W-like bound entangled states and secure key distillation

2009 Europhys. Lett. 85 50001

(http://iopscience.iop.org/0295-5075/85/5/50001)

A Letters Journal Exploring the Frontiers of Physics

March 2009

EPL, **85** (2009) 50001 www.epljournal.org
doi: 10.1209/0295-5075/85/50001

W-like bound entangled states and secure key distillation

R. Augusiak[1,2(a)] and P. Horodecki[2,3(b)]

[1] *ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park - 08860 Castelldefels (Barcelona), Spain, EU*
[2] *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology - G. Narutowicza 11/12, 80-952 Gdańsk, Poland, EU*
[3] *National Quantum Information Centre of Gdańsk - W. Andersa 27, 81-824 Sopot, Poland, EU*

received on 26 November 2008; accepted by M. Lewenstein on 18 January 2009
published online 18 March 2009

PACS 03.67.Dd – Quantum cryptography and communication security

Abstract – We construct multipartite entangled states with underlying W-type structure satisfying positive partial transpose (PPT) condition under any $(N-1)|1$ partition. Then we show how to distill a N-partite secure key from the states using two different methods: direct application of local filtering and novel random key distillation scheme in which we adopt the idea from recent results on entanglement distillation. Open problems and possible implications are also discussed.

Introduction. – Quantum cryptography [1,2] is an impressive information-theoretic application of quantum physical laws in data security theory. The proofs [3,4] of unconditional security of the pioneering quantum cryptographic protocol [1] refer to the idea of quantum privacy amplification [5] based on the entanglement distillation protocol [6]. This refers back to the cryptographic protocol [2] which is based on shared pure entanglement and is in fact the first explicit application of entanglement in information theory. Since then we already know that all correlation-based cryptographic protocols require entanglement as a necessary resource [7]. While it was natural to expect that distillation of pure entanglement is necessary to cryptography, it happened that even nondistillable entanglement known as a bound entanglement [8] may, at least in some cases, be useful for cryptography [9] with the corresponding general entanglement-based cryptographic paradigm going beyond the entanglement distillation developed in [10] (for recent interesting applications in security proofs and physical analysis of security see refs. [11,12]). Recently a multipartite version of the latter has been worked out in refs. [13,14]. Especially in the latter multipartite bound entanglement has been constructed based on the twisted GHZ-type entanglement. Here we present a nonstandard application of the paradigm with a novel type of multipartite bound entanglement, namely the one with underlying W-like structure. We adopt here the idea of random distillation of entanglement [15,16] introducing the notion of random distillation of secure key. The latter seems to be much more efficient for the present states than the concatenation of the usual bipartite protocols with classical postprocessing.

N-partite noisy W-like states passing single-system PPT test. – Below we provide a detailed construction of bound entangled states, which exhibit the structure of noisy W states, where the latter are defined as N-qubit pure states of the form

$$|W\rangle\langle W| = (1/\sqrt{N})(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |0\ldots01\rangle). \quad (1)$$

We give a detailed proof that partial transposition with respect to each single-party subsystem is positive.

Let us start by introducing the following matrices:

$$Z_D = \sum_{i,j=0}^{D-1} u_{ij}|ii\rangle\langle jj|, \qquad R_D = \sum_{i=0}^{D-1} |ii\rangle\langle ii|, \quad (2)$$

where u_{ij} denote elements of some unitary matrix U_D. The sum of absolute values of all elements of U_D will be denoted by $\mathcal{U}_D$. For simplicity we can also assume U_D to be Hermitian. Now let us define

$$X_D^{(N)} = Z_{1,2}^{\Gamma_2} \otimes \ldots \otimes Z_{i-1,i}^{\Gamma_i} \otimes Z_{i,i+1}^{\Gamma_{i+1}} \otimes \ldots \otimes Z_{N,1}^{\Gamma_1}, \quad (3)$$

where subscripts indicate that the matrix represents parts of the i-th and j-th party and Γ_j stands for partial transposition with respect the subsystem belonging to the j-th party. For instance $Z_{1,2}^{\Gamma_2}$ is a part of quantum systems belonging to the first and second party that must be transposed with respect to the second party.

Let us now shortly discuss the properties of $X_D^{(N)}$. Firstly, since $|Z_{i,i+1}| = |Z_{i,i+1}^T| = R_D$ $(i = 1, \ldots, N)$ and

(a) E-mail: remigiusz.augusiak@icfo.es
(b) E-mail: pawel@mif.pg.gda.pl

$\left|Z_{k-1,k}^{\Gamma_k}\right| = \sum_{i,j=0}^{D-1} |u_{ij}||ji\rangle\langle ji| \,(\equiv \mathcal{Z}_{k-1,k})$, one concludes that

$$\left|\mathcal{X}_D^{(N)\Gamma_i}\right| = \bigotimes_{k=1}^{i-2} \mathcal{Z}_{k,k+1} \otimes R_D^{(2)} \otimes R_D^{(2)} \otimes \bigotimes_{k=i+1}^{N} \mathcal{Z}_{k,k+1}. \tag{4}$$

