemma V.3.** Assume that \(Z_D^{(N)}\) is arbitrary matrix acting on \(\mathbb{C}^D \otimes \mathbb{C}^N\) and that the following conditions

\[
(i) \quad \left| Z_D^{(N)} \right|_{max}^{T_i} > \left| Z_D^{(N)} \right|_{max}^{T_i} \quad \text{for all } i = 1, \ldots, N,
\]

FIG. 1: An exemplary plot of \(K_{DW} \equiv I(A_1 : A_2)(\Theta_{A_1 A_2 E}^{(cq)}) - I(A_1 : E)(\Theta_{A_1 A_2 E}^{(cq)})\) with \(N = 3\) (a) and for comparison in the case of \(N = 2\) (b), which was discussed in Ref. [27]. For the sake of clarity, zero is put whenever the plotted function is less than zero. Notice also that even though \(k\) and \(D\) are discrete parameters, the graph is made as if \(K_{DW}\) were a function of continuous parameters. It follows from both the figures that the number of parties \(N\) significantly influences the obtained lower bound. Namely, for \(N = 3\) one needs to spend more copies of a given state to get nonzero values of \(K_{DW}\).
(iii) Finally, assume that $Z_D^{(N)} \geq 0$ and that there exists such $k$ that $Z_D^{(N)T_k} \geq 0$. Then $\left\| Z_D^{(N)T_k} \right\|_1 = \left\| Z_D^{(N)} \right\|_1$. This contradicts the first assumption. \[ \blacksquare \]

This lemma says that a matrix can be used in the above construction if it is not positive and all its elementary partial transpositions are not positive. Thus, in particular, a general density matrix is not suitable for this construction.

### B. The second construction

The crucial ideas behind the second construction are actually the same as in the case of the first one, however, considerations will be a little bit more sophisticated.

Let us first define the analog of $X_D^{(N)}$ from the first construction to be

$$\tilde{X}_D^{(N)} = \sum_{i,j=0}^{D-1} u_{ij} |i\rangle\langle j|^{\otimes N}, \quad (96)$$

where we assume that $u_{ij}$ are elements of some $D \times D$ general unitary or unitary Hermitian matrix, hereafter denoted by $U_D$. Thus $\tilde{X}_D^{(N)}$ is an embedding of $U_D \in M_D(\mathbb{C})$ ($M_D(\mathbb{C})$ denotes the set of $D \times D$ matrices with complex entries) in $M_{DN}(\mathbb{C})$ and therefore

$$\left\| \tilde{X}_D^{(N)} \right\| = R_D^{(N)}. \quad (97)$$

For further simplicity we also impose the condition that $|u_{ij}| = 1/\sqrt{D}$ for $i,j = 0, \ldots, D - 1$, however whenever possible all proofs will be given assuming that $U_D$ is a general unitary matrix.

It should be also pointed out that the distinction on unitary or unitary and Hermitian matrices $U_D$ made above plays an important role here. This comes from the LOCC protocol presented in Section [IVC] as in the case of unitary but not Hermitian matrices it needs to be slightly modified. Namely, in its last step all the parties keep the state only if all zeros occurred.

A particular example of a unitary but in general not Hermitian matrix satisfying the above condition is the matrix $\tilde{V}_D = (1/\sqrt{D})V_D$, where $V_D$ denotes the Vandermonde matrix of solutions to the equation $z^D - 1 = 0$ with $z \in \mathbb{C}$. As one knows the solutions are of the form $\omega_k = e^{2\pi ik/D}$ ($k = 0, \ldots, D - 1$). It is then clear that $\tilde{V}_D$ is a unitary matrix for any $D \geq 2$, however not always a Hermitian one. For instance, in the particular case of $D = 2$ one easily recognizes that $\tilde{V}_2$ is the known Hadamard matrix. A good example of some unitary and Hermitian matrix is $k$th tensor power of $\tilde{V}_2$. Since $\tilde{V}_2$ is unitary and Hermitian any matrix of the form $\tilde{V}_2^{\otimes k}$ is also unitary and Hermitian.
Now, let us consider following family of matrices

