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 and ICFO-Institute Ciéncies Fotóniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Paweł Horodecki†
Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland
(Received 27 November 2008; published 7 October 2009)

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 Greenberger-Horne-Zeilinger (GHZ) structure and nonzero distillable cryptographic key. We quantitatively estimate the key from below with the help of the privacy squeezing technique.

DOI: 10.1103/PhysRevA.80.042307 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography is one of the most successful applications of quantum physics in information theory. The original pioneering Bennett-Brassard 1984 protocol (BB84) scheme [1] was based on sending nonorthogonal states through an insecure quantum channel. Then the alternative approach [Ekert 1991 protocol (E91)] [2] based on generating key from pure entangled quantum state has 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 the 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 the 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) were also 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 [17–19]. 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 nonintuitive 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. [9,21,23–25]).

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 d-dimensional private states (multipartite p-dits) has been introduced and analyzed already in the previous paper [27].

It should be stressed here that, as extensively discussed in [14], 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 based on local von Neumann measurements, while it is possible also to consider local positive operator valued measure (POVMs) [17]. Both approaches were proved to be equivalent in terms of the amount of distillable key contained in a given bipartite

*remigiusz.augusiak@icfo.es
†pawel@mif.pg.gda.pl

state in Ref. [14]. 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 properties of the so-called classical-...-classical-quantum (**cq**) states was needed. The second part of the paper contains constructions of novel multiparite states that contain secure key though are bound entangled. The states are based on the underlying (twisted) N-partite Greenberger-Horne-Zeilinger (GHZ) structure and have positive partial transposition (PPT) with respect to any $N-1$ versus one subsystem cut. 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 p-dit and its properties are discussed including especially the condition for ϵ closeness to multipartite private states. Distillable cryptographic key in terms of p-dits is analyzed in Sec. 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 [9,10] 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 entangled states with cryptographic key. Note that the first construction, being an extension and modification of bipartite examples from Ref. [15], 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 local operations and classical communication (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 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])

$$\varrho_{AA'BE} = \sum_i \varrho^{(i)}_{ABE} \otimes |i\rangle\langle i|_{A'} \to \varrho_{AA'BB'EE'} = \sum_i \varrho^{(i)}_{ABE} \otimes |i\rangle\langle i|_{A'} \otimes |i\rangle\langle i|_{B'} \otimes |i\rangle\langle i|_{E'}, \quad (1)$$

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:

$$\varrho^{(N,\mathrm{id})}_{\mathsf{AE}} = \frac{1}{d}\sum_{i=0}^{d-1} |e_i^{(1)}\cdots e_i^{(N)}\rangle\langle e_i^{(1)}\cdots e_i^{(N)}| \otimes \varrho^E, \quad (2)$$

called hereafter *ideal* $c\ldots cq$(**cq**) *state*, by means of LOPC. Here $\mathsf{A}\equiv A_1\cdots A_N$ and $\{|e_i^{(j)}\rangle\}_{i=0}^{d-1}$ is some orthonormal basis in the Hilbert space corresponding to the jth party (denoted hereafter by $\mathcal{H}_j$). Their tensor product constitutes the product basis in $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_N$, which we shall denote as

$$\mathcal{B}_N^{\mathrm{prod}} = \{|e_{i_1}^{(1)}\rangle \otimes \cdots \otimes |e_{i_N}^{(N)}\rangle\}_{i_1,\ldots,i_N=0}^{d-1}. \quad (3)$$

(In what follows we will be often assuming $\{|e_i^{(j)}\rangle\}_{i=0}^{d-1}$ to be the standard basis in $\mathcal{H}_j$.) One sees that the ideal **cq** states represent perfect classical correlations with respect to the product basis $\mathcal{B}_N^{\mathrm{prod}}$ that are uncorrelated to the eavesdropper's degrees of freedom.

We may also define a general **cq** state to be

$$\varrho^{(N,\mathbf{cq})}_{\mathsf{AE}} = \sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N} |e_{i_1}^{(1)}\cdots e_{i_N}^{(N)}\rangle\langle e_{i_1}^{(1)}\cdots e_{i_N}^{(N)}| \otimes \varrho^E_{i_1\cdots i_N}. \quad (4)$$

In the above considerations 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 jth party is assumed to have an additional "garbage" quantum system defined on some Hilbert space $\mathcal{H}'_j$. 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 $\mathcal{H}=\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_N$ and $\mathcal{H}'=\mathcal{H}'_1\otimes\cdots\otimes\mathcal{H}'_N$, and $\mathcal{B}_N^{\mathrm{prod}}$ 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. [13,19], using the notion of **cq** states, we may define the distillable cryptographic key in the multipartite scenario as follows.

Definition II.1. Let ϱ_{AE} be a state acting on $\mathbb{C}^{d_1}\otimes\cdots\otimes\mathbb{C}^{d_N}\otimes\mathbb{C}^{d_E}$ and $(P_n)_{n=1}^{\infty}$ be a sequence of LOPC operations such that $P_n(\varrho_{\mathsf{AE}}^{\otimes n})=\varrho_{\mathsf{AE}}^{(\mathbf{cq},n)}$, where $\varrho_{\mathsf{AE}}^{(\mathbf{cq},n)}$ is a **cq** state with A part defined on $(\mathbb{C}^{d_n})^{\otimes N}$. The set of operations $P=(\Lambda_n)_{n=1}^{\infty}$ is

said to be a cryptographic key distillation protocol if

$$\lim_{n\to\infty}\|\varrho_{\mathsf{AE}}^{(\mathbf{cq},n)}-\varrho_{\mathsf{AE}}^{(\mathrm{id},n)}\|_1=0, \tag{5}$$

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

$$R_P(\varrho_{\mathsf{AE}})=\lim_{n\to\infty}\sup\frac{\log d_n}{n} \tag{6}$$

and the distillable classical key as

$$C_D(\varrho_{\mathsf{AE}})=\sup_P R_P(\varrho_{\mathsf{AE}}). \tag{7}$$

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

Let us also mention that a good indicator of the secrecy of our correlations as well as the uniformity of the probability distribution $p_{i_1\cdots i_N}$ is the trace norm distance $\|\varrho_{\mathsf{AE}}^{(\mathrm{id})}-\varrho_{\mathsf{AE}}^{(\mathbf{cq})}\|_1$.

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 $(U_{i_1\cdots i_N})_{i_1\cdots i_N}$ be some family of unitary operations acting on $\mathcal{H}'$. Given the N-partite product basis $\mathcal{B}_N^{\mathrm{prod}}$ we define *multipartite twisting* to be the unitary operation given by the following formula:

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

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 $\mathcal{B}_N^{\mathrm{prod}}$) to a given state $\varrho_{\mathsf{AA}'}$ does not have any effect on the **cq** state obtained upon a measurement of the A part of the purification of $\varrho_{\mathsf{AA}'}$ in the product basis $\mathcal{B}_N^{\mathrm{prod}}$. More precisely states $\varrho_{\mathsf{AA}'}$ and $U_t\varrho_{\mathsf{AA}'}U_t^{\dagger}$ have the same **cq** state with respect to $\mathcal{B}_N^{\mathrm{prod}}$ for any twisting that is constructed using $\mathcal{B}_N^{\mathrm{prod}}$.

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. [27].

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

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

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 $\Gamma_{\mathsf{AA}'}^{(d)}=U_t(P_{d,N}^{(+)}\otimes\varrho_{\mathsf{A}'})U_t^{\dagger}$ with $\varrho_{\mathsf{A}'}$ and U_t denoting some density matrix acting on $\mathcal{H}'$ and some twisting, respectively. Moreover, $P_{d,N}^{(+)}$ stands for the projector onto the GHZ state [28] given by

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

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

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

$$\begin{aligned}\Gamma_{\mathrm{ex}}^{(2)}&=\frac{1}{2D^N}\begin{bmatrix}\mathbb{1}_{D^N}&0&\ldots&V_\pi^{(D)}\\0&0&\ldots&0\\\vdots&\vdots&\ddots&\vdots\\V_\pi^{(D)\dagger}&0&\ldots&\mathbb{1}_{D^N}\end{bmatrix}\\&=\frac{1}{2D^N}[(|0\rangle\langle 0|^{\otimes N}+|1\rangle\langle 1|^{\otimes N})\otimes\mathbb{1}_{D^N}\\&\quad+(|0\rangle\langle 1|^{\otimes N}+|1\rangle\langle 0|^{\otimes N})\otimes V_\pi^{(D)}].\end{aligned} \tag{11}$$

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

$$V_\pi^{(D)}=\sum_{i_1,\ldots,i_N=0}^{D-1}|i_1\rangle\langle i_{\pi(1)}|\otimes|i_2\rangle\langle i_{\pi(2)}|\otimes\cdots\otimes|i_N\rangle\langle i_{\pi(N)}|, \tag{12}$$

with π being an arbitrary permutation of N-element set. Clearly $V_\pi^{(D)}$ is unitary matrix for any permutation π and thus $|V_\pi^{(D)}|=\mathbb{1}_{D^N}$ ($|A|$ is defined as $\sqrt{A^{\dagger}A}$). This, in view of the Lemma A.1 (Appendix), means that $\mathcal{M}_2(\mathbb{1}_{D^N},V_\pi^{(D)})\geqslant 0$ (for the definition of $\mathcal{M}_2$ see the Appendix) for any π and hence $\Gamma_{\mathrm{ex}}^{(2)}$ represents quantum state. Moreover, $\Gamma_{\mathrm{ex}}^{(2)}$ may be derived from general form (9) by substituting $\varrho_{\mathsf{A}'}=\mathbb{1}_{D^N}/D^N$, i.e., maximally mixed state acting on $(\mathbb{C}^D)^{\otimes N}$. Finally, both unitary operations in Eq. (9) may be taken to be $U_0=V_\pi^{(D)}$ and $U_1=\mathbb{1}_{D^N}$.

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 **cq** state is the ideal one with respect to some basis $\mathcal{B}_N$ must be of form (9) and *vice versa*.

Theorem III.1. Let $\varrho_{\mathsf{AA}'}$ be a state defined on $\mathcal{H}\otimes\mathcal{H}'$ with $\mathcal{H}=(\mathbb{C}^d)^{\otimes N}$ and arbitrary but finite-dimensional $\mathcal{H}'$. Let also $\varrho_{\mathsf{AE}}^{(\mathbf{cq})}$ denote the **cq** state obtained from the purification of $\varrho_{\mathsf{AA}'}$ upon the measurement of the A part in $\mathcal{B}_N^{\mathrm{prod}}$ and tracing out the A' part. Then $\varrho_{\mathsf{AE}}^{(\mathbf{cq})}$ is of form (2) if and only if $\varrho_{\mathsf{AA}'}$ is of form (9), both with respect to $\mathcal{B}_N^{\mathrm{prod}}$.

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 $\Gamma^{(d)}_{\mathsf{AA}'}$ its distillable entanglement is bounded as

$$E_D(\Gamma^{(d)}_{\mathsf{AA}'}) \geqslant \max_{\substack{i,j=0,\ldots,d-1\\ i<j}} \left\{ a_{ij}^{\max}\left[1 - H\left(\frac{1}{2} + \frac{\eta_{ij}}{2\sqrt{a_{ij}^{(1)}a_{ij}^{(2)}}}\right)\right]\right\}, \tag{13}$$

where η_{ij}, $a_{ij}^{(1)}$, $a_{ij}^{(1)}$, and finally $a_{ij}^{\max}$ are parameters characterizing the given private state $\Gamma^{(d)}_{\mathsf{AA}'}$. They are defined as follows:

$$\eta_{ij} = \max|\langle f_1|\cdots\langle f_N|U_i\varrho_{\mathsf{A}'}U_j^\dagger|g_1\rangle\cdots|g_N\rangle|, \tag{14}$$

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

$$a_{ij}^{(1)} = \langle\tilde{f}_1^{(ij)}|\cdots\langle\tilde{f}_N^{(ij)}|U_i\varrho_{\mathsf{A}'}U_i^\dagger|\tilde{f}_1^{(ij)}\rangle\cdots|\tilde{f}_N^{(ij)}\rangle \tag{15}$$

and

$$a_{ij}^{(2)} = \langle\tilde{g}_1^{(ij)}|\cdots\langle\tilde{g}_N^{(ij)}|U_j\varrho_{\mathsf{A}'}U_j^\dagger|\tilde{g}_1^{(ij)}\rangle\cdots|\tilde{g}_N^{(ij)}\rangle, \tag{16}$$

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

It follows from Eqs. (14)–(16) that η_{ij} is always positive and on the other hand $\eta_{ij} \leqslant \sqrt{a_{ij}^{(1)}a_{ij}^{(2)}}$. This means that $a_{ij}^{\max} > 0$ 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

$$E_C(\gamma^{(d)}_{A_1A_2A_1'A_2'}) \geqslant \log d \tag{17}$$

and, due to the fact that entanglement of formation is not smaller than the entanglement cost, $E_F(\gamma^{(d)}_{A_1A_2A_1'A_2'}) \geqslant \log d$.

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 $\varrho_{\mathsf{AA}'}$ 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:

$$\varrho_{\mathsf{AA}'} = \sum_{i_1,\ldots,i_N=0}^{d-1}\sum_{j_1,\ldots,j_N=0}^{d-1} |i_1\cdots i_N\rangle\langle j_1\cdots j_N| \otimes \Omega_{i_1\cdots i_N}^{j_1\cdots j_N}, \tag{18}$$

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

Lemma III.1. Let $\varrho_{\mathsf{AA}'}$ be some density matrix acting on $\mathcal{H}\otimes\mathcal{H}'$ with $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$ and arbitrary finite-dimensional $\mathcal{H}'$. Then there exists such twisting U_t that for a fixed index i all the elements $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}$ and $(\tilde{\varrho}_{\mathsf{A}})_{j\cdots j}^{i\cdots i}$ $(j=0,\cdots,d-1)$ of the ith row and column of $\tilde{\varrho}_{\mathsf{A}} = \mathrm{Tr}_{\mathsf{A}'}(U_t\varrho_{\mathsf{AA}'}U_t^\dagger)$ equal $\|\Omega_{i\cdots i}^{j\cdots j}\|_1$ and $\|\Omega_{j\cdots j}^{i\cdots i}\|_1$, respectively.