All the matrices $\left|\mathcal{X}_D^{(N)\Gamma_i}\right|$ are diagonal and, as such, they are invariant under the action of partial transposition. It is also clear that $\left|X_D^{(N)}\right| = \bigotimes_{k=1}^{N} \mathcal{Z}_{k,k+1}$ which together with eq. (4) allows to infer that

$$\left\|X_D^{(N)\Gamma_i}\right\|_1 = \mathcal{U}_D^{N-2} D^2 \quad \text{and} \quad \left\|X_D^{(N)}\right\|_1 = \mathcal{U}_D^N, \tag{5}$$

for any $i = 1, \ldots, N$. Now we are prepared to present the construction. For this purpose, let us introduce

$$Y_D^{(N)} = \sum_{i=1}^{N} \left|X_D^{(N)\Gamma_i}\right| \tag{6}$$

and denote by $|\psi_i^{(N)}\rangle$ ($|\psi_{ij}^{(N)}\rangle$) pure N-qubit states in which the i-th party (i-th and j-th parties) posses $|1\rangle$ and the remaining parties have $|0\rangle$. Let also $\mathcal{P}_i^{(N)}$ and $\mathcal{P}_{ij}^{(N)}$ be projectors onto $|\psi_i^{(N)}\rangle$ and $|\psi_{ij}^{(N)}\rangle$, respectively.

Then we can consider the following class of states:

$$\begin{aligned}\varrho_{\mathsf{AA}'}^{(D,N)} = \frac{1}{\mathscr{N}_D^{(N)}} \Bigg\{ & \sum_{\substack{i,j=1 \\ i\neq j}}^{N} \left|\psi_i^{(N)}\right\rangle\!\left\langle\psi_j^{(N)}\right| \otimes X_D^{(N)} \\ & + (N-1)|0\rangle\langle 0|^{\otimes N} \otimes Y_D^{(N)} + \sum_{\substack{i,j=1 \\ i<j}}^{N} \mathcal{P}_{ij}^{(N)} \otimes Y_D^{(N)} \\ & + \sum_{i=1}^{N} \mathcal{P}_i^{(N)} \otimes \left[(N-1)\left|X_D^{(N)}\right| + (N-2) Y_D^{(N)}\right] \Bigg\}, \end{aligned} \tag{7}$$

where the normalization factor is given by

$$\mathscr{N}_D^{(N)} = N\mathcal{U}_D^{N-2}\left[(N-1)\mathcal{U}_D^2 + (D^2/2)(3N^2 - 3N - 2)\right].$$

The subscripts $\mathsf{A} \equiv A_1 \ldots A_N$ and $\mathsf{A}' \equiv A_1' \ldots A_N'$ denote the *key part* and *shield part* of the state. They are separated by the tensor product visible in eq. (7). "Everything" that is on the left-hand side of this sign belongs to A and everything on the right-hand side belongs to A'. Usually one considers the situation in which the i-th party has two subsystems denoted here by A_i and A_i' (one from A and one from A'). However, in a more general scenario we can also assume that the whole A' is held by some other but trusted party or even more trusted parties.

Let us now check the positivity of partial transposition with respect to the i-th subsystem. Straightforward algebra shows that $\varrho_{\mathsf{AA}'}^{(D,N)\Gamma_i}$ is of the form,

$$\begin{aligned}\varrho_{\mathsf{AA}'}^{(D,N)\Gamma_k} = \frac{1}{\mathscr{N}_D^{(N)}} \Bigg\{ & \Bigg[\sum_{\substack{i=1 \\ i\neq k}}^{N} (|0\rangle^{\otimes N}\!\left\langle\psi_{ik}^{(N)}\right| + \left|\psi_{ik}^{(N)}\right\rangle\!\langle 0|^{\otimes N}) \\ & \otimes X_D^{(N)\Gamma_k} + (N-1)|0\rangle\langle 0|^{\otimes N} \otimes Y_D^{(N)} + \sum_{\substack{i=1 \\ i\neq k}}^{N} \mathcal{P}_{ik}^{(N)} \otimes Y_D^{(N)} \Bigg] \\ & + \Bigg[(N-2) \sum_{\substack{i=1 \\ i\neq k}}^{N} \mathcal{P}_i^{(N)} \otimes Y_D^{(N)} + \sum_{\substack{i,j=1 \\ i\neq j,\, i,j\neq k}}^{N} \left|\psi_i^{(N)}\right\rangle\!\left\langle\psi_j^{(N)}\right| \\ & + \otimes X_D^{(N)\Gamma_k} \Bigg] + \mathcal{P}_k^{(N)} \otimes \left[(N-1)\left|X_D^{(N)}\right| + (N-2) Y_D^{(N)}\right] \\ & + \sum_{\substack{i,j=1 \\ i<j,\, i,j\neq k}}^{N} \mathcal{P}_{ij}^{(N)} \otimes Y_D^{(N)} \Bigg\}. \end{aligned} \tag{8}$$

To make the analysis simpler, some of the terms in the above were grouped in square brackets. The positivity of the first and second brackets follows straightforwardly from results of ref. [14] (see Lemma A.1). The remaining two terms are positive as $Y_D^{(N)} \geqslant 0$.

Thus we showed that partial transposition with respect to any single-party subsystem $A_i A_i'$ is positive. This indicates that the states $\varrho_{\mathsf{AA}'}^{(D,N)}$ are bound entangled provided that they are entangled. However, the latter still need to be shown. For this purpose, below we discuss cryptographical applicability of these states.