\[ \tilde{\varrho}^{(D,N)}_{D,N} = \frac{1}{N_D^{(N)}} \left[ N \sum_{j=0}^{N} \left( \tilde{\varrho}^{(N)}_{D,j} + \tilde{\varrho}^{(N)}_{D,j} \right) \otimes \sum_{i=1}^{N} \tilde{X}^{(N)}_{D,i} \right] + |0\rangle |0\rangle \otimes \sum_{i=1}^{N} \tilde{X}^{(N)}_{D,i} + |1\rangle |0\rangle \otimes \sum_{i=1}^{N} \tilde{X}^{(N)}_{D,i}, \tag{98} \]

where \( N_D^{(N)} \) stands for the normalization factor, which for arbitrary unitary \( U_D \) is given by

\[ N_D^{(N)} = 2N \left( D + N \sum_{i,j=0}^{D-1} |u_{ij}| \right). \tag{99} \]

Obviously for \( \tilde{X}^{(N)}_D \) that comes from unitary Hermitian \( U_D \) the conjugation in the last term in Eq. (98) may be omitted. Moreover, taking into account the assumption that \( |u_{ij}| = 1/\sqrt{D} \), the normalization factor becomes

\[ N_D^{(N)} = 2N D \left( 1 + N \sqrt{D} \right). \]

As in the case of the first construction, we need to prove that \( \tilde{\varrho}^{(D,N)}_{D,N} \) represent quantum states. Moreover, we show also that they have positive partial transpositions with respect to any elementary subsystem. From Eq. (98) it follows that to prove positivity of \( \tilde{\varrho}^{(D,N)}_{D,N} \) one has to show that the inequalities

\[ \sum_{i=1}^{N} \tilde{X}^{(N)}_{D,i} \leq \sum_{i=1}^{N} \tilde{X}^{(N)}_{D,i} \tag{100} \]

are satisfied. Then simply utilizing Lemma A.1 and noting that the remaining blocks lying on the diagonal of \( \tilde{\varrho}^{(D,N)}_{D,N} \) are positive by definition, the positivity of \( \tilde{\varrho}^{(D,N)}_{D,N} \) is proved.

To deal with the problem of positivity of partial transpositions let us look on the particular example of form of \( \tilde{\varrho}^{(D,3)}_{D,3} \). From Eq. (98) one infers that

\[
\begin{bmatrix}
\sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \sum_{i=1}^{3} \left| \tilde{X}^{(3)}_{D,i} \right|^2 \\
\end{bmatrix}
\]

where we used the fact that \( \left| \tilde{X}^{(n)T}_{D,i} \right| \) are diagonal in the standard basis and therefore are not affected by partial transposition with respect to any subsystems.

To show positivity of \( \tilde{\varrho}^{(D,N)}_{D,N} \) as well as its partial transpositions we prove the following lemma.

**Lemma V.4.** Let \( \tilde{X}^{(N)}_D \) be defined as in Eq. (98). Then the following equalities holds

\[ \sum_{i=1}^{N} \tilde{X}^{(N)T}_{D,i} = \sum_{i=1}^{N} \tilde{X}^{(N)T}_{D,i}, \quad (j = 0, \ldots, N). \tag{102} \]

**Proof.** Firstly we start by the above statement for \( j = 0 \). For this purpose let us notice that its left–hand side may
where we utilized Eq. \((102)\). One notices that the above inequality may be further reduced to

\[ |U_D + (N - 1)| \leq 1 + (N - 1)/\sqrt{D}, \tag{107} \]

To prove this inequality we can utilize the polar decomposition to its left-hand side. More precisely we can write

\[ |U + (N - 1)| = V^\dagger U + (N - 1)V^\dagger D \]

with some unitary matrix. This allows us to write

\[ \langle \Psi | U + (N - 1) | \Psi \rangle = |\langle \Psi | U + (N - 1) | D \rangle| \]

\[ + (N - 1) |\langle \Psi | V^\dagger D \rangle| \]

\[ \leq 1 + (N - 1) |\langle \Psi | V^\dagger D \rangle| \]

\[ \leq 1 + (N - 1) \sqrt{D}. \tag{108} \]

where $|\Psi\rangle$ is an arbitrary normalized vector from $\mathbb{C}^D$. The second and third inequality are consequences of the fact that the product of unitary matrices is a unitary matrix and that for any normalized $|\psi\rangle$ and unitary $U$

it holds that $|\langle \psi | U | \psi \rangle| \leq 1$. Moreover, we put here the polar decomposition of $D$, i.e., $D = |D| W$ with some unitary $W$. The last inequality is also a result of application of aforementioned fact that $|D| = (1/\sqrt{D}) I_D$.