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

$$\tilde{\varrho}_{\mathsf{A}} = \sum_{i_1,\ldots,i_N=0}^{d-1}\sum_{j_1,\ldots,j_N=0}^{d-1} \mathrm{Tr}(U_{i_1\cdots i_N}\Omega_{i_1\cdots i_N}^{j_1\cdots j_N}U_{j_1\cdots j_N}^\dagger) \times|i_1\cdots i_N\rangle\langle j_1\cdots j_N|. \tag{19}$$

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 $\varrho_{\mathsf{AA}'}$ as the blocks $\Omega_{i_1\cdots i_N}^{i_1\cdots i_N}$ must be positive and the following holds:

$$\mathrm{Tr}(U_{i_1\cdots i_N}\Omega_{i_1\cdots i_N}^{i_1\cdots i_N}U_{i_1\cdots i_N}^\dagger) = \|\Omega_{i_1\cdots i_N}^{i_1\cdots i_N}\|_1. \tag{20}$$

Now, let us focus now on the matrices $\Omega_{i\cdots i}^{j\cdots j}$ 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 $j=1,\cdots,d-1$. At the beginning let us concentrate on the matrix $\Omega_{0\cdots0}^{1\cdots1}$. We can express it with the singular-value decomposition as $\Omega_{0\cdots0}^{1\cdots1} = V_1D_1W_1^\dagger$, where V_1 and W_1 are unitary matrices and D_1 stands for a diagonal matrix containing singular values of $\Omega_{0\cdots0}^{1\cdots1}$, i.e., eigenvalues of $|\Omega_{0\cdots0}^{1\cdots1}|$. Then from Eq. (19) one infers that it suffices to take $U_{0\cdots0} = V_1^\dagger$ and $U_{1\cdots1} = W$ in the twisting U_t to get

$$\begin{aligned}\mathrm{Tr}(U_{0\cdots0}\Omega_{0\cdots0}^{1\cdots1}U_{1\cdots1}^\dagger) &= \mathrm{Tr}(V^\dagger VDW^\dagger W)\\ &= \mathrm{Tr}D = \|\Omega_{0\cdots0}^{1\cdots1}\|_1.\end{aligned} \tag{21}$$

Now we may proceed with the remaining matrices $\Omega_{0\cdots0}^{j\cdots j}$ $(j=2,\ldots,d-1)$. We need to find such matrices in the twisting U_t that Eq. (21) holds also for the remaining $\Omega_{0\cdots0}^{j\cdots j}$. Notice that unitary matrices $U_{0\cdots0}$ and $U_{1\cdots1}$ have just been fixed, however, we have still some freedom provided by $U_{j\cdots j}$ $(j=2,\ldots,d-1)$. Using the singular value decomposition of all $\Omega_{0\cdots0}^{j\cdots j}$ $(j=2,\cdots,d-1)$ we may write $\Omega_{0\cdots0}^{j\cdots j} = V_jD_jW_j^\dagger$. This leads to

$$\begin{aligned}\mathrm{Tr}(U_{0\cdots0}\Omega_{0\cdots0}^{j\cdots j}U_{j\cdots j}^\dagger) &= \mathrm{Tr}(V^\dagger\Omega_{0\cdots0}^{j\cdots j}U_{j\cdots j}^\dagger)\\ &= \mathrm{Tr}(V^\dagger V_jD_jW_j^\dagger U_{j\cdots j}^\dagger)\\ &= \mathrm{Tr}(D_jW_j^\dagger U_{j\cdots j}^\dagger V^\dagger V_j),\end{aligned} \tag{22}$$

where we used the property of trace saying that $\mathrm{Tr}AB = \mathrm{Tr}BA$. It is clear from the above that to get the trace norm of $\Omega_{0\cdots0}^{j\cdots j}$ for any $j=2,\ldots,d-1$, it suffices to choose $U_{j\cdots j}$ in such way that $W_j^\dagger U_{j\cdots j}^\dagger V_1^\dagger V_j = \mathbf{1}$. This means that $U_{j\cdots j} = V_1^\dagger V_jW_j^\dagger$ $(j=2,\ldots,d-1)$. The remaining $U_{i_1\cdots i_N}$ appearing in the definition of U_t may be chosen at will. Concluding we showed that there exists such U_t that for a fixed i it holds that $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} = \|\Omega_{i\cdots i}^{j\cdots j}\|_1$ $(j=0,\ldots,d-1)$. The fact that also $(\tilde{\varrho}_{\mathsf{A}})_{j\cdots j}^{i\cdots i} = \|\Omega_{i\cdots i}^{j\cdots j}\|_1$ follows obviously from hermiticity of $\tilde{\varrho}_{\mathsf{A}}$. ∎

This is a very useful lemma due to the fact that twistings

do not change the **c**q state. It allows us to concentrate on a particular form of a given state $\varrho_{\mathsf{AA}'}$. In other words, we can think about the state $\varrho_{\mathsf{AA}'}$ 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 $\varrho_{\mathsf{AA}'}$ (obviously with respect to the same product basis $\mathcal{B}_N^{\mathrm{prod}}$). As an illustrative example we can consider $\varrho_{\mathsf{AA}'}$ with $d=2$. Then from Eq. (18) it can be written as

$$\varrho_{\mathsf{AA}'} = \begin{bmatrix} \Omega_{0\cdots0}^{0\cdots0} & \Omega_{0\cdots0}^{0\cdots1} & \cdots & \Omega_{0\cdots0}^{1\cdots1} \\ \Omega_{0\cdots1}^{0\cdots0} & \Omega_{0\cdots1}^{0\cdots1} & \cdots & \Omega_{0\cdots1}^{1\cdots1} \\ \vdots & \vdots & \ddots & \vdots \\ \Omega_{1\cdots1}^{0\cdots0} & \Omega_{1\cdots1}^{0\cdots1} & \cdots & \Omega_{1\cdots1}^{1\cdots1} \end{bmatrix}, \tag{23}$$

where $\Omega_{i_1\cdots i_N}^{j_1\cdots i_N}=(\Omega_{j_1\cdots j_N}^{i_1\cdots i_N})^\dagger$ and $\Omega_{i_1\cdots i_N}^{i_1\cdots i_N}\geqslant 0$ for any $i_k,j_k=0,1$. In view of Lemma 3.2 the above may be brought to the following state:

$$\begin{aligned}\widetilde{\varrho}_{\mathsf{A}} &\equiv \mathrm{Tr}_{\mathsf{A}'}(U_t\varrho_{\mathsf{AA}'}U_t^\dagger) \\ &= \begin{bmatrix} \|\Omega_{0\cdots0}^{0\cdots0}\|_1 & (\widetilde{\varrho}_{\mathsf{A}})_{0\cdots0}^{0\cdots1} & \cdots & \|\Omega_{0\cdots0}^{1\cdots1}\|_1 \\ (\widetilde{\varrho}_{\mathsf{A}})_{0\cdots1}^{0\cdots0} & \|\Omega_{0\cdots1}^{0\cdots1}\|_1 & \cdots & (\widetilde{\varrho}_{\mathsf{A}})_{0\cdots1}^{1\cdots1} \\ \vdots & \vdots & \ddots & \vdots \\ \|\Omega_{1\cdots1}^{0\cdots0}\|_1 & (\widetilde{\varrho}_{\mathsf{A}})_{1\cdots1}^{0\cdots1} & \cdots & \|\Omega_{1\cdots1}^{1\cdots1}\|_1 \end{bmatrix}.\end{aligned} \tag{24}$$

Now we are prepared to provide the aforementioned conditions for closeness to multipartite private states (the bipartite case was discussed in Ref. [13]). Firstly we show that if a given $\varrho_{\mathsf{AA}'}$ is close to some multipartite p-dit then (due to the above lemma), there exist such U_t that the A subsystem has all the elements $(\mathrm{Tr}_{\mathsf{A}'}U_t\varrho_{\mathsf{AA}'}U_t^\dagger)_{i\cdots i}^{j\cdots j}=\|\Omega_{i\cdots i}^{j\cdots j}\|_1$ for $j=0,\ldots,d-1$ close to $1/d$.

Theorem III.2. Let $\Omega_{i_1\cdots i_N}^{j_1\cdots j_N}$ be some matrices and $\varrho_{\mathsf{AA}'}$ be an N-partite state of the form (18) such that $\|\varrho_{\mathsf{AA}'}-\Gamma_{\mathsf{AA}'}^{(d)}\|_1 \leqslant \epsilon$ for some multipartite private state $\Gamma_{\mathsf{AA}'}^{(d)}$, for some $\epsilon>0$. Then for a fixed index i one has $|\|\Omega_{i\cdots i}^{j\cdots j}\|_1-(1/d)|\leqslant\epsilon$ and $|\|\Omega_{j\cdots j}^{i\cdots i}\|_1-(1/d)|\leqslant\epsilon$ for any $j=0,\ldots,d-1$.

Proof. The proof is a modification of the one given in Ref. [13] (Proposition 3). Let $\Gamma_{\mathsf{AA}'}^{(d)}$ be such a private state that $\|\varrho_{\mathsf{AA}'}-\Gamma_{\mathsf{AA}'}^{(d)}\|_1\leqslant\epsilon$ and U_t be such twisting that $\Gamma_{\mathsf{AA}'}^{(d)}=U_t(P_{d,N}^{(+)}\otimes\sigma_{\mathsf{A}'})U_t^\dagger$ with $\sigma_{\mathsf{A}'}$ denoting some state on $\mathcal{H}'$. Then, due to the invariance of the trace norm under unitary operations, we have

$$\|U_t^\dagger\varrho_{\mathsf{AA}'}U_t-P_{d,N}^{(+)}\otimes\sigma_{\mathsf{A}'}\|_1\leqslant\epsilon. \tag{25}$$

Now, utilizing the fact that the trace norm can only decrease under the partial trace, we get

$$\|\widetilde{\varrho}_{\mathsf{A}}-P_{d,N}^{(+)}\|_1\leqslant\epsilon, \tag{26}$$

where $\widetilde{\varrho}_{\mathsf{A}}$ is of form (19). Notice that in general U_t does not have to be the one bringing $\widetilde{\varrho}_{\mathsf{A}}$ to the form discussed in Lemma III.1. After application of the explicit form of $P_{d,N}^{(+)}$ and $\widetilde{\varrho}_{\mathsf{A}}$ given by Eq. (19), one can rewrite the above as

$$\left\| \sum_{\substack{i_1,\ldots,i_N=0 \\ j_1,\ldots,j_N=0}}^{d-1} |i_1\cdots i_N\rangle\langle j_1\cdots j_N|\mathrm{Tr}(U_{i_1\cdots i_N}\Omega_{i_1\cdots i_N}^{j_1\cdots j_N}U_{j_1\cdots j_N}^\dagger) - \frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j|^{\otimes N}\right\|_1 \leqslant \epsilon. \tag{27}$$

Now we may utilize the fact that for any $A=\Sigma_{ij}a_{ij}|i\rangle\langle j|$ square of its Hilbert-Schmidt norm is given by $\|A\|_2^2=\Sigma_{ij}|a_{ij}|^2$ and that $\|A\|_2\leqslant\|A\|_1$. Therefore, if $\|A\|_2\leqslant\epsilon$ for some $\epsilon>0$ then one infers that any of its elements obeys $|a_{ij}|\leqslant\epsilon$ $(i,j=0,\ldots,d-1)$. This reasoning, after application to the matrix $\widetilde{\varrho}_{\mathsf{A}}-P_{d,N}^{(+)}$, leads us to the conclusion that for any $i,j=0,\ldots,d-1$ it holds

$$\left|\mathrm{Tr}(U_{i\cdots i}\Omega_{i\cdots i}^{j\cdots j}U_{j\cdots j}^\dagger)-\frac{1}{d}\right|\leqslant\epsilon, \tag{28}$$

which eventually gives $|\mathrm{Tr}(U_{i\cdots i}\Omega_{i\cdots i}^{j\cdots j}U_{j\cdots j}^\dagger)|\geqslant 1/d-\epsilon$. This, after application of the polar decomposition of $\Omega_{i\cdots i}^{j\cdots j}$ and properties of trace, can be rewritten as $|\mathrm{Tr}(W_{ij}|\Omega_{i\cdots i}^{j\cdots j}|)|\geqslant 1/d-\epsilon$ 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:

$$\begin{aligned}|\mathrm{Tr}(WA)| &= |\mathrm{Tr}(W\sqrt{A}\sqrt{A})| \\ &\leqslant \sqrt{\mathrm{Tr}(W\sqrt{A}\sqrt{A}W^\dagger)}\sqrt{\mathrm{Tr}\sqrt{A}\sqrt{A}} \\ &= \mathrm{Tr}A=\|A\|_1.\end{aligned} \tag{29}$$

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

On the other hand we can apply such twisting $\widetilde{U}_t$ that after application to $\varrho_{\mathsf{AA}'}$ and tracing out the A' subsystem, we get $\widetilde{\varrho}_{\mathsf{A}}$ such that in its ith row (or column) $(\widetilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}=\|\Omega_{i\cdots i}^{j\cdots j}\|$ for $j=1,\ldots,d-1$. Then, one easily concludes that

$$\|\widetilde{\varrho}_{\mathsf{AA}'}-\widetilde{U}_t^\dagger\Gamma_{\mathsf{AA}'}^{(d)}\widetilde{U}_t\|_1\leqslant\epsilon \tag{30}$$

with $\widetilde{\varrho}_{\mathsf{AA}'}=\widetilde{U}_t\varrho_{\mathsf{AA}'}\widetilde{U}_t^\dagger$. After the analogous reasoning as in the previous case we get

$$\left|\|\Omega_{i\cdots i}^{j\cdots j}\|_1-\frac{1}{d}\mathrm{Tr}(\widetilde{W}_{ij}\sigma_{\mathsf{A}'})\right|\leqslant\epsilon \tag{31}$$

for some chosen i and $j=0,\ldots,d-1$. Here by W_{ij} we denoted all product of the respective unitary matrices following from product of $\widetilde{U}_t$ and U_t. Using the fact that $|z_1-z_2|\geqslant|z_1|-|z_2|$, we infer from the above inequality that

$$\|\Omega_{i\cdots i}^{j\cdots j}\|_1\leqslant\epsilon+\frac{1}{d}|\mathrm{Tr}(\widetilde{W}_{ij}\sigma_{\mathsf{A}'})|. \tag{32}$$

It follows from the Cauchy-Schwarz inequality that the absolute value on the right-hand side is not greater that one. Thus we get the inequalities

$$\|\Omega_{i\cdots i}^{j\cdots j}\|_1 \leqslant \epsilon + \frac{1}{d} \tag{33}$$

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 $\|\Omega_{0\cdots 0}^{1\cdots 1}\|_1 \geqslant 1/2-\epsilon$. This is because, due to the fact that $\mathrm{Tr}\tilde{\varrho}_{\mathsf{A}}=1$ and the positivity of $\tilde{\varrho}_{\mathsf{A}}\geqslant 0$ (and thus also of the 2×2 matrix containing the elements $\|\Omega_{i\cdots i}^{j\cdots j}\|_1$ with $i,j=0,1$) $\|\Omega_{0\cdots 0}^{1\cdots 1}\|_1 \leqslant 1/2$.