Secure key distillation. – We prove that it is possible to distill a nonzero amount of cryptographic key from the states $\varrho_{\mathsf{AA}'}^{(D,N)}$. For this purpose we show that one can distill a bipartite secure key between any pair of parties of $\varrho_{\mathsf{AA}'}^{(D,N)}$. Let us focus on the scenario in which the remaining $N-2$ parties cooperate "passively", *i.e.*, they perform no action but are trusted (do not cooperate with Eve). In this case the distillable key[1] can only be higher than in a scenario in which the remaining $N-2$ parties would give some of their systems to Eve. Thus, for our purposes it suffices to investigate the bipartite distillable key of the states[2] $\varrho_{A_k A_l \mathsf{A}'}^{(D,N)} = \mathrm{Tr}_{\mathsf{A}\setminus\{k,l\}} \varrho_{\mathsf{AA}'}^{(D,N)}$ for any $k \neq l$ (note that tracing out the subsystems may be treated as giving them to Eve). As in what follows the additional systems are not directly used in secure key distillation and the remaining parties are trusted, we can considerably simplify the analysis by applying the general bipartite cryptographical paradigm studied in [9,10]. Indeed, we can

[1] For definitions of the bipartite and multipartite distillable key C_D and K_D the reader is referred to [9,10] and [13,14], respectively.

[2] The notation $\mathrm{Tr}_{\mathsf{A}\setminus\{k,l\}}$ means that we trace out the A subsystem except for A_k and A_l subsystems.

even consider the system A' as one distributed between A_k and A_l. However, it does not mean that the considered scenario is only bipartite since the total protocol will consist of bipartite protocols with different pairs $\{k,l\}$.

We investigate the bipartite distillable key using two methods. The first one is quite simple application of local filtering, while the second one, probably more efficient, bases on the ideas of random distillation of entanglement given in refs. [15,16]. Both protocols, are finally concatenated with the Devetak-Winter (DW) protocol [17,18].

We also simplify our considerations by imposing some constraints on U_D, namely, we assume that all of its entries obey $|u_{ij}|=1/\sqrt{D}$. An example of such a unitary Hermitian matrix is the matrix $H^{\otimes k}$, with H being the Hadamard matrix (here $D=2^k$). In this case $\mathcal{U}_D=D\sqrt{D}$ and what is important here $\| X_D^{(N)} \| / \| Y_D^{(N)} \| = D/N$, which is greater than one for sufficiently large D.

Twistings and privacy squeezing. In view of what was said previously it suffices to restrict our considerations to the distillation of the bipartite secure key. The general cryptographical paradigm of refs. [9,10,19] is exactly what we need here. Thus, below we recall some of its main ideas, namely, twistings and the privacy squeezing [10] with its application in the recent method [19] of bounding the key from below. Possible multipartite generalizations of the paradigm were studied in [13,14].

Let then $\varrho_{ABA'B'}$ denote some bipartite state with the AB ($A'B'$) part called the key (shield) part (notice once more that in general in the considered scenario one does not have to demand that the $A'B'$ part belong to the involved parties as it may be in possession of some other trusted party). Now, let $\mathcal{B}=\{|ij\rangle\}$ denote some product basis in the Hilbert space corresponding to the AB part. Then one defines the *ccq state* $\varrho_{ABE}^{(\mathrm{ccq})}$ to be a state that arises upon a measurement of the AB part of a purification $|\psi_{ABA'B'E}\rangle$ of $\varrho_{ABA'B'}$ in the product basis $\mathcal{B}$ and tracing out the shield part $A'B'$ (in the usual scenarios the shield part is treated then as a trivial subsystem).

Now, we define *twisting* (with respect to the basis $\mathcal{B}$) to be the following operation:

$$U_t=\sum_{i,j}|ij\rangle\langle ij|\otimes U_{ij}, \tag{9}$$

where in general U_{ij} denote some isometries acting on the $A'B'$ part. The important fact connected to twistings is that $\varrho_{ABA'B'}$ and its twisted version $U_t\varrho_{ABA'B'}U_t^\dagger$ have the same ccq state (with respect to the same basis).

The last concept we would like to mention here is the so-called *privacy squeezing*. Namely, by "rotating" the state $\varrho_{ABA'B'}$ with some appropriately chosen twisting U_t and then tracing out its shield part we get the *privacy squeezed state* $\widetilde{\varrho}_{AB}=\mathrm{Tr}_{A'B'}\big(U_t\varrho_{ABA'B'}U_t^\dagger\big)$.