Now, to finish the proof, it suffices to mention that the resulting inequality is equivalent to \((107)\).

From the above lemma it clearly follows that $\vartheta_{AA'}^{(D)}$ represent quantum states for any $D \geq 2$ and $N \geq 2$, and they have positive partial transpositions with respect to all elementary subsystems. The last thing we need to prove is that the distillable key of $\vartheta_{AA'}^{(D)}$ is nonzero. This would also imply that $\vartheta_{AA'}^{(D)}$ represent entangled states.

Let us then apply the recursive protocol described previously in Section IV.C to $k$ copies of $\vartheta_{AA'}^{(D)}$, obtaining

\[ \vartheta_{AA'}^{(D,k)} = \frac{1}{N^\dagger k} \sum_{j=0}^{N} \left( P_j^{(N)} + \varphi_j^{(N)} \right) \otimes \left( \sum_{i=1}^{N} |\tilde{X}_{D,i}\rangle \right)^{\otimes k} \]

\[ + |0\rangle^\otimes N \otimes \left( \sum_{i=1}^{N} |\tilde{X}_{D,i}\rangle \right)^{\otimes k} \]

\[ + |1\rangle^\otimes N \otimes \left( \sum_{i=1}^{N} |\tilde{X}_{D,i}\rangle \right)^{\otimes k}, \tag{109} \]

with the normalization factor given by

\[ \mathcal{N}_{D,N}^{(k)} = 2 \left( N D \sqrt{k} \right) + 2 N D^k \left[ 1 + (N - 1) \sqrt{k} \right]. \tag{110} \]

Notice that as previously mentioned, the LOCC protocol should be modified in case when $\tilde{X}_{D,N}^{(N)}$ follows from in general unitary $U_D$. Due to the modification of the LOCC protocol, the probability of obtaining $\vartheta_{AA'}^{(N,k)}$ in the case of unitary and unitary Hermitian $U_D$ is different. Namely, in the case of unitary Hermitian matrices amounts to

\[ p_{D,N}^{(k,1)} = 2^{k-1} \tilde{X}_{D,N}^{(N)} / \left( \tilde{X}_{D,N}^{(N)} \right)^k, \tag{111} \]

while in the case of unitary non Hermitian the probability of success is considerably smaller and is given by

\[ p_{D,N}^{(k,2)} = \tilde{X}_{D,N}^{(N)} / \left( \tilde{X}_{D,N}^{(N)} \right)^k. \tag{112} \]

Now the multipartite privacy squeezing (see Section IV.D) allows us to change blocks in Eq. \((109)\) with their norms, obtaining

\[ \bar{\vartheta}_{A}^{(N,k)} = \frac{1}{\mathcal{N}_{D,N}^{(k)}} \left[ \sum_{j=0}^{N} \left( P_j^{(N)} + \varphi_j^{(N)} \right) \sum_{i=1}^{N} |\tilde{X}_{D,i}\rangle \right]^{k} \]

\[ + \left( |0\rangle^\otimes N + |1\rangle^\otimes N \right) \sum_{i=1}^{N} |\tilde{X}_{D,i}\rangle \right]^{k}. \tag{113} \]
Calculating the respective norms in the above, one may rewrite Eq. (113) as

\[
\tilde{\varrho}_A^{(N,k)} = \frac{D^k}{N_{D,N}^{(k)}} \left[ 2(N\sqrt{D})^k P_{2,N}^{(+)} + |1 + (N-1)\sqrt{D}|^k \sum_{j=1}^N \left(P_j^{(N)} + \bar{P}_j^{(N)}\right) \right] .
\]

(114)