Interestingly, one may prove also a converse statement, namely, if for some fixed row, say the ith one, all $\|\Omega_{i\cdots i}^{j\cdots j}\|_1$ are close to $1/d$, then there exists some multipartite private state close to a given state $\varrho_{\mathsf{AA}'}$.

Theorem III.3. Let $\varrho_{\mathsf{AA}'}$ given by Eq. (18) be such that for a fixed i the blocks $\Omega_{i\cdots i}^{j\cdots j}$ obey $|\|\Omega_{i\cdots i}^{j\cdots j}\|_1 - 1/d| \leqslant \epsilon$ for any $j=0,\ldots,d-1$ and $0<\epsilon<1/d$. Then there exists such a multipartite private state $\Gamma_{\mathsf{AA}'}^{(d)}$ that

$$\|\varrho_{\mathsf{AA}'} - \Gamma_{\mathsf{AA}'}^{(d)}\|_1 \leqslant \sqrt{\log 2[2N\sqrt{d\eta(\epsilon)}\log d + H(2\sqrt{d\eta(\epsilon)})]} + 2\sqrt{d\eta(\epsilon)}, \tag{34}$$

where $\eta(\epsilon)\to 0$ if $\epsilon\to 0$ and consequently the function on the right-hand side tends to zero whenever $\epsilon\to 0$. Here H denotes the binary entropy.

Proof. The proof is based on the one given in Ref. [13]. Let U_t be such twisting that for fixed i it holds of $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} = \|\Omega_{i\cdots i}^{j\cdots j}\|_1$ $(j=0,\ldots,d-1)$. Then since $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} = [(\tilde{\varrho}_{\mathsf{A}})_{j\cdots j}^{i\cdots i}]^*$ with asterisk denoting complex conjugation, the Hilbert-Schmidt scalar product of $\tilde{\varrho}_{\mathsf{A}}$ and $P_{D,N}^{(+)}$ may be expressed as

$$\begin{aligned}\mathrm{Tr}(\tilde{\varrho}_{\mathsf{A}}P_{d,N}^{(+)}) &= \frac{1}{d}\sum_{i,j=0}^{d-1}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} \\ &= \frac{1}{d}\sum_{i=0}^{d-1}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{i\cdots i} + \frac{2}{d}\sum_{\substack{i,j=0\\ i<j}}^{d-1}\mathrm{Re}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}.\end{aligned} \tag{35}$$

On the other hand from the positivity of $\tilde{\varrho}_{\mathsf{A}}$ one may prove the following inequality:

$$\sum_{i=0}^{d-1}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{i\cdots i} \geqslant \frac{2}{d-1}\sum_{\substack{i,j=0\\ i<j}}^{d-1}\mathrm{Re}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}, \tag{36}$$

which after substitution to Eq. (35) gives

$$\mathrm{Tr}(\tilde{\varrho}_{\mathsf{A}}P_{d,N}^{(+)}) \geqslant \frac{2}{d-1}\sum_{\substack{i,j=0\\ i<j}}^{d-1}\mathrm{Re}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}. \tag{37}$$

Now we can utilize Lemma A.2 (see the Appendix) to the $d\times d$ matrix with entries $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}$ $(i,j=0,\ldots,d-1)$. Namely, due to the assumption that for some fixed i the elements $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}$ satisfy $|(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} - 1/d| \leqslant \epsilon$, we have from Lemma A.2 that $|(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} - 1/d| \leqslant \eta(\epsilon)$ 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 $(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j}$ also satisfies the above condition. In this light we get from Eq. (37) that

$$\begin{aligned}\mathrm{Tr}(\tilde{\varrho}_{\mathsf{A}}P_{d,N}^{(+)}) &\geqslant \frac{2}{d-1}\sum_{\substack{i,j=0\\ i<j}}^{d-1}\mathrm{Re}(\tilde{\varrho}_{\mathsf{A}})_{i\cdots i}^{j\cdots j} \\ &\geqslant \frac{2}{d-1}\sum_{\substack{i,j=0\\ i<j}}^{d-1}\left(\frac{1}{d}-\eta(\epsilon)\right) \\ &= \frac{2}{d-1}\frac{d(d-1)}{2}\left(\frac{1}{d}-\eta(\epsilon)\right) \\ &= 1-d\eta(\epsilon),\end{aligned} \tag{38}$$

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 $\|\Omega_{0\cdots 0}^{1\cdots 1}\|_1 \geqslant 1/2-\epsilon$.

Concluding we obtained necessary and sufficient conditions for a given state $\varrho_{\mathsf{AA}'}$ to be close to some multipartite private state expressed in terms of the trace norm of some blocks of $\varrho_{\mathsf{AA}'}$ [see Eq. (18)].

IV. DISTILLABLE CRYPTOGRAPHIC KEY

A. 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 do not need to take the eavesdropper into account explicitly.

Definition IV.1. Let ϱ_{A} denote a given multipartite state acting on $\mathbb{C}^{d_1}\otimes\cdots\otimes\mathbb{C}^{d_N}$ and $(\Lambda_n)_{n=1}^{\infty}$ a sequence of LOCC operations giving $\Lambda_n(\varrho_{\mathsf{A}}^{\otimes n})=\varrho_{\mathsf{AA}'}^{(n)}$ with $\varrho_{\mathsf{AA}'}^{(n)}$ being a state acting on $(\mathbb{C}^{d_n})^{\otimes N}\otimes\mathcal{H}_n'$. Here $\mathcal{H}_n'$ stands for a finite-dimensional Hilbert space corresponding to the A' part of $\varrho_{\mathsf{AA}'}^{(n)}$. 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 $(\Gamma_{\mathsf{AA}'}^{(d_n)})_{n=1}^{\infty}$ that the condition

$$\lim_{n\to\infty}\|\varrho_{\mathsf{AA}'}^{(n)} - \Gamma_{\mathsf{AA}'}^{(d_n)}\|_1 = 0 \tag{39}$$

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

$$K_D(\varrho_{\mathsf{A}}) = \sup_{\Lambda} R_{\Lambda}(\varrho_{\mathsf{A}}). \tag{40}$$

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.

Theorem IV.1. The following two implications hold. Assume that from a given state σ_{A} such that Eve has its purification $|\psi_{\mathsf{A}E}\rangle$ one may create by LOPC some **cq** state $\varrho_{\mathsf{A}E}^{(\mathrm{cq})}$ [see Eq. (4)] obeying $\|\varrho_{\mathsf{A}E}^{(\mathrm{cq})}-\varrho_{\mathsf{A}E}^{(\mathrm{id})}\|_1\leq\epsilon$ for some $\epsilon>0$ [recall that $\varrho_{\mathsf{A}E}^{(\mathrm{id})}$ denotes the ideal **cq** state given by Eq. (2)]. Then there exists such LOCC protocol that can distill a state $\varrho_{\mathsf{A}\mathsf{A}'}$ from σ_{A} that satisfies $\|\varrho_{\mathsf{A}\mathsf{A}'}-\Gamma_{\mathsf{A}\mathsf{A}'}^{(d)}\|_1\leq 2\sqrt{\epsilon}$ for some multipartite private state $\Gamma_{\mathsf{A}\mathsf{A}'}^{(d)}$. On the other hand if from σ_{A} one can distill a state $\varrho_{\mathsf{A}\mathsf{A}'}$ close to some p-dit $\Gamma_{\mathsf{A}\mathsf{A}'}^{(d)}$, i.e., such that $\|\varrho_{\mathsf{A}\mathsf{A}'}-\Gamma_{\mathsf{A}\mathsf{A}'}^{(d)}\|_1\leq\epsilon$ then there exists a LOPC protocol distilling from ϱ_{A} a **cq** state such that $\|\varrho_{\mathsf{A}E}^{(\mathrm{cq})}-\varrho_{\mathsf{A}E}^{(\mathrm{id})}\|_1\leq 2\sqrt{\epsilon}$. Each subsystem of the A part of $\varrho_{\mathsf{A}E}^{(\mathrm{cq})}$ and of the key part of $\Gamma_{\mathsf{A}\mathsf{A}'}^{(d)}$ is defined on $\mathbb{C}^d$.

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 Refs. [5,6] 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.

B. 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 [9,10]. Let us start from the upper bound.

Theorem IV.2. Let ϱ_{A} be some N-partite state. Then

$$K_D(\varrho_{\mathsf{A}})\leq E_r^{\infty}(\varrho_{\mathsf{A}}), \tag{41}$$

where $E_r^{\infty}(\varrho_{\mathsf{A}})$ is a regularized version of the relative entropy, i.e.,

$$E_r^{\infty}(\varrho_{\mathsf{A}})=\lim_{n\to\infty}\frac{1}{n}\inf_{\varrho_{\mathsf{A}}^{\mathrm{sep}}\in\mathcal{D}} S(\varrho_{\mathsf{A}}^{\otimes n}\|\varrho_{\mathsf{A}}^{\mathrm{sep}}) \tag{42}$$

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

$$\varrho_{\mathsf{A}}^{\mathrm{sep}}=\sum_i p_i\varrho_{A_1}^{(i)}\otimes\cdots\otimes\varrho_{A_N}^{(i)}. \tag{43}$$

Proof. The proof is a generalization of the one from Ref. [13].

Interestingly, we may also bound K_D from below. For this purpose we need to prove the following theorem.

Theorem IV.3. Let $\varrho_{\mathsf{A}E}^{(\mathrm{cq})}$ be some multipartite **cq** state acting on $(\mathbb{C}^d)^{\otimes N}\otimes\mathbb{C}^{d_E}$ and given by

$$\varrho_{\mathsf{A}E}^{(\mathrm{cq})}=\sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N}|i_1\cdots i_N\rangle\langle i_1\cdots i_N|. \tag{44}$$

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_iA_jE with $j\neq i$ are arbitrarily close to the bipartite ideal ccq state. More precisely, if $\|\varrho_{\mathsf{A}E}^{(\mathrm{cq})}-\varrho_{\mathsf{A}E}^{(N,\mathrm{id})}\|\leq\epsilon$ holds for $\epsilon>0$, then for the fixed party A_i the following inequalities:

$$\left\|\sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N}|i_ki_l\rangle\langle i_ki_l|\otimes\varrho_{i_1\cdots i_N}^{E}-\varrho_{\mathsf{A}E}^{(2,\mathrm{id})}\right\|_1\leq\epsilon, \tag{45}$$

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

$$\|\varrho_{\mathsf{A}E}^{(\mathrm{cq})}-\varrho_{\mathsf{A}E}^{(N,\mathrm{id})}\|_1\leq(4N-3)\epsilon. \tag{46}$$

Proof. We proceed in two steps. In the first step we show that if the trace norm distance between some multipartite **cq** state $\varrho_{\mathsf{A}E}^{(\mathrm{cq})}$ 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 ccq 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 [31]. The proof of the converse statement is much more sophisticated.

Let us assume that the following:

$$\|\varrho_{\mathsf{A}E}^{(\mathrm{cq})}-\varrho_{\mathsf{A}E}^{(N,\mathrm{id})}\|_1\leq\epsilon, \tag{47}$$

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:

$$\left\|\sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N}|i_ki_l\rangle\langle i_ki_l|\otimes\varrho_{i_1\cdots i_N}^{E}-\varrho_{\mathsf{A}E}^{(2,\mathrm{id})}\right\|_1\leq\epsilon \tag{48}$$

for any pair of indices $k,l=1,\ldots,N$. To end the first part of the proof it suffices to substitute $\Sigma_{I\setminus\{k,l\}}p_{i_1\cdots i_N}\varrho_{i_1\cdots i_N}^{E}=q_{i_ki_l}\tilde{\varrho}_{i_ki_l}^{E}$, where summation over $I\setminus\{k,l\}$ means that we sum over all i_j but i_k 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:

$$\left\|\sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N}|i_1i_j\rangle\langle i_1i_j|\otimes\varrho_{i_1\cdots i_N}^{E}-\varrho_{\mathsf{A}E}^{(2,\mathrm{id})}\right\|_1\leq\epsilon, \tag{49}$$

are satisfied. Basing on this set of inequalities we will show that the left-hand side of Eq. (47) is bounded from above by some linear function of ϵ vanishing for $\epsilon\to 0$. For this purpose let us denote the left-hand side of Eq. (47) by LHS and notice that it can be split into two sums [see Eqs. (2) and (4)], namely, the one containing the elements for $i_1=\cdots=i_N$ 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 $i_1=\cdots=i_N$ from the set of all possible sequences, we can write

$$\mathrm{LHS} = \sum_{(i_1,\ldots,i_N)\in I} p_{i_1\cdots i_N} + \sum_{i=0}^{d-1} \left\| p_{i\cdots i}\varrho^E_{i\cdots i} - \frac{1}{d}\varrho^E \right\|_1$$
$$\leqslant \sum_{(i_1,\ldots,i_N)\in I} p_{i_1\cdots i_N} + \sum_{i=0}^{d-1} p_{i\cdots i}\left\|\varrho^E_{i\cdots i} - \varrho^E\right\|_1 + \sum_{i=0}^{d-1}\left| p_{i\cdots i} - \frac{1}{d}\right|, \tag{50}$$

where the inequality comes from the fact that the term $p_{i\cdots i}\varrho^E_{i\cdots i}$ was added and subtracted in the second term in the first line and from the inequality $\|A+B\|_1 \leqslant \|A\|_1 + \|B\|_1$. 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 inequalities (49), we show that all the three terms appearing in the above are bounded by linear functions of ϵ vanishing for $\epsilon \to 0$. With this aim, utilizing once more the fact that the trace norm does not increase under the partial trace [31], we can infer from Eq. (49) that

$$\left\| \sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N} |i_1 i_j\rangle\langle i_1 i_j| - \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \right\|_1 \leqslant \epsilon \tag{51}$$