Now, the method applied first in ref. [19] implies that taking the purification $|\widetilde{\Psi}_{ABE}\rangle$ of the latter and measuring it in the basis AB produces the ccq state with C_D being a lower bound on the distillable key of the original state $\varrho_{ABA'B'}$. Let us apply this technique carefully to our example with general shield system A'. Firstly, it follows from ref. [10] that in general $K_D(\varrho_{A_kA_l\mathsf{A}'})=C_D(|\psi_{A_kA_l\mathsf{A}'E}\rangle)\geqslant C_D(\varrho_{A_kA_lE}^{(\mathrm{ccq})})$, where $|\psi_{A_kA_l\mathsf{A}'E}\rangle$ stands for the purification of $\varrho_{A_kA_l\mathsf{A}'}$, while $\varrho_{A_kA_lE}^{(\mathrm{ccq})}$ denotes the ccq derived according to the aforementioned prescription. On the other hand, we can consider a twisted purification $|\psi_t\rangle\equiv U_t\otimes\mathbb{1}_E|\psi_{A_kA_l\mathsf{A}'E}\rangle$. As previously mentioned the ccq state (denoted as $\sigma_{A_kA_lE}^{(\mathrm{ccq})}$) following this purification is exactly the same as $\varrho_{A_kA_lE}^{(\mathrm{ccq})}$ (in $\mathcal{B}$). Finally, we can consider a worse situation from the point of secure key distillation between the parties A_k and A_l. Namely giving now the A' subsystem we can only lower the key. In other words, we can look at the twisted purification $|\psi_t\rangle$ as coming from purifying only the A_kA_l (with the whole system $E'=\mathsf{A}'E$ considered to be in Eve's hands). In this way we have $C_D(\sigma_{A_kA_lE}^{(\mathrm{ccq})})\geqslant C_D(\widetilde{\varrho}_{A_kA_lE'}^{(\mathrm{ccq})})$, where $\widetilde{\varrho}_{A_kA_lE'}^{(\mathrm{ccq})}$ denotes the ccq state derived in this way. The last step is an application of the Devetak-Winter protocol to $\widetilde{\varrho}_{A_kA_lE}^{(\mathrm{ccq})}$ which gives $C_D(\widetilde{\varrho}_{A_kA_lE}^{(\mathrm{ccq})})\geqslant I(A_k{:}A_l)-I(A_k{:}E)$, where the quantities[3] $I(A_k:A_l)$ and $I(A_k:E)$ are calculated for respective bipartite reductions of $\widetilde{\varrho}_{A_kA_lE}^{(\mathrm{ccq})}$. The conclusion following this analysis is that $K_D(\varrho_{A_kA_l\mathsf{A}'})\geqslant C_D(\widetilde{\varrho}_{A_kA_lE}^{(\mathrm{ccq})})$ and therefore in what follows we can restrict to the analysis of the distillable key of $\widetilde{\varrho}_{A_kA_lE}^{(\mathrm{ccq})}$. In other words we need to take the privacy-squeezed $\widetilde{\varrho}_{A_kA_l}^{(D,N)}$ version of $\varrho_{A_kA_l\mathsf{A}'}^{(D,N)}$ and analyze lower bounds on the distillable key of its ccq state.

Note also that any filtering operation diagonal in $\mathcal{B}$ and performed on the key part of the state commutes with the privacy squeezing operation with respect to the same basis. This allows to perform local filters on the privacy-squeezed state instead of on the initial one $\varrho_{\mathsf{AA}'}^{(D,N)}$.

Direct application of local filters. Without loss of generality we can assume $\mathcal{B}$ to be the standard basis in $\mathbb{C}^2\otimes\mathbb{C}^2$. Then we can derive the privacy-squeezed state of an arbitrary state $\varrho_{A_kA_l\mathsf{A}'}$ ($k\neq l$). Choosing in (9) $U_{01}^\dagger$ and $U_{10}^\dagger$ to be unitary matrices from the singular-value decomposition of $X_D^{(N)}$ and $U_{00}=U_{11}=\mathbb{1}_{D^{2N}}$, we get after some calculations from eq. (7) that

$$\widetilde{\varrho}_{A_kA_l}^{(D,N)}=\frac{1}{\widetilde{\mathcal{N}_D^{(N)}}}\begin{bmatrix}\alpha_{D,N} & 0 & 0 & 0\\ 0 & \beta_{D,N} & D & 0\\ 0 & D & \beta_{D,N} & 0\\ 0 & 0 & 0 & N\end{bmatrix}, \tag{10}$$

where $\widetilde{\mathcal{N}_D^{(N)}}=N[(N-1)D+(3N^2-3N-2)/2]$, $\alpha_{D,N}=(N-2)(N-1)D+[(3N^2-11N+12)/2]N$, and $\beta_{D,N}=(N-1)D+2(N-2)N$.

Since $\alpha_{D,N}$ considerably dominates the remaining entries of $\widetilde{\varrho}_{A_kA_l}^{(D,N)}$, the DW protocol does not

[3] The quantum mutual information $I(A:B)$ is defined for ϱ_{AB} as $I(A:B)=S(\varrho_A)+S(\varrho_B)-S(\varrho_{AB})$ with S denoting the von Neumann entropy.

apply here. However, using some local filters[4] we can change the respective entries. So, let us consider the filter $V_\epsilon = \mathrm{diag}[\epsilon, 1]$ $(0 \leqslant \epsilon \leqslant 1)$ and let the k-th and l-th party apply it. This with probability $q_{D,N}^{(\epsilon)} = \mathrm{Tr}\big(V_\epsilon^\dagger V_\epsilon \otimes V_\epsilon^\dagger V_\epsilon \, \widetilde{\varrho}_{A_k A_l}^{(D,N)}\big)$ brings $\widetilde{\varrho}_{A_k A_l}^{(D,N)}$ to the following state:

$$\overline{\varrho}_{A_k A_l}^{(D,N,\epsilon)} = \frac{\epsilon^2}{\overline{\mathscr{N}}_{D,N}^{(\epsilon)}} \begin{bmatrix} \alpha_{D,N}\epsilon^2 & 0 & 0 & 0 \\ 0 & \beta_{D,N} & D & 0 \\ 0 & D & \beta_{D,N} & 0 \\ 0 & 0 & 0 & \frac{N}{\epsilon^2} \end{bmatrix} \tag{11}$$

