# Efficient bounds on quantum-communication rates via their reduced variants

Marcin L. Nowakowski and Pawel Horodecki*

*Faculty of Applied Physics and Mathematics, Gdansk University of Technology, PL-80-952 Gdansk, Poland and National Quantum Information Centre of Gdańsk, Andersa 27, PL-81-824 Sopot, Poland*

(Received 15 July 2010; published 29 October 2010)

We investigate one-way communication scenarios where Bob operating on his component can transfer some subsystem to the environment. We define reduced versions of quantum-communication rates and, further, prove upper bounds on a one-way quantum secret key, distillable entanglement, and quantum-channel capacity by means of their reduced versions. It is shown that in some cases they drastically improve their estimation.

DOI: 10.1103/PhysRevA.82.042342 PACS number(s): 03.67.Hk

## I. INTRODUCTION

Recent years have seen enormous advances in quantum-information theory proving it has been well established as a basis for a concept of quantum computation and communication. Much work [1–7] has been performed to understand how to operate on quantum states and distill entanglement enabling quantum data processing or to establish quantum secure communication between two or more parties. One of the central problems of the quantum-communication field is to estimate the efficiency of communication protocols establishing secure communication between involved parties or distilling quantum entanglement [5–11]. Most simple communication scenarios are those that do not use a classical side channel or use it only in a one-way setup. The challenge for the present theory is to determine good bounds on such quantities as the secret key rate or quantum channel capacity and distillable entanglement of a quantum state, which allow the estimation of communication capabilities. In this paper, we provide efficient upper bounds, avoiding a massive overestimation of communication rates. We are inspired by classical information and entanglement measures theory where so-called reduced quantities have been used [8,10,12]. Herewith we consider two pairs of quantities: private capacity $\mathcal{P}$ and quantum one-way secret key $K_{\rightarrow}$, and one-way quantum channel capacity $\mathcal{Q}_{\rightarrow}$ and one-way distillable entanglement $D_{\rightarrow}$, providing efficient upper bounds. We prove that in some cases the bounds explicitly show that the corresponding quantity is relatively small if compared to sender and receiver systems. The main method is again the fact that all of the aforementioned quantities vanish on some classes of systems. Moreover, we introduce "defect" parameters $\Delta$ for the reduced quantities resulting from possible transfer of subsystems on the receivers' side, which are (sub)additive and, hence, can be exploited in the case of composite systems and regularization.

## II. REDUCED ONE-WAY SECRET KEY

A secret key is a quantum resource allowing two parties, Alice and Bob, a private communication over a public channel. In an ideal scenario, they generate a pair of maximally correlated classical secure bit strings such that Eve, representing the adversary in the communication, is not able to receive any sensible information from further communication between Alice and Bob. In this section, we elaborate on the generation of a one-way secret key from a tripartite quantum state shared by the parties with Eve that means Alice and Bob can use only protocols consisting of local operations and one-way public communication. We propose a new reduced measure of the one-way secret key that simplifies in many cases an analysis of the one-way security of quantum states.

To derive new observations about the one-way quantum secret key, in this section we use fundamental information notions engaging entropy[1] and quantum mutual information,[2] which play a vital role in quantum-information theory. We state a new result about the upper bound on the Holevo function,[3] $\chi(\cdot)$:

*Observation 1.* For any ensemble of density matrices $\mathfrak{A} = \{\lambda_i, \rho^i_{BB'}\}$ with the average density matrix $\rho_{BB'} = \sum_i \lambda_i \rho^i_{BB'}$, the following holds:

$$\chi(\rho_{BB'}) \leqslant \chi(\rho_B) + 2S(\rho_{B'}). \tag{1}$$

*Proof.* On the basis of subadditivity and concavity of quantum entropy, we can easily show that

$$\begin{aligned}
&\left| S(\rho_{BB'}) - \sum_i p_i S\left(\rho^i_{BB'}\right) - S(\rho_B) + \sum_i p_i S\left(\rho^i_B\right) \right| \\
&\quad \leqslant |S(\rho_{BB'}) - S(\rho_B)| + \left| \sum_i p_i S\left(\rho^i_{BB'}\right) - \sum_i p_i S\left(\rho^i_B\right) \right| \\
&\quad \leqslant S(\rho_{B'}) + \sum_i p_i S\left(\rho^i_{B'}\right) \leqslant 2S(\rho_{B'}),
\end{aligned}$$