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:

$$\sum_{i=0}^{d-1}\left| \sum_{i_2,\ldots,i_{j-1},i_{j+1},\ldots,i_N=0}^{d-1} p_{ii_2\cdots i_{j-1}ii_{j+1}\cdots i_N} - \frac{1}{d}\right| + \sum_{\substack{i_1,\ldots,i_N=0 \\ i_1\neq i_j}}^{d-1} p_{i_1\cdots i_N} \leqslant \epsilon. \tag{52}$$

Obviously, since both terms in the above are non-negative, any of them must be less or equal to ϵ. This allows us to write the inequalities

$$\sum_{i=0}^{d-1}\left| \sum_{i_2,\ldots,i_{j-1},i_{j+1},\ldots,i_N=0}^{d-1} p_{ii_2\cdots i_{j-1}ii_{j+1}\cdots i_N} - \frac{1}{d}\right| \leqslant \epsilon \tag{53}$$

and

$$\sum_{\substack{i_1,\ldots,i_N=0 \\ i_1\neq i_j}}^{d-1} p_{i_1\cdots i_N} \leqslant \epsilon. \tag{54}$$

From the sum appearing under the sign of an absolute value in Eq. (53) we can extract the probability $p_{i\cdots i}$, obtaining

$$\sum_{i=0}^{d-1}\left| p_{i\ldots i} - \frac{1}{d} + \sum_{\substack{i_2,\ldots i_{j-1},i_{j+1},\ldots,i_N=0 \\ (i_2,\ldots i_{j-1},i_{j+1},\ldots,i_N)\in\mathcal{I}_i}}^{d-1} p_{ii_2\cdots i_{j-1}ii_{j+1}\cdots i_N}\right| \leqslant \epsilon, \tag{55}$$

where $\mathcal{I}_i$ 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 $|z_1-z_2| \geqslant |z_1| - |z_2|$ satisfied by all $z_1, z_2 \in \mathbb{C}$, we get

$$\sum_{i=0}^{d-1}\left| p_{i\ldots i} - \frac{1}{d}\right| \leqslant \epsilon + \sum_{i=0}^{d-1}\sum_{(i_2,\ldots,i_{j-1},i_{j+1},\ldots,i_N)\in\mathcal{I}_i} p_{ii_2\cdots i_{j-1}ii_{j+1}\cdots i_N}$$
$$= \epsilon + \sum_{(i_1,\ldots,i_N)\in\tilde{\mathcal{I}}_j} p_{i_1\cdots i_N}, \tag{56}$$

where $\tilde{\mathcal{I}}_j$ denotes the string of N indices such that the first and jth 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:

$$\sum_{(i_1,\ldots,i_N)\in\tilde{\mathcal{I}}_j} p_{i_1\cdots i_N} \leqslant \sum_{k=2}^{j-1}\sum_{\substack{i_1,\ldots,i_N=0 \\ i_k\neq i_1}}^{d-1} p_{i_1\cdots i_N} + \sum_{k=j+1}^{N}\sum_{\substack{i_1,\ldots,i_N=0 \\ i_k\neq i_1}}^{d-1} p_{i_1\cdots i_N}$$
$$\leqslant \sum_{k=2}^{j-1}\epsilon + \sum_{k=j+1}^{N}\epsilon = (N-2)\epsilon, \tag{57}$$

where the second inequality is a consequence of the inequality given in Eq. (54). Finally, application of Eq. (57) to Eq. (56), gives

$$\sum_{i=0}^{d-1}\left| p_{i\cdots i} - \frac{1}{d}\right| \leqslant (N-1)\epsilon. \tag{58}$$

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 $|z_1-z_2| \geqslant |z_1| - |z_2| (z_1, z_2 \in \mathbb{C})$ and the fact that $p_{i_1\cdots i_N}$ represents some probability distribution, we may write

$$\sum_{(i_1,\ldots,i_N)\in I} p_{i_1\ldots i_N} = 1 - \sum_{i=0}^{d-1} p_{i\cdots i} \leqslant 1 - [1-(N-1)\epsilon]$$
$$= (N-1)\epsilon. \tag{59}$$

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 whole set (49), say the one for $j=2$. The we can write

$$\left\| \sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N} |i_1 i_2\rangle\langle i_1 i_2| \otimes \varrho^E_{i_1\cdots i_N} - \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \otimes \varrho^E \right\|_1$$
$$= \Bigg\| \sum_{i=0}^{d-1} p_{i\cdots i} |ii\rangle\langle ii| \otimes \varrho^E_{i\cdots i} - \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \otimes \varrho^E + \sum_{(i_1,\ldots,i_N)\in\tilde{\mathcal{I}}_2} p_{i_1\cdots i_N} |i_1 i_1\rangle\langle i_1 i_1| \otimes \varrho^E_{i_1\cdots i_N}$$
$$+ \sum_{\substack{i_1,\ldots,i_N=0 \\ i_1\neq i_2}}^{d-1} p_{i_1\cdots i_N} |i_1 i_2\rangle\langle i_1 i_2| \otimes \varrho^E_{i_1\cdots i_N} \Bigg\|_1. \tag{60}$$

Then, due to the fact that $\|A-B\|_1 \geqslant \|A\|_1 - \|B\|_1$, we may rewrite the above equation as

$$\left\| \sum_{i=0}^{d-1} p_{i\cdots i} |ii\rangle\langle ii| \otimes \varrho^E_{i\cdots i} - \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \otimes \varrho^E \right\|_1$$
$$\leqslant \epsilon + \sum_{(i_1,\ldots,i_N)\in\tilde{\mathcal{I}}_2} p_{i_1\cdots i_N} + \sum_{\substack{i_1,\ldots,i_N=0 \\ i_1\neq i_2}}^{d-1} p_{i_1\cdots i_N}$$
$$\leqslant \epsilon + (N-2)\epsilon + \epsilon = N\epsilon, \tag{61}$$

where the second inequality follows from Eqs. (52) and (57) (with $j=2$). On the other hand, we can easily show that

$$\left\| \sum_{i=0}^{d-1} p_{i\cdots i} |ii\rangle\langle ii| \otimes \varrho^E_{i\cdots i} - \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii| \otimes \varrho^E \right\|_1$$
$$\geqslant \sum_{i=0}^{d-1} p_{i\cdots i} \|\varrho^E_{i\cdots i} - \varrho^E\|_1 - \sum_{i=0}^{d-1} \left| p_{i\cdots i} - \frac{1}{d} \right|. \tag{62}$$

Comparison of Eqs. (58), (61), and (62) allows us to write

$$\sum_{i=0}^{d-1} p_{i\cdots i} \|\varrho^E_{i\cdots i} - \varrho^E\|_1 \leqslant N\epsilon + \sum_{i=0}^{d-1} \left| p_{i\cdots i} - \frac{1}{d} \right|$$
$$\leqslant N\epsilon + (N-1)\epsilon$$
$$= (2N-1)\epsilon. \tag{63}$$

Putting now all the pieces together, that is, substituting Eqs. (58), (59), and (63) to Eq. (50), we finally have

$$\left\| \sum_{i_1,\ldots,i_N=0}^{d-1} p_{i_1\cdots i_N} |i_1\cdots i_N\rangle\langle i_1\cdots i_N| \otimes \varrho^E_{i_1\cdots i_N} - \frac{1}{d}\sum_{i=0}^{d-1} |i\rangle\langle i|^{\otimes N} \otimes \varrho^E \right\|_1 \leqslant (4N-3)\epsilon. \tag{64}$$

Noting that for fixed N it holds that $(4N-3)\epsilon \to 0$ whenever $\epsilon \to 0$ 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 Eq. (49). Actually it suffices to assume that a single inequality from 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_iA_j (with fixed i and arbitrary $j\neq i$) are perfectly correlated and Eve has a 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 $\varrho_{\mathsf{A}E}$ 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)

$$\varrho^{(\mathbf{cq})}_{\mathsf{A}E} = \sum_i p_i |i\rangle\langle i|_{A_1} \otimes \varrho^{(i)}_{A_2\cdots A_N E}. \tag{65}$$

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 $I(A_1{:}A_j)(\varrho^{(\mathrm{cqq})}_{A_1A_jE})$. However, the establish common multipartite key we need to consider the worst case, i.e., $\min_{j=2,\ldots,N} I(A_1{:}A_j)(\varrho^{(\mathrm{cqq})}_{A_1A_jE})$. 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 substracted at the privacy amplification stage of the process.

Consequently, the rate of the protocol is

$$\min_{j=2,\ldots,N} I(A_1{:}A_j)(\varrho^{(\mathrm{cqq})}_{A_1A_jE}) - I(A_1{:}E)(\varrho^{(\mathrm{cqq})}_{A_1A_jE}) \tag{66}$$

and, therefore, the multipartite distillable key satisfies

$$C_D(\varrho_{\mathsf{A}E}) \geqslant \min_{j=2,\ldots,N} I(A_1{:}A_j)(\varrho^{(\mathrm{cqq})}_{A_1A_jE}) - I(A_1{:}E)(\varrho^{(\mathrm{cqq})}_{A_1A_jE}). \tag{67}$$

Here, $\varrho^{(\mathrm{cqq})}_{A_1A_jE}$ denotes the cqq state, which arises from Eq. (65) by tracing out all the parties but the first and jth 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

$$C_D(\varrho_{\mathsf{A}E}) \geqslant \max_{i=1,\ldots,N} \left[\min_{\substack{j=1,\ldots,N \\ j\neq i}} I(A_i{:}A_j)(\varrho^{(\mathrm{cqq})}_{A_iA_jE}) - I(A_i{:}E)(\varrho^{(\mathrm{cqq})}_{A_iA_jE}) \right], \tag{68}$$

Let us finally mention that due to Theorem IV.1 we can also bound K_D from below using Eq. (68). Namely, since $K_D(\varrho_{\mathsf{A}}) = C_D(|\psi_{\mathsf{A}E}\rangle)$, we have the following:

$$K_D(\varrho_{\mathsf{A}}) \geqslant \max_{i=1,\ldots,N} \left[\min_{\substack{j=1,\ldots,N \\ j\neq i}} I(A_i{:}A_j) - I(A_i{:}E) \right], \tag{69}$$

where the respective quantities are calculated from, e.g., the **c**q state following the purification of ϱ_{A}.

Now we can go back to the definition of K_D. As previously mentioned, it holds that $K_D(P_{d,N}^{(+)})=\log d$. To show it explicitly, on the one hand we can utilize the above bound. We know from Theorem IV.1 that $K_D(P_{d,N}^{(+)})=C_D(|\psi_{AE}^{(+)}\rangle)$, where $|\psi_{AE}^{(+)}\rangle$ is a purification of $P_{d,N}^{(+)}$ and obviously has the form $|\psi_{d,N}^{(+)}\rangle_{\mathsf{A}}|E\rangle$ with $|E\rangle$ being some state kept by Eve. Measurement of the A subsystem of $|\psi_{AE}^{(+)}\rangle$ with respect to the standard basis leads us to the ideal **c**q state $\varrho_{AE}^{(\mathrm{cq})}=\omega_{\mathsf{A}}^{(d,N)}\otimes|E\rangle\langle E|$, where

$$\omega_{\mathsf{A}}^{(d,N)}=\frac{1}{d}\sum_{i=0}^{d-1}|i\rangle\langle i|^{\otimes N}, \tag{70}$$

which has the quantities $I(A_i:A_j)=\log d(i,j=1,\ldots,N)$ and $I(A_i:E)=0(i=1,\ldots,N)$. Substituting both these facts into Eq. (68) gives us $K_D(P_{d,N}^{(+)})\geqslant\log d$.

On the other hand we can utilize the bound given in Eq. (41). Firstly, notice that $S(\rho^{\otimes n}\|\sigma^{\otimes n})=nS(\rho\|\sigma)$ for an arbitrary natural number n and arbitrary density matrices ρ and σ. Secondly, one easily finds that (see, e.g., Refs. [32])

$$S(P_{d,N}^{(+)}\|\omega_{\mathsf{A}}^{(d,N)})=\log d \tag{71}$$

and consequently the following estimate holds:

$$\begin{aligned}K_D(P_{d,N}^{(+)})&=\lim_{n\to\infty}\frac{1}{n}\inf_{\varrho_{\mathsf{A}}^{\mathrm{sep}}\in\mathcal{D}}S(P_{d,N}^{(+)\otimes n}\|\varrho_{\mathsf{A}}^{\mathrm{sep}})\\&\leqslant\lim_{n\to\infty}\frac{1}{n}S(P_{d,N}^{(+)\otimes n}\|\omega_{\mathsf{A}}^{(d,N)\otimes n})\\&=\lim_{n\to\infty}\frac{1}{n}nS(P_{d,N}^{(+)}\|\omega_{\mathsf{A}}^{(d,N)})\\&=\log d.\end{aligned} \tag{72}$$

Thus $K_D(P_{d,N}^{(+)})\leqslant\log d$ and taking into account the previously obtained inequality $K_D(P_{d,N}^{(+)})\leqslant\log d$, we infer $K_D(P_{d,N}^{(+)})=\log d$. 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 **c**q state by means of LOPC. This in turn means that the closer some particular state $\varrho_{\mathsf{AA}'}$ is to some multipartite private state, the closer is a **c**q state obtained from it to the ideal **c**q state. Then, from Theorem IV.3 it follows that the closer some **c**q state is to the ideal **c**q state, the closer are its bipartite reductions to the bipartite ideal ccq 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. (69)] 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. (68) 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. [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 $\rho_{\mathsf{AA}'}$ in their possession. In ith step each party performs the following operations:

(i) Take the state $\rho_{\mathsf{AA}'}^{(i-1)}$ (where $\rho_{\mathsf{AA}'}^{(0)}=\rho_{\mathsf{AA}'}$) and one of the remaining $k-i$ copies of $\rho_{\mathsf{AA}'}$.