From Eqs. (110) and (114) one easily infers that \( \tilde{\varrho}_A^{(N,k)} \rightarrow P_{2,N}^{(+)} \) for \( k \rightarrow \infty \) for any \( D \geq 2 \), which by virtue of Theorem III.3 means that the recursive protocol when applied to copies of \( \tilde{\varrho}_{AA'}^{(D,N)} \) produces a state that is arbitrarily close to some multipartite pdit in the limit of \( k \rightarrow \infty \). In fact, as the probabilities of success \( \tilde{P}_{D,N}^{(k,1)} \) and \( \tilde{P}_{D,N}^{(k,2)} \) (see Eqs. (111) and (112)) are positive, according to the definition of \( K_D \) (see Definition IV.1) the above method leads to distillation of secure key from \( \tilde{\varrho}_{AA'}^{(D,N)} \). Below we provide also plots of lower bounds on \( K_D \) of \( \tilde{\varrho}_{AA'}^{(D,N)} \).

For this purpose we can find the purification of \( \tilde{\varrho}_{AA'}^{(D,N)} \) and then the cq state in the standard basis. The latter has the form

\[
\tilde{\varrho}_{AE}^{(cq)} = a_{D,N}^{(k)} R_2^{(N)} \otimes |E_0\rangle\langle E_0| + b_{D,N}^{(k)}
\]

\[
\times \sum_{j=1}^N \left( P_j^{(N)} \otimes |E_j\rangle\langle E_j| + \bar{P}_j^{(N)} \otimes |E_j\rangle\langle E_j| \right) ,
\]

(115)

where \( |E_0\rangle, |E_j\rangle \), and \( |E_j\rangle \) (\( j = 1, \ldots, N \)) are orthonormal states kept by Eve, and coefficients \( a_{D,N}^{(k)} \) and \( b_{D,N}^{(k)} \) are given by

\[
a_{D,N}^{(k)} = \frac{D^k}{N_{D,N}^{(k)}} \]

and

\[
b_{D,N}^{(k)} = \frac{D^k}{N_{D,N}^{(k)}} - [1 + (N-1)\sqrt{D}]^k .
\]

(116)

(117)

One can see from the above that the limit of \( k \rightarrow \infty \) leads us to the ideal cq state. Now we can apply the bound given in Eq. (65). It is easy to verify that all the quantities \( I(A_1 : A_2) \) are equal here (the same holds for \( I(A_1 : E) \)) and therefore we can rewrite Eq. (69) as

\[
K_D(\tilde{\varrho}_{AA'}^{(N,k)}) \geq I(A_1 : A_2)(\tilde{\varrho}_{AA_1A_2E}^{(cq)}) - I(A_1 : E)(\tilde{\varrho}_{A_1A_2E}^{(cq)})
\]

(118)

Exemplary plot of the function appearing on the right–hand side of Eq. (118) (denoted here by \( K_D(\tilde{\varrho}_{AA'}^{(N,k)}) \)) is presented in Figure 3. The behavior of \( K_D \) (see Fig. 3) confirms the previous analysis, namely, the more copies we spend the closer the state is to some multipartite private state we obtain using the recursive protocol. Thus the higher key rate we can get from the obtained state \( \tilde{\varrho}_{AA'}^{(N,k)} \).

We can also get a lower bound on distillable key of the initial states \( \tilde{\varrho}_{AA'}^{(D,N)} \). Here we need to take into account the probability of success \( \tilde{P}_{D,N}^{(k,1)} \) and \( \tilde{P}_{D,N}^{(k,2)} \) in the recursive protocol.

The corresponding bounds on the distillable keys of \( \tilde{\varrho}_{AA'}^{(D,N)} \) are

\[
K_D^{(1)}(\tilde{\varrho}_{AA'}^{(D,N)}) \geq \tilde{P}_{D,N}^{(k,1)} \left[ I(A_1 : A_2)(\tilde{\varrho}_{A_1A_2E}^{(cq)}) - I(A_1 : E)(\tilde{\varrho}_{A_1A_2E}^{(cq)}) \right] .
\]

(119)

Exemplary plots of the right–hand side of the above (denoted by \( K_D^{(1)}(\tilde{\varrho}_{AA'}^{(D,N)}) \)) both in the case of a unitary Hermitian matrix (e.g. \( \tilde{V}_{D}^{(k)} \)) and only a unitary matrix (e.g. \( \tilde{V}_{D} \)) are given in Figure 3a and 3b.