with $\overline{\mathscr{N}}_{D,N}^{(\epsilon)} = \alpha_{D,N}\epsilon^4 + 2\beta_{D,N}\epsilon^2 + N$. According to the previous prescription what we need now is to bound from below the distillable key of the ccq state (in $\mathcal{B}$) of $\widetilde{\varrho}_{A_k A_l}^{(D,N)}$. For this purpose we can firstly find a lower bound on C_D of $\overline{\varrho}_{A_k A_l E}^{(\mathrm{ccq},\epsilon)}$ using the DW protocol, where by $\overline{\varrho}_{A_k A_l E}^{(\mathrm{ccq},\epsilon)}$ we denoted the ccq state[5] corresponding to the output of the filtering, *i.e.*, $\overline{\varrho}_{A_k A_l}^{(D,N,\epsilon)}$. Secondly, as local filtering is a stochastic operation, multiplying the latter with the success probability $q_{D,N}^{(\epsilon)}$, we get the desired result. This, however, according to the discussion above allows us to write

$$K_D(\varrho_{A_k A_l \mathsf{A}\mathsf{A}'}^{(D,N)}) \geqslant q_{D,N}^{(\epsilon)} \left[I(A_k{:}A_l) - I(A_k{:}E) \right], \tag{12}$$

where both I are calculated from reductions of $\overline{\varrho}_{A_k A_l E}^{(\mathrm{ccq},\epsilon)}$. The behaviour of the right-hand side (denoted by $\widetilde{K}_{DW}^{(\epsilon,N)}$) of eq. (12) as a function of the filter parameter ϵ and the dimension D is plotted in fig. 1 for $N=3$ and $N=5$. Despite the rather small values of $\widetilde{K}_{DW}^{(\epsilon,N)}$ and the large dimension D of A_i', it is clear from fig. 1 that one may distill a nonzero amount of bipartite key from the states $\varrho_{\mathsf{A}\mathsf{A}'}^{(D,3)}$ and $\varrho_{\mathsf{A}\mathsf{A}'}^{(D,5)}$.

Finally, we need to show that indeed the possibility of secure-key distillation between any pair of parties of $\varrho_{\mathsf{A}\mathsf{A}}^{(D,N)}$ leads to the distillation of a genuine multipartite secure key among all the parties. For this purpose notice firstly that in the general case of a N-partite state it suffices to have a bipartite secure key among pairs $A_i A_{i+1}$ $(i = 1, \ldots, N-1)$. Secondly, let us assume that each such pair distills a secure key at a rate r. Then one concludes that in such a configuration all the parties can distill a multipartite key at a rate at least $r/(N-1)$. Since we showed that in the case of our states r is nonzero, the multipartite distillable key of $\varrho_{\mathsf{A}\mathsf{A}'}^{(D,N)}$ is nonzero, at least in the cases of $N = 3, 5$.

Alternative approach: the idea of random distillation of secure key. Now, basing on the very recent results of Lo and Fortescue [15,16], we consider a little bit more sophisticated way of the bipartite key distillation

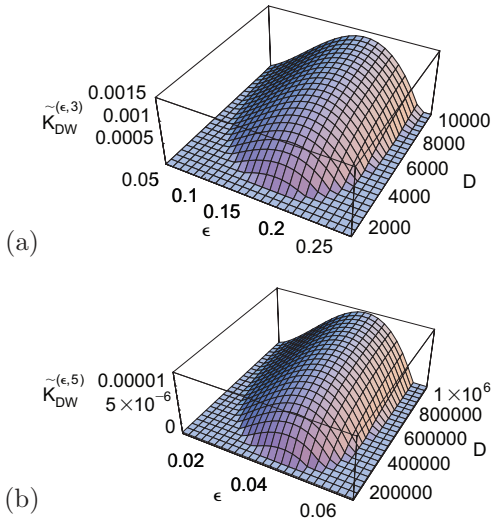

Fig. 1: The dependence of $\widetilde{K}_{DW}^{(\epsilon,N)}$ on the parameters ϵ and D for two different values of N, namely, $N=3$ (a) and $N=5$ (b). Zero is put whenever the plotted function is less than zero. Also, for clarity, the function is plotted as if it were continuous in D. It is clear from both the plots that the number of parties lowers the plotted function.

from $\varrho_{\mathsf{A}\mathsf{A}'}^{(D,N)}$. For simplicity we focus here only on the case of $N=3$, however, generalization to more parties is straightforward.

Let us then consider the following POVM $\mathscr{V}_\epsilon = \mathrm{diag}[\sqrt{1-\epsilon^2}, 1]$ and $\mathscr{W}_\epsilon = \mathrm{diag}[\epsilon, 0]$ $(0 \leqslant \epsilon \leqslant 1)$. It is clear that $\mathscr{V}_\epsilon^\dagger \mathscr{V}_\epsilon + \mathscr{W}_\epsilon^\dagger \mathscr{W}_\epsilon = \mathbb{1}_2$, where $\mathbb{1}_2$ denotes the 2×2 identity. Each of the parties applies this POVM to their "nonprimed" subsystems A_i $(i = 1, 2, 3)$. Now, we divide the possible outcomes into three groups. The first one contains a single element, *i.e.*, a result of the application of $\mathscr{V}_\epsilon^{\otimes 3}$. The second group contains the outcome of the application of $\mathscr{V}_\epsilon^{\otimes 2} \otimes \mathscr{W}_\epsilon$ and two other outcomes being permutations of $\mathscr{V}_\epsilon$ and $\mathscr{W}_\epsilon$ in $\mathscr{V}_\epsilon^{\otimes 2} \otimes \mathscr{W}_\epsilon$. Finally, the third group consists of the remaining outcomes. The results from the second group are treated as a success since they lead to secure-key distillation. On the contrary any result from the third group is considered as a failure as the resulting state has a separable structure with respect to the key part. In the case when the obtained result belongs to the second or third group, the protocol stops. On the other hand, when the result belongs to the first group we have to repeat our protocol as the obtained result keeps the structure of the initial state.