(ii) Treating A part of $\rho_{\mathsf{AA}'}^{(i-1)}(\rho_{\mathsf{AA}'})$ as source (target) qubits, perform controlled NOT (CNOT) operations.

(iii) 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 $\rho_{\mathsf{AA}'}$, all the parties can distill a state $\varrho_{\mathsf{AA}'}^{(k)}$ which is closer to some multipartite private state than the initial one, i.e., $\rho_{\mathsf{AA}'}$. Quantitative analysis concerning this protocol after application to two different constructions of states may be found in Secs. V A and V B.

D. Multipartite 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 $\varrho_{\mathsf{AA}'}$ expressed in form (18), there always exists a twisting U_t that the state $\tilde{\varrho}_{\mathsf{A}}=\mathrm{Tr}_{\mathsf{A}'}(U_t\varrho_{\mathsf{AA}'}U_t^{\dagger})$ has some special form. Namely, in some chosen row (column) some of its entries are trace norms of respective blocks of $\varrho_{\mathsf{AA}'}$. We will call the state $\tilde{\varrho}_{\mathsf{A}}$ obtained in this way *privacy squeezed state*. Furthermore, we already know that twistings do not change the **c**q state with respect to some basis $\mathcal{B}_N^{\mathrm{prod}}$.

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

$$K_D(\varrho_{\mathsf{AA}'})=C_D(|\psi_{\mathsf{AA}'E}\rangle)\geqslant C_D(\varrho_{AE})\geqslant C_D(\varrho_{AE}^{(\mathrm{cq})}). \tag{73}$$

Here $\varrho_{AE}=\mathrm{Tr}_{\mathsf{A}'}|\psi_{\mathsf{AA}'E}\rangle\langle\psi_{\mathsf{AA}'E}|$ and $\varrho_{AE}^{(\mathrm{cq})}$ stands for a **c**q state obtained upon the measurement of the A subsystem in $\mathcal{B}_N^{\mathrm{prod}}$. 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., Ref. [14]), which exploit privacy squeezing to bound the secure key from below.

Theorem IV.4. Let $\varrho_{\mathsf{AA}'}$ be some N-partite state defined on $\mathcal{H}\otimes\mathcal{H}'$. Then

$$K_D(\varrho_{\mathsf{AA}'}) \geqslant C_D(\tilde{\varrho}_{\mathsf{A}E}^{(\mathbf{cq})}), \tag{74}$$

where $\tilde{\varrho}_{\mathsf{A}E}^{(\mathbf{cq})}$ is a **cq** state derived from purification $|\tilde{\varrho}_{\mathsf{A}E}\rangle$ of privacy squeezed state $\tilde{\varrho}_{\mathsf{A}}=\mathrm{Tr}_{\mathsf{A}'}(U_t\varrho_{\mathsf{AA}'}U_t^\dagger)$.

Proof. Denoting by $|\psi_{\mathsf{AA}'E}\rangle$ the purification of $\varrho_{\mathsf{AA}'}$, we have immediately from Eq. (73) that $K_D(\varrho_{\mathsf{AA}'})\geqslant C_D(\varrho_{\mathsf{A}E}^{(\mathbf{cq})})$ with $\varrho_{\mathsf{A}E}^{(\mathbf{cq})}$ standing for a **cq** state being a result of the measurement of A part in $\mathcal{B}_N^{\mathrm{prod}}$ and tracing A' part of $|\psi_{\mathsf{AA}'E}\rangle$. Then, as already stated, for any twisting U_t (in $\mathcal{B}_N^{\mathrm{prod}}$) the states $\varrho_{\mathsf{AA}'}$ and $\tilde{\varrho}_{\mathsf{AA}'}\equiv U_t\varrho_{\mathsf{AA}'}U_t^\dagger$ have the same **cq** states with respect to the basis $\mathcal{B}_N^{\mathrm{prod}}$. Consequently, $C_D(\varrho_{\mathsf{A}E}^{(\mathbf{cq})})=C_D(\sigma_{\mathsf{A}E}^{(\mathbf{cq})})$ with $\sigma_{\mathsf{A}E}^{(\mathbf{cq})}$ being a **cq** state derived from the twisted state $U_t\varrho_{\mathsf{AA}'}U_t^\dagger$ (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 $|\tilde{\psi}_{\mathsf{AA}'E}\rangle$ of the privacy squeezed state $\tilde{\varrho}_{\mathsf{A}}=\mathrm{Tr}_{\mathsf{A}'}\tilde{\varrho}_{\mathsf{AA}'}=\mathrm{Tr}_{\mathsf{A}'}(U_t\varrho_{\mathsf{AA}'}U_t^\dagger)$ we can take a "smaller" version denoted by $|\tilde{\varrho}_{\mathsf{A}E}\rangle$ (more precisely to purify some density matrix acting on $\mathcal{H}$ it suffices to use a Hilbert space of lower dimensionality than to purify a state acting on $\mathcal{H}\otimes\mathcal{H}'$). The new purification obviously must obey $\tilde{\varrho}_{\mathsf{A}}=\mathrm{Tr}_E|\tilde{\varrho}_{\mathsf{A}E}\rangle\langle\tilde{\varrho}_{\mathsf{A}E}|$. Now comparing these two situations we infer that $C_D(\sigma_{\mathsf{A}E}^{(\mathbf{cq})})\geqslant C_D(\tilde{\varrho}_{\mathsf{A}E}^{(\mathbf{cq})})$ holds, where $\tilde{\varrho}_{\mathsf{A}E}^{(\mathbf{cq})}$ is **cq** state appearing upon measurement of A subsystem of $|\tilde{\varrho}_{\mathsf{A}E}\rangle$ in $\mathcal{B}_N^{\mathrm{prod}}$. 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 $\tilde{\varrho}_{\mathsf{A}E}^{(\mathbf{cq})}$. 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. [15]. 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 $\mathcal{P}_0^{(N)}$ we shall denote a projector onto the N-partite pure state $|\psi_0^{(N)}\rangle=|0\rangle^{\otimes N}$ and $\mathcal{P}_i^{(N)}$ $(i=1,\ldots,N)$ is a projector onto the N-partite state $|\psi_i^{(N)}\rangle$, in which the ith party possesses $|1\rangle$, while other particles are in the $|0\rangle$ state. For instance $\mathcal{P}_2^{(4)}$ denotes the projector onto the four-partite pure state $|\psi_2^{(4)}\rangle=|0100\rangle$. Moreover, let $\bar{\mathcal{P}}_0^{(N)}$ and $\bar{\mathcal{P}}_i^{(N)}$ denote projectors obtained from $\mathcal{P}_0^{(N)}$ and $\mathcal{P}_i^{(N)}$, respectively, by exchanging all zeros and ones. Thus, for example $\bar{\mathcal{P}}_2^{(4)}$ is the projector onto $|\bar{\psi}_2^{(4)}\rangle=|1011\rangle$. We will denote in an analogous way by $|\psi_{ij}^{(N)}\rangle$ $(|\bar{\psi}_{ij}^{(N)}\rangle)$ an N-qubit pure state, in which ith and jth qubits are in the $|1\rangle$ $(|0\rangle)$ state and the remaining ones are in the $|0\rangle$ $(|1\rangle)$ state. Then by $\mathcal{P}_{ij}^{(N)}$ and $\bar{\mathcal{P}}_{ij}^{(N)}$ we denote projectors onto $|\psi_{ij}^{(N)}\rangle$ and $|\bar{\psi}_{ij}^{(N)}\rangle$, respectively.

Let also T_i denote the partial transposition with respect to ith 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 $\varrho_{\mathsf{AA}'}$ 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 $T_{1,\ldots,k}$.

A. 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 $\mathcal{H}_i'=\mathbb{C}^D$ $(i=1,\ldots,N)$.

Now, let us introduce the following matrix:

$$X_D^{(N)}=\frac{1}{D^N+2D-4}[(D-2)P_{D,N}^{(+)}-2P_D^{(N)}+Q_D^{(N)}], \tag{75}$$

where, as previously, $P_{D,N}^{(+)}$ 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

$$P_D^{(N)}=R_D^{(N)}-P_{D,N}^{(+)},\quad Q_D^{(N)}=\mathbb{1}_{D^N}-R_D^{(N)}, \tag{76}$$

where

$$R_D^{(N)}=\sum_{i=0}^{D-1}|i\rangle\langle i|^{\otimes N}. \tag{77}$$

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 $X_D^{(N)}$ is normalized in the trace norm.

The states under consideration are of the form

$$\varrho_{\mathsf{AA}'}^{(D,N)} = \frac{1}{\mathcal{N}_D^{(N)}}\Bigg[\sum_{i=0}^{N}(\mathcal{P}_i^{(N)} + \bar{\mathcal{P}}_i^{(N)})_{\mathsf{A}} \otimes (|X_D^{(N)T_i}|^{T_i})_{\mathsf{A}'} + (|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N})_{\mathsf{A}} \otimes (X_D^{(N)})_{\mathsf{A}'}\Bigg], \tag{78}$$

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

$$\mathcal{N}_D^{(N)} = 2\frac{(N+1)D^N + 2D - 4}{D^N + 2D - 4}. \tag{79}$$

At the beginning we need to show that the matrices $\varrho_{\mathsf{AA}'}^{(D,N)}$ 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 $\bar{\mathcal{P}}_0$ and the two off-diagonal blocks in Eq. (78) constitute a matrix of the form $\mathcal{M}_2(|X_D^{(N)}|, X_D^{(N)})$ (see Lemma A.1 for the definition of $\mathcal{M}_N$), 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 $\varrho_{\mathsf{AA}'}^{(D,N)}$ are positive. To achieve this goal, below we prove a more general lemma.

Lemma V.1. Let $X_D^{(N)}$ be defined by Eq. (75). Then the matrices $|X_D^{(N)T_k}|^{T_l}$ are positive semidefinite for all $k,l = 1,\ldots,N$.

Proof. Noticing that $R_D^{(N)}$ is diagonal for arbitrary D and N, the partial transposition of $X_D^{(N)}$ with respect to the kth subsystem may be written as $X_D^{(N)T_k} = [1/(D^N + 2D - 4)](S_D^{(N)T_k} - R_D^{(N)})$, where $S_D^{(N)}$ is defined as

$$S_D^{(N)} = \mathbb{1}_{D^N} + DP_{D,N}^{(+)} - 2R_D^{(N)}. \tag{80}$$

As we will see below $S_D^{(N)T_k}$ is positive for any $k=1,\ldots,N$ and $S_D^{(N)T_k}R_D^{(N)} = 0$. Consequently, the absolute value of $X_D^{(N)T_k}$ may be obtained by simple changing the sign before the projector $R_D^{(N)}$. To prove positivity of $S_D^{(N)T_k}$ let $|\psi\rangle = \Sigma_{i_1,\ldots,i_N}^{D-1}\alpha_{i_1\ldots i_N}|i_1\ldots i_N\rangle$ denote an arbitrary vector from $(\mathbb{C}^D)^{\otimes N}$ written in the standard basis of $(\mathbb{C}^D)^{\otimes N}$. Then we have

$$\begin{aligned}\langle\psi|S_D^{(N)T_k}|\psi\rangle &= \sum_{i\neq j}\alpha^*_{i\ldots j\ldots i}\alpha_{j\ldots i\ldots j} + \sum_{(i_1,\ldots,i_N)\in I}|\alpha_{i_1\ldots i_N}|^2 \\ &= \sum_{(i_1,\ldots,i_N)\in I_k}|\alpha_{i_1\ldots i_N}|^2 \\ &\quad + \frac{1}{2}\sum_{i\neq j}|\alpha_{i\ldots j\ldots i} + \alpha_{j\ldots i\ldots j}|^2 \geqslant 0.\end{aligned} \tag{81}$$

Here the notation $\alpha_{i\ldots j\ldots i}$ means that all indices of αs excluding the kth 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 $i_1 = \cdots = i_N$, while I_k is the set I minus all sequences in which all indices but the one on kth 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 positiveness 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 positiveness 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 lth subsystem gives

$$|X_D^{(N)T_k}|^{T_l} = \frac{1}{D^N + 2D - 4}(S_D^{(N)T_{k,l}} + R_D^{(N)}), \tag{82}$$

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

$$|X_D^{(N)T_k}|^{T_k} = \frac{1}{D^N + 2D - 4}(Q_D^{(N)} + DP_{D,N}^{(+)}), \tag{83}$$

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 (not only one-partite) subsystem is a positive matrix. This ends the proof. ■

Thus we have just proven that $\varrho_{\mathsf{AA}'}^{(D,N)}$ 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_i') of $\varrho_{\mathsf{AA}'}^{(D,N)}$ 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 $D\geqslant 3$.