VI. REMARKS ON LIMITATIONS IN MULTIPARTITE QUANTUM CRYPTOGRAPHY

So far, we discussed the general scheme allowing for distilling secure key from multipartite states. It is desirable however to discuss also what are the limitations of multipartite secure key distillation.

An interesting effect, which we shall recall here, was reported in Ref. 33, namely, it was shown that though maximal violation of some Bell inequality it is impossible to distill secure key from the so–called Smolin state 34:

\[
\psi^S = \frac{1}{4} \sum_{i=0}^{3} |\psi_i^B\rangle |\psi_i^B\rangle \otimes |\psi_i^B\rangle\langle \psi_i^B| ,
\]

(120)

where \( |\psi_i^B\rangle \) (\( i = 0, \ldots, 3 \)) are the so–called Bell states given by \( |\psi_i^B\rangle = (1/\sqrt{2}) (|01\rangle \pm |10\rangle) \) and \( |\psi_2^B\rangle = \ldots \).
in the case of unitary but not Hermitian matrix \( K_{DW} \) plotted in Figure 4. One infers that in the case of unitary but not Hermitian matrix \( U_D \) the region of non-zero values of the plotted function is wider than in the case of unitary Hermitian matrices.

\[
(1/\sqrt{2}) (|00\rangle \pm |11\rangle)
\]

This conclusion may be also inferred for the generalizations of the Smolin state provided in Ref. [37] and independently in Ref. [36] (see also Ref. [38]) for further generalizations. These are states of the form

\[
\varphi_{2} = |\psi_{0}^{B}\rangle|\psi_{0}^{A}\rangle,
\]

\[
\varphi_{4}^{S} = \frac{1}{4} \sum_{m=0}^{3} U_{2}^{(m)} \varphi_{2} U_{2}^{(m)} \otimes U_{2}^{(m)} \varphi_{2} U_{2}^{(m)} = \varphi_{S},
\]

\[
\varphi_{0}^{S} = \frac{1}{4} \sum_{m=0}^{3} U_{2}^{(m)} \varphi_{4} U_{2}^{(m)} \otimes U_{2}^{(m)} \varphi_{2} U_{2}^{(m)}
\]

\[
\vdots
\]

\[
\varphi_{2(n+1)}^{S} = \frac{1}{4} \sum_{m=0}^{3} U_{2}^{(m)} \varphi_{2n} U_{2}^{(m)} \otimes U_{2}^{(m)} \varphi_{2} U_{2}^{(m)}
\]

(121)

with \( U_{k}^{(m)} = 1 \otimes \sigma_{m} \otimes \sigma_{m} \otimes \sigma_{m} \otimes \sigma_{m} \otimes \sigma_{m} \otimes \sigma_{m} \otimes \sigma_{m} \), where \( \sigma_{m} \) (\( m = 0, 1, 2, 3 \)) denote the usual Pauli matrices and \( \sigma_{0} = 1 \). The state \( \varphi_{2} \) is just one of the Bell states, while \( \varphi_{4}^{S} \) is the Smolin state. All states \( \varphi_{2n} \) for \( n \geq 2 \) are bound entangled and for suitable choice of local observables all states for \( n \geq 1 \) violate the Bell inequality

\[
|E_{1...11} + E_{1...12} + E_{2...21} - E_{2...22}| \leq 2 \quad (122)
\]

maximally (\( E \) denotes the so-called correlation function, i.e., an average of products of local measurement outcomes taken over many runs of experiment). On the other hand, due to the results of Refs. [3, 6], and Ref. [30], one may show that it is impossible to distill multipartite secure key from states \( \varphi_{2n}^{S} \) for \( n \geq 2 \). This shows that multipartite Ekert protocol [2] cannot be straightforwardly generalized to multipartite scenario since as discussed above the maximal violation of most natural multipartite analog of the CHSH–Bell inequality [38] does not imply nonzero secret key rate, whereas maximal violation of CHSH–Bell inequality by two qubits guarantees secrecy. Still, it would be an interesting problem for further research to identify all Bell inequalities that do the job in multipartite case as CHSH–Bell inequality does in the case of two qubits. It should be stressed that some achievements in a similar direction were already obtained in Refs. [39, 40], where it was shown that violation of some Bell inequalities is sufficient condition for security of multipartite secret sharing protocols [41] under an individual attack of some external party.