*pawel@mif.pg.gda.pl

[1] For any quantum state $\rho$ one can define a concave function $S(\rho) \equiv -\mathrm{Tr}(\rho \log_2 \rho)$, called the von Neumann entropy, and its classical counterpart, the Shannon entropy, for a probability distribution $P$: $H(P) \equiv -\sum_x P(x) \log_2 P(x)$.

[2] For any bipartite state $\rho_{AB}$, one defines the quantum mutual information $I(A:B) = S(A) + S(B) - S(AB)$, and further, for a tripartite system $\rho_{ABC}$, the conditional quantum mutual information $I(A:B|C) = S(AC) + S(BC) - S(ABC) - S(C)$, where we use the notation for the entropy of $X$ system $S(\rho_X) = S(X)$.

[3] The Holevo function $\chi(\cdot)$ is defined for any ensemble of density matrices $\mathfrak{A} = \{p_i, \rho_i\}$ with average density matrix $\rho = \sum_i p_i \rho_i$ as follows: $\chi(\rho) = S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i)$, which is a good upper bound [13,14] on the accessible information.

 

where we applied the triangle inequality. This completes the proof. ■

One can use [5,6] a general tripartite pure state $\rho_{ABE}$ to generate a secret key between Alice and Bob. Alice engages in a particular strategy to perform a quantum measurement [positive operator-valued measure (POVM)] described by $Q=(Q_x)_{x\in\mathcal{X}}$, which leads to $\widetilde{\rho}_{ABE}=\sum_x |x\rangle\langle x|_A\otimes \mathrm{Tr}_A[\rho_{ABE}(Q_x)\otimes I_{BE}]$. Therefore, starting from many copies of $\rho_{ABE}$, we obtain many copies of cqq states $\widetilde{\rho}_{ABE}$ and we restate the theorem, defining a one-way secret key $K_{\rightarrow}$.

*Theorem 1* [5]. For every state $\rho_{ABE}$, $K_{\rightarrow}(\rho)=\lim_{n\to\infty}\frac{K^{(1)}_{\rightarrow}(\rho^{\otimes n})}{n}$, with $K^{(1)}_{\rightarrow}(\rho)=\max_{Q,T|X} I(X:B|T)-I(X:E|T)$, where the maximization is over all POVMs $Q=(Q_x)_{x\in\mathcal{X}}$ and channels $R$ such that $T=R(X)$ and the information quantities refer to the state $\omega_{TABE}=\sum_{t,x} R(t|x)P(x)|t\rangle\langle t|_T\otimes|x\rangle\langle x|_A\otimes \mathrm{Tr}_A(\rho_{ABE}(Q_x)\otimes I_{BE})$. The range of the measurement $Q$ and the random variable $T$ may be assumed to be bounded as $|T|\leqslant d_A^2$ and $|\mathcal{X}|\leqslant d_A^2$, where $T$ can be taken as a (deterministic) function of $\mathcal{X}$.

In the following, we define a modified version of the one-way secret key rate $K_{\rightarrow}$ based on the results of [8,10] for reduced intrinsic information and reduced entanglement measure.