Let us now pass to the protocol. Assume that the parties repeat the measurement M times, but in such a way that in each round the value of ϵ in the definition of POVM differs. Precisely, following ref. [15] we utilize $\epsilon_i = 1/\sqrt{1+i}$, however, in a reversed order, *i.e.*, in the first round we take $\epsilon_M = 1/\sqrt{1+M}$ and in the last one $\epsilon_1 = 1/2$.

Taking into account a single success outcome $\mathscr{V}_\epsilon^{\otimes 2} \otimes \mathscr{W}_\epsilon$ (corresponding to the secure-key distillation between the first and second party), the state after M measurements

[4] Physically the filters are performed on subsystems of the key part of $\varrho_{\mathsf{A}\mathsf{A}'}^{(D,N)}$ by respective parties, however as they commute with the privacy squeezing we can mathematically perform it on $\widetilde{\varrho}_{A_k A_l}^{(D,N)}$.

[5] For the sake of clarity, we do not provide the explicit form of the purification of $\overline{\varrho}_{A_k A_l}^{(D,N,\epsilon)}$ and of the ccq state $\overline{\varrho}_{A_k A_l E}^{(\mathrm{ccq},\epsilon)}$.

is of the form $\rho^{(D,M)}_{\mathsf{AA}'} = G^{(M)}_D/\mathrm{Tr}(G^{(M)}_D)$, where[6]

$$\begin{aligned} G^{(M)}_D &= \widetilde{\mathscr{V}}^{\otimes 2}_{\epsilon_M} \otimes \widetilde{\mathscr{W}}_{\epsilon_M} \varrho^{(D,3)}_{\mathsf{AA}'} \widetilde{\mathscr{V}}^{\otimes 2}_{\epsilon_M} \otimes \widetilde{\mathscr{W}}_{\epsilon_M} \\ &+ \widetilde{\mathscr{V}}_{\epsilon_{M-1}} \widetilde{\mathscr{V}}_{\epsilon_M} \otimes \widetilde{\mathscr{V}}_{\epsilon_{M-1}} \widetilde{\mathscr{V}}_{\epsilon_M} \otimes \widetilde{\mathscr{W}}_{\epsilon_{M-1}} \widetilde{\mathscr{V}}_{\epsilon_M} \\ &\times \varrho^{(D,3)}_{\mathsf{AA}'} \widetilde{\mathscr{V}}_{\epsilon_M} \widetilde{\mathscr{V}}_{\epsilon_{M-1}} \otimes \widetilde{\mathscr{V}}_{\epsilon_M} \widetilde{\mathscr{V}}_{\epsilon_{M-1}} \otimes \widetilde{\mathscr{V}}_{\epsilon_M} \widetilde{\mathscr{W}}_{\epsilon_{M-1}} \\ &\vdots \\ &+ \widetilde{\mathscr{V}}_{\epsilon_1} \ldots \widetilde{\mathscr{V}}_{\epsilon_M} \otimes \widetilde{\mathscr{V}}_{\epsilon_1} \ldots \widetilde{\mathscr{V}}_{\epsilon_M} \otimes \widetilde{\mathscr{W}}_{\epsilon_1} \widetilde{\mathscr{V}}_{\epsilon_2} \ldots \widetilde{\mathscr{V}}_{\epsilon_M} \varrho^{(D,3)}_{\mathsf{AA}'} \\ &\times \widetilde{\mathscr{V}}_{\epsilon_M} \ldots \widetilde{\mathscr{V}}_{\epsilon_1} \otimes \widetilde{\mathscr{V}}_{\epsilon_M} \ldots \widetilde{\mathscr{V}}_{\epsilon_1} \otimes \widetilde{\mathscr{V}}_{\epsilon_M} \widetilde{\mathscr{V}}_{\epsilon_2} \ldots \widetilde{\mathscr{W}}_{\epsilon_1}. \end{aligned} \tag{13}$$

The probability of appearance of $\rho^{(D,M)}_{\mathsf{AA}'}$ is given by $q^{(M)}_D = (2M^2(D+4) + M(2D+7))/6(D+4)(M+1)^2$.

Let us briefly explain eq. (13). The first term corresponds to the success obtained in the first round of the protocol, while the second terms is responsible for the outcome from the first group obtained in the first round and the success obtained in the second round. The remaining terms may be derived in an analogous way.

Since we chose the success outcome corresponding to the key distillation between parties A_1 and A_2 we can trace the key part of the last party of $\rho^{(D,M)}_{\mathsf{AA}'}$, getting the state $\rho^{(D,M)}_{A_1A_2\mathsf{A}'}$. As we are interested in application of the DW protocol we can apply the privacy squeezing with the same twisting operation U_t as in the previous subsection, which effectively removes the shield part and produces finally

$$\widetilde{\rho}^{(D,M)}_{A_1A_2} = \frac{1}{\mathcal{G}^{(M)}_D} \begin{bmatrix} 2\frac{2M+1}{M+1} & 0 & 0 & 0 \\ 0 & 2D+3 & D & 0 \\ 0 & D & 2D+3 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}, \tag{14}$$

where $\mathcal{G}^{(M)}_D = 2[2M(D+4) + 2D + 7]/(M+1)$.