VII. CONCLUSIONS

Quantum cryptography beyond entanglement distillation is a very young subject. Until recent times it was natural to expect that the latter is impossible. While there were significant developments concerning the bipartite scenario the general formulation for multipartite case was missing. The present paper fills this gap by not only generalizing the scheme, but also by providing new constructions of multipartite bound entangled states which is really nontrivial. However, there are many unsolved questions. First it seems to be true that the unconditional security proof [22] can be extended here at a cost of the number of estimated local observables, but an exact analysis of this issue is needed. Moreover, given a fixed number of parties, it is not known what is the minimal dimension of elementary system of PPT like bound entangled state that allows one-way secure key distillation. Does it increase with number of particles and if so - how the dependence looks like? Are there bound entangled states with multipartite cryptographic key with underlying structure corresponding to other classes of pure states like graph states (see Ref. [12])? One may ask why we have considered only bound entanglement in multipartite scenario. This is when it is necessary to apply the generalized scheme. Otherwise qualitatively (though may be not quantitatively – see subsequent discussion) just pure entanglement distillation is a sufficient tool. Quite natural is a question of interplay between the two approaches in distilling key – to what extent can we abandon distillation of p–dits? Finally, can the two processes always be separated in optimal key distillation scheme: in a sense
that one gets some number of singlet states and some large p–dit which is bound entangled? If it were so, the two parts might serve as a natural measures of free and bound entanglement in the system. Most likely this is impossible, but one needs a proof. The closely related bound entanglement in the system. Most likely this is two parts might serve as a natural measures of free and bound entanglement in multipartite case 45 but naturally emerges from bound entanglement in multipartite case 45. In this context novel upper and lower bounds on $K_D$ are needed (for recent development see Ref. 46). This point is also interesting from the point of view of entanglement as $K_D$ is also an entanglement measure. Further analysis of $K_D$ and finding its multi–coordinate extensions to help in characterization of multipartite entanglement seems to be rich program for future research.

Also, though in the present paper we are concerned with a general problem of two–way distillability of secure key, it is interesting to discuss the problem in the context of one–way schemes. For instance one could ask about bounds on key within such schemes (see e.g. Ref. 23). On the other hand, it would be desirable to discuss the present approach in the context of secure key distillation from continuous variables systems (see e.g. Refs. 47, 48, 49). For instance, it was shown in Ref. 47 that the generalized version of the protocol from Ref. 47 does not allow for secure key distillation from bound entangled states. It seems that within the multipartite scenario the problem could be simpler a little as one can have bound entangled multipartite states with some of its partitions being still NPT.

Needless to say due to Choi–Jamiołkowski isomorphism 51 the present analysis provides new classes of multiparty quantum channels for which natural questions on superactivation of the type found in bipartite case 20 and other possible effects of similar type arise.

### Acknowledgments

This work was supported by UE IP project SCALA. Partial support from LFPPI network is also acknowledged. R.A. gratefully acknowledges the support from Ingenio 2010 QOIT and Foundation for Polish Science.
taking into account the fact that $|\sum_i \xi_i| \leq \sum_i |\xi_i|$, we obtain

$$\langle \Psi | M_N(A, B) | \Psi \rangle \geq \sum_k |\lambda_k| \left( \sum_{i=1}^N a_{ik}^2 - 2 \sum_{i<j}^N a_{ik} a_{jk} \right).$$

(A6)

It is clear from Eq. (A6) that to show nonnegativity of $\langle \Psi | M_N(A, B) | \Psi \rangle$ for any $|\Psi\rangle \in \mathbb{C}^{N^d}$, one has to prove that for all $k$ the term in brackets in Eq. (A6) is nonnegative. This, however, follows from the fact that

$$\sum_{i,j=1}^N (a_{ik} - a_{jk})^2 \geq 0,$$

(A7)

finishing the proof.