*Definition 1*. For the one-way secret key rate $K^{(1)}_{\rightarrow}(\rho_{ABB'})$ of a bipartite state $\rho_{ABB'}\in B(\mathcal{H}_A\otimes\mathcal{H}_{BB'})$ shared between Alice and Bob, the reduced one-way secret key rate $K^{(1)}_{\rightarrow}\downarrow(\rho_{ABB'})$ is defined as

$$K^{(1)}_{\rightarrow}\downarrow(\rho_{ABB'})=\inf_{\mathcal{U}}[K^{(1)}_{\rightarrow}(\mathcal{U}(\rho_{AB}))+\Delta_{K_{\rightarrow}}], \tag{2}$$

where $\mathcal{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve; that is, $\mathcal{U}(\rho_{AB})=\mathrm{Tr}_{B'}(I\otimes\mathcal{U})\rho_{ABB'}$. $\Delta_{K_{\rightarrow}}=4S(\rho_{B'})$ denotes the defect parameter related to the increase of entropy produced by the transfer of the $B'$-subsystem from Bob's side to Eve after the action of $\mathcal{U}$.

The reduced one-way secret key rate is an upper bound on $K_{\rightarrow}$, which we prove now for every cqq state $\rho$.

*Theorem 2*. For every cqq state $\rho_{ABE}$, the following holds:

$$K_{\rightarrow}(\rho)=\lim_{n\to\infty}\frac{K^{(1)}_{\rightarrow}(\rho^{\otimes n})}{n}\leqslant K_{\rightarrow}\downarrow(\rho), \tag{3}$$

where $K_{\rightarrow}\downarrow(\rho)=\lim_{n\to\infty}\frac{K^{(1)}_{\rightarrow}\downarrow(\rho^{\otimes n})}{N}$. In particular, for the identity operation $\mathcal{U}=id$ on Bob's side, one obtains $K_{\rightarrow}(\rho_{ABB'})\leqslant K_{\rightarrow}(\rho_{AB})+4S(\rho_{B'})$.

To prove this theorem, one can start showing how the formula behaves for a one-copy secret key.

*Lemma 1*. For every cqq state $\rho_{ABE}$, the following holds:

$$K^{(1)}_{\rightarrow}(\rho)\leqslant K^{(1)}_{\rightarrow}\downarrow(\rho). \tag{4}$$

*Proof.* Since

$$\begin{cases} I(A:B|C)=S(AC)+S(BC)-S(ABC)-S(C),\\ I(A:E|C)=S(AC)+S(EC)-S(AEC)-S(C),\end{cases}$$

then

$$K^{(1)}_{\rightarrow}(\rho)=\max_{Q,C|A}[S(BC)-S(ABC)-S(EC)+S(AEC)].$$

To prove Lemma 1, it suffices to show that

$$K^{(1)}_{\rightarrow}(\rho_{A(BB')E})\leqslant K^{(1)}_{\rightarrow}(\rho_{AB(B'E)})+4S(B') \tag{5}$$

because, in the case of an application of $\mathcal{U}$ without discarding subsystem $B'$, one obtains an equality. We denote by $\rho_{AB(B'E)}$ a transition of the $B'$ subsystem to the environment. Both parts (Alice and Bob) use the maximizing local operations and classical communication (1-LOCC) protocol to find the secret key rate; thus, we omit further the maximization symbol, which reflects a choice of the maximizing protocol by Alice and Bob:

$$\begin{aligned}&S(BB'C)-S(ABB'C)-S(EC)+S(AEC)\\&\quad\leqslant S(BC)-S(ABC)-S(B'EC)+S(AB'EC)+4S(B').\end{aligned}$$

It is easy to note that the application of unitary operations on Bob's side does not change the inequality, mainly due to the property of unitary invariancy of the von Neumann entropy. To simplify the proof, one can decompose this inequality into the following two inequalities:

$$\begin{aligned}S(BB'C)-S(ABB'C)&\leqslant S(BC)-S(ABC)+2S(B'),\\ S(B'EC)-S(AB'EC)&\leqslant S(EC)-S(AEC)+2S(B'),\end{aligned} \tag{6}$$

or, equivalently considering the assumption that the initial state is of cqq type and $A$ represents the classical distribution, we can rewrite the first inequality in the form

$$\begin{aligned}S\Big(\sum_i p_i\rho_i^{BB'}\Big)-H(p_i)-\sum_i p_i S\big(\rho_i^{BB'}\big)-S\Big(\sum_i p_i\rho_i^{B}\Big)\\ +H(p_i)+\sum_i p_i S\big(\rho_i^{B}\big)\leqslant 2S(B')\end{aligned}$$

and, similarly for the second inequality, which gives as a result a more compact structure, we can write

$$\chi\big(\textstyle\sum_i p_i\rho_i^{BB'C}\big)-\chi\big(\sum_i p_i\rho_i^{BC}\big)\leqslant 2S(B'),$$

$$\chi\big(\textstyle\sum_i p_i\rho_i^{B'EC}\big)-\chi\big(\sum_i p_i\rho_i^{EC}\big)\leqslant 2S(B').$$