Firstly, we concentrate on the positivity of all partial transpositions of $\varrho_{\mathsf{AA}'}^{(D,N)}$. To gain a better look on the problem let us consider a particular example of such a partial transposition, namely, $\varrho_{\mathsf{AA}'}^{(D,3)T_3}$. From Eq. (78) it follows that

$$\varrho_{\mathsf{AA}'}^{(D,3)T_3} = \frac{1}{\mathcal{N}_D^{(3)}} \begin{bmatrix} |X_D^{(3)}|^{T_3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & |X_D^{(3)T_3}| & 0 & 0 & 0 & 0 & X_D^{(3)T_3} & 0 \\ 0 & 0 & |X_D^{(3)T_2}|^{T_{2,3}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & |X_D^{(3)T_1}|^{T_{1,3}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & |X_D^{(3)T_1}|^{T_{1,3}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & |X_D^{(3)T_2}|^{T_{2,3}} & 0 & 0 \\ 0 & X_D^{(3)T_3} & 0 & 0 & 0 & 0 & |X_D^{(3)T_3}| & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & |X_D^{(3)}|^{T_3} \end{bmatrix}. \tag{84}$$

As, due to Lemma A.1, the square matrix consisting of two diagonal and two off-diagonal blocks of $\varrho_{\mathsf{AA}'}^{(D,N)T_i}$ [cf., Eq. (84)] i.e., the matrix $\mathcal{M}_2(|X_D^{(N)T_i}|, X_D^{(N)T_i})$, is already positive, what we need to prove is positivity of $|X_D^{(N)}|^{T_i}$ and $|X_D^{(N)T_i}|^{T_{j,k}}$ for any $i,j,k=1,\ldots,N$. Let us therefore prove the following lemma:

Lemma V.2. Let $X_D^{(N)}$ be given by Eq. (75). Then for any $i,j,k=1,\ldots,N$ it holds that

$$|X_D^{(N)}|^{T_i} \geqslant 0, \quad |X_D^{(N)T_i}|^{T_{j,k}} \geqslant 0. \tag{85}$$

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

$$|X_D^{(N)}| = \frac{1}{D^N + 2D - 4}[(D-2)P_{D,N}^{(+)} + 2P_D^{(N)} + Q_D^{(N)}]. \tag{86}$$

Application of partial transposition with respect to the ith subsystem followed by substitution of Eq. (76) leads us to

$$|X_D^{(N)}|^{T_i} = \frac{1}{D^N + 2D - 4}[\mathbb{1}_D + R_D^{(N)} + (D-4)P_{D,N}^{(+)T_i}] \tag{87}$$

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

The second fact of the lemma may be proven just by noting that by virtue of Eq. (82) it holds

$$|X_D^{(N)T_i}|^{T_{j,k}} = \frac{1}{D^N + 2D - 4}(S_D^{(N)T_{i,j,k}} + R_D^{(N)}). \tag{88}$$

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

The above lemma proves actually that all the partial transpositions $\varrho_{\mathsf{AA}'}^{(D,N)T_i}$ $(i=1,\ldots,N)$ are positive. Therefore, the states $\varrho_{\mathsf{AA}'}^{(D,N)}$ 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 $\varrho_{\mathsf{AA}'}^{(D,N)}$ for $D \geqslant 3$ has nonzero K_D. For this purpose we show that using the protocol from Sec. IV C, we can produce a state that is closer to some multipartite private state out of copies of $\varrho_{\mathsf{AA}'}^{(D,N)}$. 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. (69) strictly positive.

Application of the recursive LOCC protocol presented in Sec. IV C to k copies of $\varrho_{\mathsf{AA}'}^{(D,N)}$ gives with probability $p_{D,N}^{(k)} = 2^{k-1}\mathcal{N}_{D,N}^{(k)}/(\mathcal{N}_D^{(N)})^k$ the following state:

$$\Theta_{\mathsf{AA}'}^{(N,k)} = \frac{1}{\mathcal{N}_{D,N}^{(k)}}\Bigg[\sum_{i=0}^{N}(\mathcal{P}_i^{(N)} + \bar{\mathcal{P}}_i^{(N)}) \otimes (|X_D^{(N)T_i}|^{T_i})^{\otimes k} + (|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N}) \otimes (X_D^{(N)})^{\otimes k}\Bigg], \tag{89}$$

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

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

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

$$\tilde{\Theta}_{\mathsf{A}}^{(N,k)} = \frac{1}{\mathcal{N}_{D,N}^{(k)}}\Bigg[\sum_{i=0}^{N}(\mathcal{P}_i^{(N)} + \bar{\mathcal{P}}_i^{(N)})\||X_D^{(N)T_i}|^{T_i}\|_1^k + (|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N})\|X_D^{(N)}\|_1^k\Bigg]. \tag{91}$$

In other words, after "rotation" with $U_t^{(k)}$ 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.4 that the distillable key of the **cq** state obtained from the privacy squeezed state $\tilde{\Theta}_{\mathsf{A}}^{(N,k)}$ (measurement is performed in the same basis as twisting) cannot be greater than the distillable key of $\Theta_{\mathsf{AA}'}^{(N,k)}$.

From Eq. (90) it follows that since $D^N + 2D - 4 > D^N$ for any $D \geqslant 3$ one has $\mathcal{N}_{D,N}^{(k)} \to 2$, while for $D=2$, $\mathcal{N}_{2,N}^{(k)} \to 2(N$

+1). In turn this means that for the off-diagonal elements of $\widetilde{\Theta}_{\mathsf{A}}^{(N,k)}$ one has that

$$\frac{1}{\mathcal{N}_{D,N}^{(k)}}\|X_D^{(N)}\|_1^k = \frac{1}{\mathcal{N}_{D,N}^{(k)}} \xrightarrow{k\to\infty} \frac{1}{2} \tag{92}$$

with $D\geqslant 3$. By virtue of Theorem III.3 one infers that the more copies of $\varrho_{\mathsf{AA}'}^{(D,N)}$ we put into the recurrence protocol, the closer we are to some multipartite private state. This also means that with $k\to\infty$ the sequence of states $\widetilde{\Theta}_{\mathsf{A}}^{(N,k)}$ goes to GHZ state $P_{2,N}^{(+)}$, however, for $D\geqslant 3$.

Now, to bound from below the distillable key of $\Theta_{\mathsf{AA}'}^{(N,k)}$ according to the prescription given above we need to calculate a **c**q state of the privacy squeezed state $\widetilde{\Theta}_{\mathsf{A}}^{(N,k)}$. (The **c**q state is found here with respect to the basis in which the original state is defined.) Simple algebra gives

$$\widetilde{\Theta}_{\mathsf{AE}}^{(\mathbf{cq})} = \frac{1}{\mathcal{N}_{D,N}^{(k)}}\Bigg[R_2^{(N)}\otimes|E_0\rangle\langle E_0| + \left(\frac{D^N}{D^N+2D-4}\right)^k \times\sum_{j=1}^{N}\left(P_j^{(N)}\otimes|E_j\rangle\langle E_j| + \bar{P}_j^{(N)}\otimes|\bar{E}_j\rangle\langle\bar{E}_j|\right)\Bigg], \tag{93}$$

where $|E_0\rangle$, $|E_j\rangle$, and $|\bar{E}_j\rangle$ constitute a set of orthonormal states held by Eve. One notices immediately that $\widetilde{\Theta}_{\mathsf{AE}}^{(\mathbf{cq})}$ tends to the multipartite ideal **c**q state [see Eq. (2)] for any integer $D\geqslant 3$ whenever $k\to\infty$.

To find a lower bound on distillable key of $\widetilde{\Theta}_{\mathsf{A}}^{(N,k)}$ 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 $\Theta_{\mathsf{AE}}^{(\mathbf{cq})}$. Fortunately, the initial states $\varrho_{\mathsf{AA}'}^{(D,N)}$ have such symmetrical structure, preserved by the recurrence protocol and the privacy squeezing, which 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:

$$K_D(\Theta_{\mathsf{AA}'}^{(N,k)}) \geqslant I(A_1{:}A_2)(\Theta_{A_1A_2E}^{(\mathrm{ccq})}) - I(A_1{:}E)(\Theta_{A_1A_2E}^{(\mathrm{ccq})}), \tag{94}$$

irrespectively of number of parties N. Exemplary behavior 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. 1(a).

It is clear from Fig. 1(a) that it is possible to distill one secure bit of key from bound entangled states $\Theta_{\mathsf{AA}'}^{(N,k)}$ for sufficiently large k. For comparison, Fig. 1(b) 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 $\varrho_{\mathsf{AA}'}^{(D,N)}$. However, in this case we need to take into account the probability $p_{D,N}^{(k)}$. In this way we arrive at

$$K_D(\varrho_{\mathsf{AA}'}^{(D,N)}) \geqslant p_{D,N}^{(k)}[I(A_1{:}A_2)(\Theta_{A_1A_2E}^{(\mathrm{ccq})}) - I(A_1{:}E)(\Theta_{A_1A_2E}^{(\mathrm{ccq})})]. \tag{95}$$

Figure 2(a) presents exemplary behavior of the function appearing on the right-hand side of Eq. (95) (denoted by $\widetilde{K}_{DW}$) for $N=3$. For comparison, in Fig. 2(b) it is also plotted the same function in the case of $N=2$ (this case was discussed in Ref. [27]).

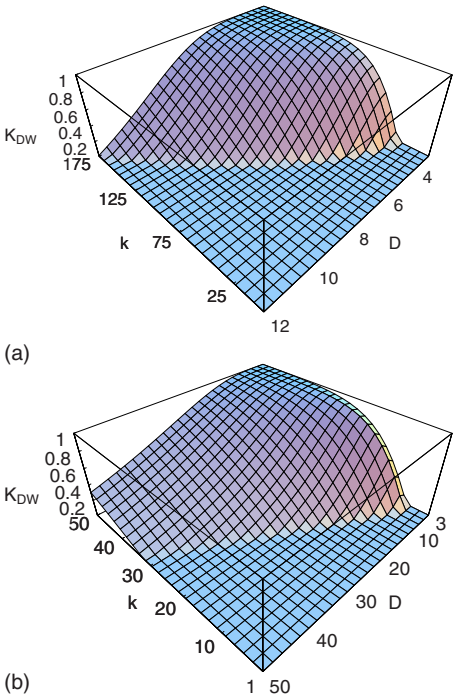

FIG. 1. (Color online) An exemplary plot of $K_{DW} \equiv I(A_1{:}A_2)(\Theta_{A_1A_2E}^{(\mathrm{ccq})}) - I(A_1{:}E)(\Theta_{A_1A_2E}^{(\mathrm{ccq})})$ with $N=3$ (a) and for comparison in the case of $N=2$ (b), which was discussed in Ref. [27]. For the sake of clarity, zero is put whenever the plotted 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 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}.

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 wether 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 $|Z_D^{(N)T_i}|^{T_i}$ 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. Other crucial conditions are $|Z_D^{(N)T_i}|^{T_i}\geqslant 0$ and $|Z_D^{(N)}|^{T_i}\geqslant 0$ for all $i=1,\ldots,N$. The first one is necessary for $\varrho_{\mathsf{AA}'}^{(D,N)}$ (when constructed with the matrix $Z_D^{(N)}$) to be positive, while the second one allows to prove that $\varrho_{\mathsf{AA}'}^{(D,N)}$ have positive partial transposition with respect to any elementary subsystem.

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

(i) $\|Z_D^{(N)}\|_1 > \||Z_D^{(N)T_i}|^{T_i}\|_1$ for all $i=1,\ldots,N$,

(ii) $|Z_D^{(N)T_i}|^{T_i}\geqslant 0$ for all $i=1,\ldots,N$,

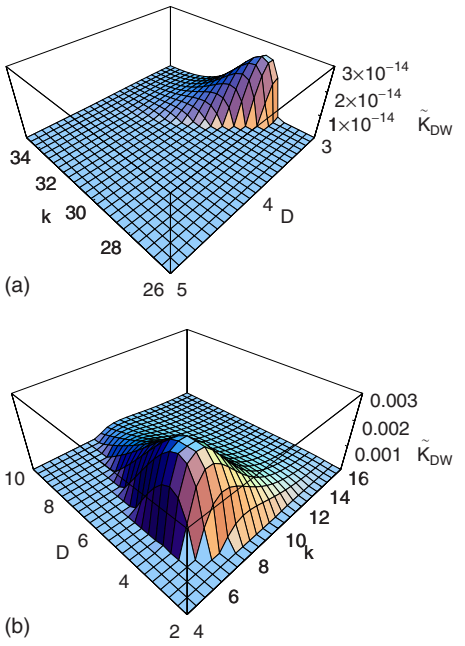

FIG. 2. (Color online) An exemplary plot of $\tilde{K}_{DW} \equiv p^{(k)}_{D,3}[I(A_1:A_2)(\Theta^{(\mathrm{ccq})}_{A_1A_2E}) - I(A_1:E)(\Theta^{(\mathrm{ccq})}_{A_1A_2E})]$ with $N=3$. For comparison it is also presented for the case with $N=2$ (b). For the sake of clarity, zero is put whenever the plotted function is less or equal to zero. Also, though both the parameters k and D are integer, for convenience, the function $\tilde{K}_{DW}$ is plotted as if it were a function of continuous k and D. It is clear that for $N=3$ the lower bound on distillable key is considerably smaller.

(iii) $|Z_D^{(N)}|^{T_i} \geqslant 0$ for all $i=1,\ldots,N$,

are satisfied. Then $Z_D^{(N)} \ngeqslant 0$ and $Z_D^{(N)T_i} \ngeqslant 0$ for all $i=1,\ldots,N$.

Proof (ad absurdum). We divide the proof into three parts.

(i) Assume that $Z_D^{(N)} \geqslant 0$ and $Z_D^{(N)T_i} \ngeqslant 0$ for any $i=1,\ldots,N$. Then one can see that $|Z_D^{(N)}|^{T_i} = Z_D^{(N)T_i} \ngeqslant 0$ for any choice of i. However, this contradicts the third assumption.

(ii) Assume that $Z_D^{(N)} \ngeqslant 0$ and there exists such k that $Z_D^{(N)T_k} \geqslant 0$. Now, one obtains $|Z_D^{(N)T_k}|^{T_k} = Z_D^{(N)} \ngeqslant 0$. Of course, this is in contradiction to the second assumption.

(iii) Finally, assume that $Z_D^{(N)} \geqslant 0$ and that there exists such k that $Z_D^{(N)T_k} \geqslant 0$. Then $\| |Z_D^{(N)T_k}|^{T_k} \|_1 = \| Z_D^{(N)} \|_1$. This contradicts the first assumption. ■

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. 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

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

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 $M_{D^N}(\mathbb{C})$ and therefore

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

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 Sec. IV C 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 $\omega_k = e^{2\pi i k/D}$ ($k=0,\ldots,D-1$). It is then clear that $\tilde{V}_D$ is a unitary matrix for any $D \geqslant 2$, 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 kth 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:

$$\tilde{\varrho}^{(D,N)}_{\mathsf{AA}'} = \frac{1}{\tilde{\mathcal{N}}_D^{(N)}} \Bigg[\sum_{j=0}^{N} (\mathcal{P}_j^{(N)} + \bar{\mathcal{P}}_j^{(N)}) \otimes \sum_{i=1}^{N} |\tilde{X}_{D,i}^{(N)T_j}| + |0\rangle\langle 1|^{\otimes N} \otimes \sum_{i=1}^{N} \tilde{X}_{D,i}^{(N)} + |1\rangle\langle 0|^{\otimes N} \otimes \sum_{i=1}^{N} \tilde{X}_{D,i}^{(N)\dagger} \Bigg], \tag{98}$$

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

$$\tilde{\mathcal{N}}_D^{(N)} = 2N \left(D + N \sum_{i,j=0}^{D-1} |u_{ij}| \right). \tag{99}$$

Obviously for $\tilde{X}_D^{(N)}$ 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 $\tilde{\mathcal{N}}_D^{(N)} = 2ND(1 + N\sqrt{D})$.