Lemma 2.3. Let $A = \sum_{i,j=0}^{d-1} a_{ij} |i\rangle \langle j|$ be a positive matrix obeying $\text{Tr} A \leq 1$. Assume that each element of $A$ lying in $i$th row (and $i$th column due to hermiticity of $A$) is close to $1/d$ in the sense that $|a_{ij} - 1/d| \leq \epsilon$ for some $1/d > \epsilon > 0$. Then $|a_{ij} - 1/d| \leq \eta(\epsilon)$ for any $i, j = 0, \ldots, d-1$, where $\eta(\epsilon) \to 0$ for $\epsilon \to 0$.

Proof. The proof is rather technical and we present only its sketch here (detailed proof may be found in Ref. 26). First, let us fix the chosen row to be the first one, i.e., $i = 0$. Then, from the positivity of $A$ it follows that any matrix of the form

$$\begin{bmatrix} a_0^0 & a_0^j \\ a_0^i & a_j^j \end{bmatrix}$$

(A8)

is positive. Now, from its positivity we have that $a_0^0 a_j^j \geq |a_0^j|^2$, which together with the assumption that $a_0^0$ and $a_j^j$ are close to $1/d$ and $\epsilon < 1/d$, implies that $a_j^j$ must obey $a_j^j \geq 1/d - 3\epsilon$ for any $j = 1, \ldots, d-1$. Taking into account the assumption that $\text{Tr} A \leq 1$, one also has that each $a_j^j$ must be bounded from above as $a_j^j \leq 1/d + 3(d-1)\epsilon$ for $j = 1, \ldots, d-1$. Therefore, we have that all diagonal elements of $A$ satisfy

$$|a_j^j - 1/d| \leq \alpha(\epsilon)$$

(A9)

with $\alpha(\epsilon) \to 0$ for $\epsilon \to 0$. Now, we need to prove that the remaining off–diagonal elements of $A$ are also close to $1/d$. For this purpose let us notice that from the fact that $A \geq 0$ one has that the following matrices

$$\begin{bmatrix} a_0^0 & a_i^i & a_j^j \\ a_0^i & a_i^i & a_i^j \\ a_0^j & a_j^i & a_j^j \end{bmatrix}$$

(A10)

are also positive. Since we can now say that all elements in the first row (and column) and all the diagonal elements obey (A9), it follows, after some technical calculations, that $a_0^i$ has to satisfy such inequality, however, with some other function which vanishes for $\epsilon \to 0$. Finally, we have that any of the elements of $A$ satisfies

$$|a_i^j - 1/d| \leq \eta(\epsilon)$$

(A11)

with $\eta(\epsilon) \to 0$ whenever $\epsilon \to 0$.

Of course, we can always assume that the elements in some fixed row of $A$ is bounded by different $\epsilon$s. Then, however, we can take the largest one.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175179, Bangalore, India, December, 1984, IEEE Computer Society Press, New York.
[2] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. 77, 2818 (1996).
[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
[5] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. 92, 217903 (2004).
[6] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A 71, 022306 (2005).
[7] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).
[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[9] I. Devetak and A. Winter, Phys. Rev. Lett. 93, 080501 (2004).
[10] I. Devetak and A. Winter, Proc. R. Soc. Lond. A 461, 207 (2005).
[11] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. 80, 5239 (1998).
[12] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. 94, 160502 (2005).
[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, arXiv:quant-ph/0506189.
[14] K. Horodecki, General paradigm for distilling classical key from quantum states - on quantum entanglement and security, PhD Thesis, submitted to Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, May 2008.
[15] P. Horodecki and R. Augusiak, On quantum cryptography with bipartite bound entangled states, in Quantum Information Processing: From Theory to Experiment, proceedings of the NATO Advanced Study Institute on
Quantum Computation and Quantum Information, eds. D. G. Angelakis, M. Christandl, A. Ekert, M. Kay, and S. Kulik, NATO Science Series, III: Computer and Systems Sciences, vol. 199, 19-29, IOS Press, Amsterdam, 2006.

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

[17] J. M. Renes and G. Smith, Phys. Rev. Lett. 98, 020502, 2007.

[18] J. M. Renes, J.–Ch. Boileau, Phys. Rev. A 78, 032335 (2008).

[19] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner Unifying classical and quantum key distillation, in Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Science vol. 4392, pp. 456-478, 2007.