The remaining two success outcomes of the POVM (corresponding to $\mathscr{V}_\epsilon \otimes \mathscr{W}_\epsilon \otimes \mathscr{V}_\epsilon$ and $\mathscr{W}_\epsilon \otimes \mathscr{V}^{\otimes 2}_\epsilon$) lead after M rounds to exactly the same two-qubit states as in eq. (14), however, shared by the parties A_1 and A_3, and A_2 and A_3, respectively. Also, probabilities of obtaining the respective states are the same and equal to $q^{(M)}_D$. Let us notice also that in the asymptotic limit $M \to \infty$ the probability $q^{(M)}_D$ tends to one-third. It means that taking into account all the three success outputs we are sure that in the limit of $M \to \infty$ the secure bit will be shared by one of the pairs of parties.

Finally, in the same way as previously we get

$$K_D(\varrho^{(D,3)}_{A_1A_2\mathsf{A}'}) \geqslant q^{(M)}_D \left[I(A_1{:}A_2) - I(A_1{:}E) \right], \tag{15}$$

where I are calculated for reductions of the ccq state $\widetilde{\rho}^{(\mathrm{ccq})}_{A_1A_2E}$ (in $\mathcal{B}$) of $\widetilde{\rho}^{(D,M)}_{A_1A_2}$. The behavior of the function appearing on the right-hand side of the above, *i.e.*, the difference between mutual information multiplied by $q^{(M)}_D$ (denoted by K_{DW}) is presented in fig. 2. On the other hand, one may prove analytically that it is possible to get a secure key from $\widetilde{\rho}^{(\mathrm{ccq})}_{A_1A_2E}$. Namely, notice that the limit of $\widetilde{\rho}^{(D,M)}_{A_1A_2}$ with $D \to \infty$ has nonzero K_D by the DW protocol and thus, by continuity of the involved functions there must exist such D that $\widetilde{\rho}^{(\mathrm{ccq})}_{A_1A_2E}$ has also nonzero K_D.

[6] By $\widetilde{\mathscr{V}_\epsilon}$ and $\widetilde{\mathscr{W}_\epsilon}$ we denoted the POVM operators $\mathscr{V}_\epsilon$ and $\mathscr{W}_\epsilon$ extended by the identity acting on A' subsystems.

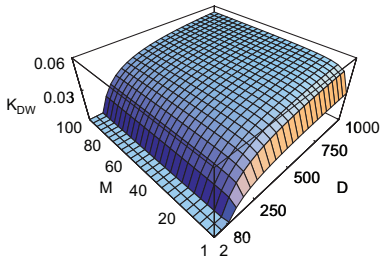

Fig. 2: The dependence of K_{DW} on M and D. Zero is put whenever the plotted function is less than zero and, for convenience, it is presented as a function of continuous M and D. Interestingly, the nonzero values appear at about $D = 80$, while in the analogous plot (fig. 1(a)) nonzero values are from about $D = 2000$. Moreover, it is clear that in the case of the random protocol the distillable key is bounded by larger values. Consequently, it is very reasonable to suspect that by using the random protocol one can distill a more secure key.

To finish our considerations, we discuss what rates of multipartite key are achievable within the described method. We already know that to get the multipartite key it suffices to have a secure key between some properly chosen parties. However in previous cases we needed to divide the protocol into separate $N-1$ bipartite deterministic protocols, while here we get different bipartite keys in *one* deterministic protocol. This suggests that we can think a little bit clever while estimating the multipartite key rate here.

For this purpose let us focus on the three-partite case and consider the rates r_1, r_2, r_3, where r_1 is a key rate between A_1 and A_2 and so on. Assume that all the rates r_i are positive and form the triangle inequality. In this case there exist a triple of positive numbers a, b, c such that $(r_1, r_2, r_3) = (a+b, b+c, c+a)$, it is not difficult to conclude that the rate of multipartite key may be lower bounded by $a+b+c = (r_1+r_2+r_3)/2$. For $\varrho^{(D,N)}_{\mathsf{AA}'}$ all rates r_i are equal to K_{DW} and the obtainable rate of multipartite key is $(3/2)K_{DW}$.

Distillation of a "truly" random secure key —is this possible for bound entangled states? In the previous section we have considered the random distillation of a secure key. In this process all the parties have to cooperate. Indeed the performances of the protocol have been estimated with privacy squeezing involving *all* "primed" parties as a shield part. This means that during the protocol the passive parties (like A_3 in the analysis from the previous subsection) were trusted in the sense that they keep their "primed" subsystems (A'_3) and do not give it to Eve.

This means that effectively the bipartite key between A_1 and A_2 can only at this early stage get correlated to the third party. But what if we were interested in a *true random bipartite key*, *i.e.*, such that after the random bipartite protocol the (random) bipartite key is secure not only against Eve but also against other parties?

This may be also related to a two-stages protocol: N trusted parties representing some public company are given N-partite state and distill such random key in a way that it is truly bipartite. After that, N different parties come and use that key having all the bipartite secure communications guaranteed.

Note that this kind of random secure key would share with entanglement the monogamy property. The natural question is which multipartite bound entangled states can lead to the key with such a property. Preliminary analysis of our W-like states seems to suggests that it is impossible to get such key form our states.