As in the case of the first construction, we need to prove that $\tilde{\varrho}^{(D,N)}_{\mathsf{AA}'}$ 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 $\tilde{\varrho}^{(D,N)}_{\mathsf{AA}'}$ one has to show that the inequalities

$$\left|\sum_{i=1}^{N}\widetilde{X}_{D,i}^{(N)}\right| \leqslant \sum_{i=1}^{N}|\widetilde{X}_{D,i}^{(N)}| \tag{100}$$

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

To deal with the problem of positivity of partial transpositions let us look on the particular example of form of $\widetilde{\varrho}_{\mathsf{AA}'}^{(D,3)T_3}$. From Eq. (98) one infers that

$$\widetilde{\varrho}_{\mathsf{AA}'}^{(D,3)T_3} = \frac{1}{\widetilde{\mathcal{N}}_D^{(3)}}\begin{bmatrix}
\sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)}| & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)T_3}| & 0 & 0 & 0 & 0 & \sum_{i=1}^{3}\widetilde{X}_{D,i}^{(3)T_3} & 0 \\
0 & 0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)T_2}| & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)T_1}| & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)T_1}| & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)T_2}| & 0 & 0 \\
0 & \sum_{i=1}^{3}\widetilde{X}_{D,i}^{(3)T_3\dagger} & 0 & 0 & 0 & 0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)T_3}| & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \sum_{i=1}^{3}|\widetilde{X}_{D,i}^{(3)}|
\end{bmatrix}, \tag{101}$$

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

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

Lemma V.4. Let $\widetilde{X}_D^{(N)}$ be defined as in Eq. (96). Then the following equalities hold:

$$\left|\sum_{i=1}^{N}\widetilde{X}_{D,i}^{(N)T_j}\right| \leqslant \sum_{i=1}^{N}|\widetilde{X}_{D,i}^{(N)T_j}| \quad (j=0,\ldots,N). \tag{102}$$

Proof. Firstly we start by the above statement for $j=0$. For this purpose let us notice that its left-hand side may be written as

$$\left|\sum_{i=1}^{N}\widetilde{X}_{D,i}^{(N)}\right| = \left|N\sum_{k=0}^{D-1}u_{kk}|k\rangle\langle k|^{\otimes N} + \sum_{i=1}^{N}\sum_{\substack{k,l=0\\k\neq l}}^{D-1}u_{kl}(|k\rangle\langle l|^{\otimes N})^{T_i}\right|. \tag{103}$$

Straightforward algebra shows that both terms under the sign of absolute value are defined on orthogonal supports. Moreover, all the partial transpositions in the second term are defined on orthogonal supports. Both these facts allow us to write

$$\left|\sum_{i=1}^{N}\widetilde{X}_{D,i}^{(N)}\right| = N\sum_{k,l=0}^{D-1}|u_{kl}||l\rangle\langle l|^{\otimes(i-1)}\otimes|k\rangle\langle k|\otimes|l\rangle\langle l|^{\otimes(N-i-1)}. \tag{104}$$

One finds immediately that this equals the right-hand side of Eq. (102), finishing the first part of the proof.

To show Eq. (102) for $j=1,\ldots,N$ we need to perform a little bit more sophisticated analysis. With the same reasoning as in the case of the first inequality we can reduce the claimed inequalities to the following:

$$\left|\widetilde{X}_D^{(N)} + (N-1)\sum_{k=0}^{D-1}u_{kk}|k\rangle\langle k|^{\otimes N}\right| \leqslant R_D^{(N)} + (N-1)\sum_{k=0}^{D-1}|u_{kk}||k\rangle\langle k|^{\otimes N}, \tag{105}$$

where we utilized Eq. (97). One notices that the above inequality may be further reduced to

$$|U_D + (N-1)\mathcal{D}| \leqslant \mathbb{1}_D + (N-1)|\mathcal{D}|, \tag{106}$$

where $\mathcal{D}$ denotes a diagonal matrix containing the diagonal elements of U_D. Utilizing the fact that $|u_{ij}| = 1/\sqrt{D}$ for any $i,j = 0,\ldots,D-1$, we infer that $|\mathcal{D}| = (1/\sqrt{D})\mathbb{1}_D$ and therefore

$$|U + (N-1)\mathcal{D}| \leqslant [1 + (N-1)/\sqrt{D}]\mathbb{1}_D. \tag{107}$$

To prove this inequality we can utilize the polar decomposition to its left-hand side. More precisely we can write $|U+(N-1)\mathcal{D}| = V^\dagger U + (N-1)V^\dagger\mathcal{D}$ with V denoting some unitary matrix. This allows us to write

$$\begin{aligned}\langle\Psi||U + (N-1)\mathcal{D}||\Psi\rangle &= |\langle\Psi||U + (N-1)\mathcal{D}||\Psi\rangle| \\ &\leqslant |\langle\Psi|V^\dagger U|\Psi\rangle| + (N-1)|\langle\Psi|V^\dagger\mathcal{D}|\Psi\rangle| \\ &\leqslant 1 + (N-1)|\langle\Psi|V^\dagger|\mathcal{D}|W|\Psi\rangle| \\ &\leqslant 1 + \frac{N-1}{\sqrt{D}},\end{aligned} \tag{108}$$

where $|\Psi\rangle$ is an arbitrary normalized vector from $\mathbb{C}^D$. The second and third inequalities 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 $|\langle\psi|U|\psi\rangle| \leqslant 1$. Moreover, we put here the polar decomposition of $\mathcal{D}$, i.e., $\mathcal{D} = |\mathcal{D}|W$ with some unitary W. The last inequality is also a result of application of aforementioned fact that $|\mathcal{D}| = (1/\sqrt{D})\mathbb{1}_D$.

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 $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$ represent quantum states for any $D \geqslant 2$ and $N \geqslant 2$, 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 $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$ is nonzero. This would also imply that $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$ represent entangled states.

Let us then apply the recursive protocol described previously in Sec. IV C to k copies of $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$, obtaining

$$\begin{aligned}\tilde{\Theta}_{\mathsf{AA}'}^{(N,k)} = \frac{1}{\tilde{\mathcal{N}}_{D,N}^{(k)}}\Bigg[\sum_{j=0}^{N}(\mathcal{P}_j^{(N)} + \bar{\mathcal{P}}_j^{(N)}) \otimes \left(\sum_{i=1}^{N}|\tilde{X}_{D,i}^{(N)T_j}|\right)^{\otimes k} + |0\rangle\langle 1|^{\otimes N} \\ \otimes \left(\sum_{i=1}^{N}\tilde{X}_{D,i}^{(N)}\right)^{\otimes k} + |1\rangle\langle 0|^{\otimes N} \otimes \left(\sum_{i=1}^{N}\tilde{X}_{D,i}^{(N)\dagger}\right)^{\otimes k}\Bigg],\end{aligned} \tag{109}$$

with the normalization factor given by

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

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

$$\tilde{p}_{D,N}^{(k,1)} = 2^{k-1}\tilde{\mathcal{N}}_{D,N}^{(k)}/(\tilde{\mathcal{N}}_{D,N}^{(1)})^k, \tag{111}$$

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

$$\tilde{p}_{D,N}^{(k,2)} = \tilde{\mathcal{N}}_{D}^{(N)}/(\tilde{\mathcal{N}}_{D}^{(N)})^k. \tag{112}$$

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

$$\begin{aligned}\tilde{\theta}_{\mathsf{A}}^{(N,k)} = \frac{1}{\tilde{\mathcal{N}}_{D,N}^{(k)}}\Bigg[\sum_{j=0}^{N}(\mathcal{P}_j^{(N)} + \bar{\mathcal{P}}_j^{(N)})\left\|\sum_{i=1}^{N}|\tilde{X}_{D,i}^{(N)T_j}|\right\|_1^k \\ + (|0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N})\left\|\sum_{i=1}^{N}\tilde{X}_{D,i}^{(N)}\right\|_1^k\Bigg].\end{aligned} \tag{113}$$

Calculating the respective norms in the above, one may rewrite Eq. (113) as

$$\begin{aligned}\tilde{\theta}_{\mathsf{A}}^{(N,k)} = \frac{D^k}{\tilde{\mathcal{N}}_{D,N}^{(k)}}\Bigg[2(N\sqrt{D})^k P_{2,N}^{(+)} \\ + [1 + (N-1)\sqrt{D}]^k\sum_{j=1}^{N}(\mathcal{P}_j^{(N)} + \bar{\mathcal{P}}_j^{(N)})\Bigg].\end{aligned} \tag{114}$$

From Eqs. (110) and (114) one easily infers that $\tilde{\theta}_{\mathsf{A}}^{(N,k)} \to P_{2,N}^{(+)}$ for $k \to \infty$ for any $D \geqslant 2$, which by virtue of Theorem III.3 means that the recursive protocol when applied to copies of $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$ produces a state that is arbitrarily close to some multipartite pdit in the limit of $k \to \infty$. 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 $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$. Below we provide also plots of lower bounds on K_D of $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$.

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

$$\begin{aligned}\tilde{\Theta}_{A\bar{E}}^{(\mathbf{cq})} = a_{D,N}^{(k)}R_2^{(N)} \otimes |E_0\rangle\langle E_0| + b_{D,N}^{(k)} \\ \times\sum_{j=1}^{N}(\mathcal{P}_j^{(N)} \otimes |E_j\rangle\langle E_j| + \bar{\mathcal{P}}_j^{(N)} \otimes |\bar{E}_j\rangle\langle\bar{E}_j|),\end{aligned} \tag{115}$$

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

$$a_{D,N}^{(k)} = \frac{(ND\sqrt{D})^k}{\tilde{\mathcal{N}}_{D,N}^{(k)}} \tag{116}$$

and

$$b_{D,N}^{(k)} = \frac{D^k}{\tilde{\mathcal{N}}_{D,N}^{(k)}}[1 + (N-1)\sqrt{D}]^k. \tag{117}$$

One can see from above that the limit of $k \to \infty$ leads us to the ideal **c**q state. Now we can apply the bound given in Eq. (69). It is easy to verify that all the quantities $I(A_i{:}A_j)$ are

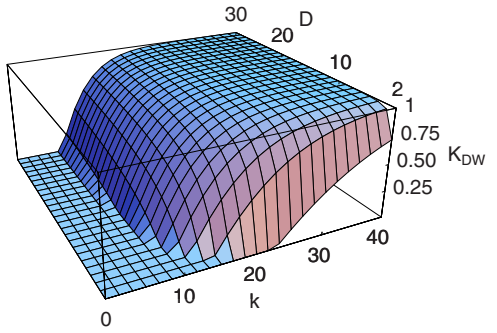

FIG. 3. (Color online) The function appearing on the right-hand side of Eq. (118) (denoted here by K_{DW}) in the function of number of copies k and the dimension D. Zero is put whenever the function is less than zero. Notice that both the parameters k and D are discrete; however, continuous plot is made to indicate better the behavior of K_{DW}. It is clear from the plot that for larger k the distillable key of $\tilde{\theta}_{\mathrm{A}}^{(\mathcal{N},k)}$ approaches one bit (this is actually a maximal value obtainable from two-qubit states) and the convergence depends on D. Namely, for higher dimensions D the convergence to the maximal value is faster.

equal here [the same holds for $I(A_i{:}E)$] and therefore we can rewrite Eq. (69) as

$$K_D(\tilde{\Theta}_{\mathsf{AA}}^{(N,k)}) \geqslant I(A_1{:}A_2)(\tilde{\Theta}_{A_1A_2E}^{(\mathrm{ccq})}) - I(A_1{:}E)(\tilde{\Theta}_{A_1A_2E}^{(\mathrm{ccq})}). \tag{118}$$

Exemplary plot of the function appearing on the right-hand side of Eq. (118) (denoted as K_{DW}) is presented in Fig. 3.

The behavior of K_{DW} (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 $\tilde{\Theta}_{\mathsf{AA}'}^{(N,k)}$.

We can also get a lower bound on distillable key of the initial states $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$. 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 $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$ are

$$K_D^{(1(2))}(\tilde{\varrho}_{\mathsf{AA}}^{(D,N)}) \geqslant \tilde{p}_{D,N}^{(k,1(2))}[I(A_1{:}A_2)(\tilde{\Theta}_{A_1A_2E}^{(\mathrm{ccq})}) - I(A_1{:}E)(\tilde{\Theta}_{A_1A_2E}^{(\mathrm{ccq})})]. \tag{119}$$

Exemplary plots of the right-hand side of the above (denoted by $\tilde{K}_{DW}^{(1(2))}$) both in the case of a unitary Hermitian matrix (e.g., $\tilde{V}_2^{\otimes k}$) and only a unitary matrix (e.g., $\tilde{V}_D$) are given in Figs. 4(a) and 4(b).

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.