[20] G. Smith and J. Yard, Science 231, 1812 (2008).

[21] R. Renner, Int. J. Quant. Inf. 6, 1 (2008); see also quant-ph/0512258

[22] K. Horodecki, M. Horodecki, P Horodecki, D. Leung, J. Oppenheim, Phys. Rev. Lett. 100, 110502 (2008); IEEE Trans. Inf. Theory 54, 2604 (2008).

[23] R. Renner and R. König, Universally composable privacy amplification against quantum adversaries in Proc. of TCC 2005, LNCS, Springer, vol. 3378 (2005), pp. 407-425 (arXiv:quant-ph/0403133).

[24] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005); B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005).

[25] T. Moroder, M. Curty, N. Lütkenhaus, Phys. Rev. A 74, 052301 (2006).

[26] R. Augusiak, On the distillation of secure key form multipartite entangled quantum states, PhD thesis, Gdańsk, Poland, April 2008.

[27] P. Horodecki and R. Augusiak, Phys. Rev. A 74, 010302(R) (2006).

[28] D. M. Greenberger, M. Horne, and A. Zeilinger, in Bells Theorem, Quantum Theory, and Conceptions of the Universe, ed. M. Kafatos, Kluwer Academic, Dodrecht, 1989.

[29] M. Horodecki, Quant. Inf. Comp. 1, 3 (2001).

[30] P. Horodecki, Bound entanglement, in Lectures on Quantum Information, eds. D. Bruss and G. Leuchs, Wiley-VCH Verlag, Weinheim, 2007, p. 209.

[31] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. 78, 2275 (1997).

[32] M. B. Ruskai, Rev. Math. Phys. 6, 1147 (1994).

[33] R. Augusiak and P. Horodecki, Phys. Rev. A 74, 010305(R) (2006).

[34] J. A. Smolin, Phys. Rev. A 63, 032306 (2001).

[35] R. Augusiak and P. Horodecki, Phys. Rev. A 73, 012318 (2006).

[36] S. Bandyopadhyay, I. Chattopadhyay, V. P. Roychowdhury, and D. Sarkar, Phys. Rev. A 71, 062317 (2005).

[37] G. Wang and M. Ying, Phys. Rev. A 75, 052332 (2007).

[38] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).

[39] V. Scarani and N. Gisin, Phys. Rev. Lett. 87, 117901 (2001); Phys. Rev. A 65, 012311 (2001).

[40] A. Sen(De), U. Sen, and M. Žukowski, Phys. Rev. A 68, 032309 (2003).

[41] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A 59, 1829 (1999).

[42] R. Raussendorf, D. E. Browne, and H.–J. Briegel, Phys. Rev. A 68, 022312 (2003).

[43] K. Li, A. Winter, X.–B. Zou, G.–C. Guo, Nonadditivity of the Private Classical Capacity of a Quantum Channel, arXiv:0903.4308

[44] R. Renner and S. Wolf, Towards proving the existence of "bound" information in Proceedings of 2002 IEEE International Symposium on Information Theory (IEEE), Lausanne, Switzerland, June 30 - July 5, 2002, p. 103.

[45] A. Acín, J. I. Cirac, and Li. Masanes, Phys. Rev. Lett 92, 107903 (2004).

[46] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof, to be published in IEEE Trans. Inf. Theory, arXiv:0704.2230

[47] M. Navascués, J. Bae, J. I. Cirac, M. Lewenstein, A. Sanpera, and A. Acín, Phys. Rev. Lett. 94, 010502 (2005); C. Rodó, O. Romero–Isart, K. Eckert and A. Sanpera, Open Syst. Inf. Dyn. 14 69 (2007).

[48] J. Rigas, O. Gühne, N. Lütkenhaus, Phys. Rev. A 73, 012341 (2006).

[49] R. García–Patrón, N. J. Cerf, Phys. Rev. Lett. 102, 130501 (2009).

[50] M. Navascués and A. Acín, Phys. Rev. A 72, 012303 (2005).

[51] M.-D. Choi, Linear Alg. Appl. 10, 285 (1975); A. Jamiołkowski, Rep. Math. Phys. 3, 275 (1972).