Discussion. – We have provided a construction of novel multipartite bound entangled states with underlying W-type structure. The states satisfy the PPT test for any $(N-1)|1$ partition. We have analyzed the distillation of a secure key from the states in two different ways. The first one is based on the usual bipartite filtering-based protocol followed by the DW scheme. The second one involves random distillation of a secure key. Though we have not proven the optimality of the protocols, the present results suggests that, as in the entanglement distillation, the random distillation of a secure key may be much more efficient in the distillation of a multipartite cryptographic key in cases when one deals with underlying W-type structure. However, since the present states are the first bound entangled states of this type, still further analysis is necessary. One also expects that bound entanglement of other multipartite types like graph states [20] may also be constructed and found to be useful in quantum cryptography. It is interesting to address this type of questions in the context of the recently discovered thermal bound entanglement in quantum arrays and lattices [21]. On the other hand, one may ask about the distillation of a quantum key in a modified sense: this would be the "truly" random bipartite key in the sense that bipartite cryptographic correlations were secure not only against Eve but also against all the remaining parties. Note that, of course, this is possible in case of some free entangled states: the Lo-Fortescue protocol followed by classical measurement of entangled pairs provides naturally such key. Here the natural question arises about which bound entangled states lead to such key.

Another natural question concerns the relation of the present results to quantum channels capacities. Indeed the present states as well as the states from [14] may be immediately used to generate a quantum channel (with k senders and $n-k$ receivers). It is interesting that while the one-sender channels created from the GHZ-type states [14] have strictly positive one-way multipartite privacy capacity $\mathcal{P}$ (due to generalized DW protocol) it seems to be rather unlikely that the channels based on the present W-like states have that property. Still, in the context of the fascinating and still uncovered role of privacy in the recently discovered superactivation effect of quantum bipartite capacity [22], and especially in the context of multipartite superactivation and activation of quantum capacities and entanglement (see [23]), further analysis of quantum channels based on the present states seems to be interesting.

* * *

The work is supported by the EU Integrated Project SCALA and by the LFPPI network. RA gratefully acknowledges the support from Ingenio 2010 QOIT and the Foundation for Polish Science.

REFERENCES

[1] Bennett C. H. and Brassard G., *Quantum cryptography: Public key distribution and coin tossing,* in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December, 1984* (IEEE Computer Society Press, New York) p. 175.
[2] Ekert A. K., *Phys. Rev. Lett.*, **67** (1991) 661.
[3] Shor P. W. and Preskill J., *Phys. Rev. Lett.*, **85** (2000) 441.
[4] Lo H.-K. and Chau H. F., *Science*, **283** (1999) 2050.
[5] Deutsch D. *et al.*, *Phys. Rev. Lett.*, **77** (1996) 2818.
[6] Bennett C. H. *et al.*, *Phys. Rev. Lett.*, **76** (1996) 722.
[7] Curty M., Lewenstein M. and Lütkenhaus N., *Phys. Rev. Lett.*, **92** (2004) 217903.
[8] Horodecki M., Horodecki P. and Horodecki R., *Phys. Rev. Lett.*, **80** (1998) 5239.
[9] Horodecki K., Horodecki M., Horodecki P. and Oppenheim J., *Phys. Rev. Lett.*, **94** (2005) 160502.
[10] Horodecki K., Horodecki M., Horodecki P. and Oppenheim J., *General paradigm for distillling classical key from quantum states*, arXiv:quant-ph/0506189, to be published in *IEEE Trans. Inf. Theory.*
[11] Renes J. M. and Smith G., *Phys. Rev. Lett.*, **98** (2007) 020502.
[12] Renes J. M. and Boileau J.-Ch., *Phys. Rev. A*, **78** (2008) 032335.
[13] Augusiak R., *On the distillation of cryptographic key from multipartite entangled quantum states*, PhD Thesis, Gdańsk, 2008.
[14] Augusiak R. and Horodecki P., *Multipartite quantum cryptography and bound entangled states*, arXiv:0811.3603.
[15] Lo H.-K. and Fortescue B., *Phys. Rev. Lett.*, **98** (2007) 260501.
[16] Lo H.-K. and Fortescue B., *Phys. Rev. A*, **78** (2008) 012348.
[17] Devetak I. and Winter A., *Phys. Rev. Lett.*, **93** (2004) 080501.
[18] Devetak I. and Winter A., *Proc. R. Soc. London, Ser. A*, **461** (2005) 207.
[19] Horodecki K., Pankowski Ł., Horodecki M. and Horodecki P., *IEEE Trans. Inf. Theory*, **54** (2008) 2621.
[20] Raussendorf R., Browne D. and Briegel H.-J., *Phys. Rev. A*, **68** (2003) 022312.
[21] Tóth G. *et al.*, *Phys. Rev. Lett.*, **99** (2007) 250405; Ferraro A. *et al.*, *Phys. Rev. Lett.*, **100** (2008) 080502.
[22] Smith G. and Yard J., *Science*, **321** (2008) 1812.
[23] Shor P. W., Smolin J. A. and Thapliyal A. V., *Phys. Rev. Lett.*, **90** (2003) 107901; Dür W., Cirac J. I. and Horodecki P., *Phys. Rev. Lett.*, **93** (2004) 020503; Czekaj Ł. and Horodecki P., arXiv:0807.3977, to be published in *Phys. Rev. Lett.*