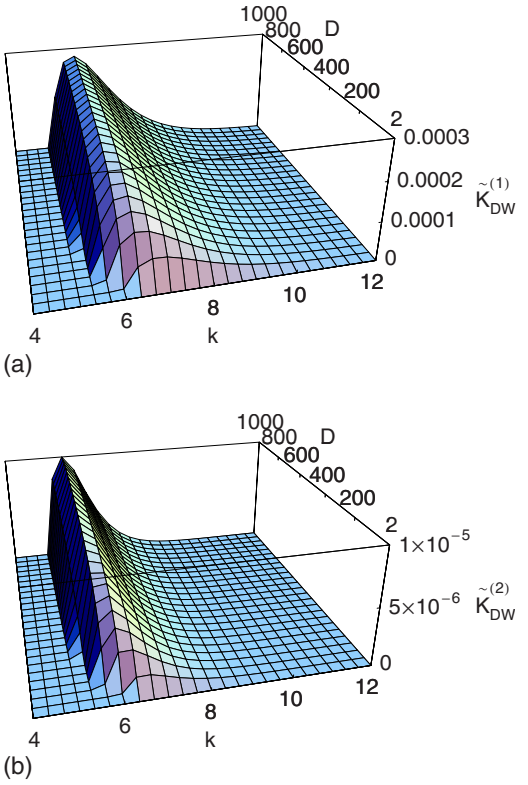

FIG. 4. (Color online) Lower bounds on K_D of $\tilde{\varrho}_{\mathsf{AA}'}^{(D,N)}$ in the function of k and D. The upper plot (a) presents lower bound (denoted here by $\tilde{K}_{DW}^{(1)}$) on K_D in the case of unitary Hermitian matrices U_D, while in the second plot (b) lower bound ($\tilde{K}_{DW}^{(2)}$) in the case of unitary but not Hermitian matrices is given. Both are just a product of probability $\tilde{p}_{D,N}^{(k1)}$ (left) or $\tilde{p}_{D,N}^{(k,2)}$ (right) and K_{DW} plotted in Fig. 3. One infers that in the case of unitary but not Hermitian matrix U_D, the region of nonzero values of the plotted function is wider than in the case of unitary Hermitian matrices.

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],

$$\varrho^S = \frac{1}{4}\sum_{i=0}^{3} |\psi_i^B\rangle\langle\psi_i^B| \otimes |\psi_i^B\rangle\langle\psi_i^B|, \tag{120}$$

where $|\psi_i^B\rangle$ ($i=0,\ldots,3$) are the so-called Bell states given by $|\psi_{0(1)}^B\rangle=(1/\sqrt{2})(|01\rangle \pm |10\rangle)$ and $|\psi_{2(3)}^B\rangle=(1/\sqrt{2})(|00\rangle \pm |11\rangle)$. This conclusion may be also inferred for the generalizations of the Smolin state provided in Ref. [35] and independently in Ref. [36] (see also Ref. [37] for further generalizations). These are states of the form

$$\varrho_2 = |\psi_0^B\rangle\langle\psi_0^B|,$$

$$\varrho_4^S = \frac{1}{4}\sum_{m=0}^{3} U_2^{(m)}\varrho_2 U_2^{(m)\dagger} \otimes U_2^{(m)}\varrho_2 U_2^{(m)\dagger} \equiv \varrho^S,$$

$$\varrho_6^S = \frac{1}{4}\sum_{m=0}^{3} U_4^{(m)} \varrho_4 U_4^{(m)\dagger} \otimes U_2^{(m)} \varrho_2 U_2^{(m)\dagger},$$

$$\vdots$$

$$\varrho_{2(n+1)}^S = \frac{1}{4}\sum_{m=0}^{3} U_{2n}^{(m)} \varrho_{2n} U_{2n}^{(m)\dagger} \otimes U_2^{(m)} \varrho_2 U_2^{(m)\dagger}, \quad (121)$$

with $U_k^{(m)} = \mathbb{1}_2^{\otimes(k-1)} \otimes \sigma_m$ $(m=0,\ldots,3$ and $k=2,\ldots)$, where σ_m $(m=1,2,3)$ denote the usual Pauli matrices and $\sigma_0 = \mathbb{1}_2$. The state ϱ_2 is just one of the Bell states, while ϱ_4^S is the Smolin state. All states ϱ_{2n} for $n \geqslant 2$ are bound entangled and for suitable choice of local observables all states for $n \geqslant 1$ violate the Bell inequality

$$|E_{1\cdots 11} + E_{1\cdots 12} + E_{2\cdots 21} - E_{2\cdots 22}| \leqslant 2 \quad (122)$$

maximally (E denotes the so-called correlation function, i.e., an average of products of local measurement outcomes taken over many runs of experiment). In fact very recently the state ϱ^S (120) have been realized in laboratory as a first experimental realization of bound entanglement [38]. The prediction [33] that they violate the above Bell inequality has been fully confirmed in this experiment. On the other hand, due to the results of Refs. [5,6,30], one may show that it is impossible to distill multipartite secure key from states ϱ_{2n}^S for $n \geqslant 2$. This shows that bipartite 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 [39] 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. [40,41], where it was shown that violation of some Bell inequalities is sufficient condition for security of multipartite secret sharing protocols [42] 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 a nontrivial task. 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, the minimal dimension of elementary system of PPT like bound entangled state that allows one-way secure key distillation is not known. Does it increase with number of particles and if so, how does the dependence look like? Are there bound entangled states with multipartite cryptographic key with underlying structure corresponding to other classes of pure states such as graph states (see Ref. [43])? 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 approximated p-dit which is bound entangled)? If it were so, the two parts might serve as natural measures of free and bound entanglement in the system. Most likely this is impossible, but one needs a proof. The closely related question is the one concerning lockability of the secure key K_D (note that nonadditivity of K_D has been proved very recently in Ref. [44]). While this seems to be a very hard question in case of bipartite states (though lockability with respect to Eve has already been ruled out in Ref. [19]) it may happen to be easier within the multipartite paradigm presented here (in analogy to classical bound information which is known only in asymptotic bipartite form [45] but naturally emerges form bound entanglement in multipartite case [46]). In this context novel upper and lower bounds on K_D are needed (for recent development see Ref. [47]). 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 multicoordinate extensions to help in characterization of multipartite entanglement seems to be rich program for future research.

Here we have been aiming at general question of two-way distillability, combining then one-way and two-way schemes together. One could, however, perform deep analysis focusing solely on one-way schemes trying for instance to prove bounds as such proved in Ref. [25]. 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. [48–50]). For instance, it was shown in Ref. [51] that the generalized version of the protocol from Ref. [48] does not allow for secure key distillation from bound entangled states. It seems that within the multipartite scenario the problem could be a little simpler as one can have bound entangled multipartite states with some of its partitions being still having nonpositive partial transposition.

Needless to say due to Choi-Jamiołkowski isomorphism [52] 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.

APPENDIX: SOME USEFUL LEMMAS

Lemma A.1. Assume that a given $d\times d$ matrix B is normal. If $A\geqslant|B|$ then the matrices

$$\mathcal{M}_N(A,B)=\begin{bmatrix}(N-1)A & B & \dots & B\\ B^\dagger & (N-1)A & \dots & B\\ \vdots & \vdots & \ddots & \vdots\\ B^\dagger & B^\dagger & \dots & (N-1)A\end{bmatrix} \tag{A1}$$

and

$$\tilde{\mathcal{M}}_N(A,B)=\begin{bmatrix}(N-1)A & B & B & \dots & B\\ B^\dagger & A & 0 & \dots & 0\\ B^\dagger & 0 & A & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ B^\dagger & 0 & 0 & \dots & A\end{bmatrix} \tag{A2}$$

are positive.

Proof. We prove the lemma only for $\mathcal{M}_N(A,B)$ as the proof for $\tilde{\mathcal{M}}_N(A,B)$ goes along the same lines.

The matrix $\mathcal{M}_N(A,B)$ consists of N^2 blocks $d\times d$ each and consequently the whole matrix has the dimensions $Nd\times Nd$. Thus to prove positiveness we need to show that for any $|\Psi\rangle\in\mathbb{C}^{Nd}$ the inequality $\langle\Psi|\mathcal{M}_N(A,B)|\Psi\rangle\geqslant 0$ holds. It is clear that an arbitrary vector $|\Psi\rangle\in\mathbb{C}^{Nd}$ may be written as

$$|\Psi\rangle=\begin{bmatrix}|x_1\rangle\\ \vdots\\ |x_N\rangle\end{bmatrix}, \tag{A3}$$

where each $|x_i\rangle$ belongs to $\mathbb{C}^d$. Then a rather straightforward algebra leads to

$$\langle\Psi|\mathcal{M}_N(A,B)|\Psi\rangle=(N-1)\sum_{i=1}^{N}\langle x_i|A|x_i\rangle+2\sum_{\substack{i,j=1\\ i<j}}^{N}\mathrm{Re}\langle x_i|B|x_j\rangle. \tag{A4}$$

By virtue of the assumption that $A\geqslant|B|$ and the inequality $\mathrm{Re}z\geqslant-|z|$ satisfied for any $z\in\mathbb{C}$, one has

$$\langle\Psi|\mathcal{M}_N(A,B)|\Psi\rangle\geqslant(N-1)\sum_{i=1}^{N}\langle x_i\|B\|x_i\rangle-2\sum_{\substack{i,j=1\\ i<j}}^{N}|\langle x_i|B|x_j\rangle|, \tag{A5}$$

Since B is assumed to be a normal matrix it may be given as $B=\Sigma_k\lambda_k|\varphi_k\rangle\langle\varphi_k|$ with $\{\lambda_k\}$ being, in general, the complex eigenvalues of B, while $\{|\varphi_k\rangle\}$ its orthonormal eigenvectors. Putting the spectral decomposition of B into Eq. (A5), introducing $a_{ik}=|\langle x_i|\varphi_k\rangle|\geqslant 0$, and taking into account the fact that $|\Sigma_i\xi_i|\leqslant\Sigma_i|\xi_i|$, we obtain

$$\langle\Psi|\mathcal{M}_N(A,B)|\Psi\rangle\geqslant\sum_k|\lambda_k|\left(\sum_{i=1}^{N}a_{ik}^2-2\sum_{\substack{i,j=1\\ i<j}}^{N}a_{ik}a_{jk}\right). \tag{A6}$$

It is clear from Eq. (A6) that to show non-negativity of $\langle\Psi|\mathcal{M}_N(A,B)|\Psi\rangle$ for any $|\Psi\rangle\in\mathbb{C}^{Nd}$, one has to prove that for all k the term in brackets in Eq. (A6) is non-negative. This, however, follows from the fact that

$$\sum_{\substack{i,j=1\\ i<j}}^{N}(a_{ik}-a_{jk})^2\geqslant 0, \tag{A7}$$

finishing the proof. ■

Lemma A.2. Let $A=\Sigma_{i,j=0}^{d-1}a_i^j|i\rangle\langle j|$ be a positive matrix obeying $\mathrm{Tr}A\leqslant 1$. Assume that each element of A lying in ith row (and ith column due to hermiticity of A) is close to $1/d$ in the sense that it obeys $|a_i^j-1/d|\leqslant\epsilon$ for some $1/d>\epsilon>0$. Then $|a_i^j-1/d|\leqslant\eta(\epsilon)$ for any $i,j=0,\dots,d-1$, 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

$$\begin{bmatrix}a_0^0 & a_0^j\\ a_0^{j*} & a_j^j\end{bmatrix} \tag{A8}$$

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

$$\left|a_j^j-\frac{1}{d}\right|\leqslant\alpha(\epsilon) \tag{A9}$$

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 $A\geqslant 0$ one has that the following matrices:

$$\begin{bmatrix}a_0^0 & a_0^i & a_0^j\\ a_0^{i*} & a_i^i & a_i^j\\ a_0^{j*} & a_i^{j*} & a_j^j\end{bmatrix}\quad(0<i<j), \tag{A10}$$

are also positive. Since we can now say that all elements in the first row (and column) and all the diagonal elements obey Eq. (A9), it follows, after some technical calculations, that a_i^j 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

$$\left| a_i^j - \frac{1}{d} \right| \leqslant \eta(\epsilon) \quad (i,j = 0, \ldots, d-1) \tag{A11}$$

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 ϵs. Then, however, we can take the largest one. ■

[1] C. H. Bennett and G. Brassard, in *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December, 1984, (IEEE Computer Society Press, New York, 1984), pp. 175–179.

[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. London, Ser. 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, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[14] K. Horodecki, Ph.D thesis, University of Warsaw, Warsaw, Poland, 2008.

[15] P. Horodecki and R. Augusiak, in *Quantum Information Processing: From Theory to Experiment*, edited by D. G. Angelakis, M. Christandl, A. Ekert, M. Kay, and S. Kulik, NATO Advances Studies Institutes Series F: Computer and Systems Sciences (IOS Press, Amsterdam, 2006), Vol. 199, pp. 19–29.

[16] K. Horodecki, Ł. 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 and J.-Ch. Boileau, Phys. Rev. A **78**, 032335 (2008).

[19] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Theory of Cryptography*, Proceedings of the Fourth Theory of Cryptography Conference, edited by S. P. Vadhan, Lecture Notes in Computer Science Vol. 4392 (Springer, Berlin, 2007), pp. 456–478.

[20] G. Smith and J. Yard, Science **321**, 1812 (2008).

[21] R. Renner, Int. J. Quantum Inf. **6**, 1 (2008).

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

[23] R. Renner and R. König, in *Theory of Cryptography*, Proceedings of the Second Theory of Cryptography Conference, edited by J. Kilian, Lecture Notes in Computer Science Vol. 3378 (Springer, Berlin, 2005), pp. 407–425.

[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, and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).

[26] R. Augusiak, Ph.D. thesis, Gdańsk University of Technology, 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 *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dodrecht, 1989).

[29] M. Horodecki, Quantum Inf. Comput. **1**, 3 (2001).

[30] P. Horodecki, in *Lectures on Quantum Information*, edited by D. Bruss and G. Leuchs (Wiley-VCH Verlag, Weinheim, 2007), p. 209.

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

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

[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] E. Amselem and M. Bourennane, Nat. Phys. **5**, 748 (2009).

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

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

[41] A. Sen(De), U. Sen, and M. Żukowski, Phys. Rev. A **68**, 032309 (2003).

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

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

[44] K. Li, A. Winter, X.-B. Zou, G.-C. Guo, e-print arXiv:0903.4308.

[45] R. Renner and S. Wolf, in *Towards Proving the Existence of "Bound" Information*, Proceedings of 2002 IEEE International Symposium on Information Theory (IEEE) (Lausanne, Switzerland, 2002), p. 103.

[46] A. Acín, J. I. Cirac, and Ll. Masanes, Phys. Rev. Lett. **92**,

107903 (2004).
[47] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, IEEE Trans. Inf. Theory **55**, 3375 (2009).
[48] 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).
[49] J. Rigas, O. Gühne, and N. Lütkenhaus, Phys. Rev. A **73**, 012341 (2006).
[50] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[51] M. Navascués and A. Acín, Phys. Rev. A **72**, 012303 (2005).
[52] M.-D. Choi, Linear Algebr. Appl. **10**, 285 (1975); A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).