However, the above was proved in Observation 1, which completes the proof. ■

Finally, we extend this result in the asymptotic regime, proving Theorem 2.

*Proof.* To prove Theorem 2, it suffices to notice that (4) holds under 1-LOCC and an arbitrarily chosen $\mathcal{U}$ for any $\rho_n=\rho^{\otimes n}$. Moreover, the existence of the defect parameter $\Delta_{K_{\rightarrow}}$ enables regularization of the reduced one-way secret rate since, in the asymptotic regime after application of unitary operations on Bob's side (one can view his operation on the $B'$ system as an action of $\Lambda$ channel resulting from the unitary operations acting on the whole Bob side), one can apply subadditivity of entropy to estimate entropy of the transferred $B'$ part. In particular, for the identity operation, one achieves $S(\rho_{B'}^{\otimes n})=nS(\rho_{B'})$. This implies $K_{\rightarrow}(\rho_{ABB'})\leqslant K_{\rightarrow}(\rho_{AB})+4S(\rho_{B'})$. ■

It is interesting that our results reflect E nonlockability of the secret key rate [15], which means that the rate cannot be locked with information on Eve's side. Measures of classical or quantum correlations are lockable if they can decrease arbitrarily after measuring one qubit in a multipartite scheme—in this case by operations on Eve's side.

Monogamy of entanglement has been used to prove that for some region the quantum depolarizing channel has zero capacity even if does not destroy the entanglement [16], which is a particular application of the symmetric extendibility of states to evaluation of the quantum channel capacity. The following examples show application of the concept.

*Example 1.* As an example of application of Theorem 2, we present a state which, after discarding a small $B'$ part on Bob's side, becomes a symmetric extendible state [17]. This example is especially important since the presented state does not possess [18] any symmetric extendible component in its decomposition for symmetric and nonsymmetric parts; thus, one cannot use the method [19] to find an upper bound on $K_{\rightarrow}$ by means of linear optimization. Let us consider a bipartite quantum state shared between Alice and Bob on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \cong \mathcal{C}^{d+2} \otimes \mathcal{C}^{d+2}$:

$$\rho_{AB} = \frac{1}{2}\begin{bmatrix} \Upsilon_{AB} & 0 & 0 & \mathcal{A} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathcal{A}^{\dagger} & 0 & 0 & \Upsilon_{AB} \end{bmatrix}, \tag{7}$$

where $\mathcal{A}$ is an arbitrarily chosen operator so that $\rho_{AB}$ represents a correct quantum state. This matrix is represented in the computational basis $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ held by Alice and Bob and possesses a canonical maximally entangled state structure. Whenever one party (Alice or Bob) measures the state, the state decoheres and off-diagonal elements vanish, which leads to a symmetric extendible state [17],

$$\Upsilon_{AB} = \frac{d}{2d-1} P_+ + \frac{1}{2d-1} \sum_{i=1}^{d-1} |i\ 0\rangle\langle i\ 0|, \tag{8}$$

from which no entanglement or secret key can be distilled by means of 1-LOCC [17,19–21]. Therefore, by applying Theorem 2, one derives $K_{\rightarrow}(\Upsilon_{AB}) = 0$ and $K_{\rightarrow}(\rho_{AB}) \leqslant K_{\rightarrow} \downarrow (\rho_{AB}) = 4$.

*Example 2.* Let us consider a graph state [22] $|\mathcal{G}\rangle$ of a $(3n+1)$-qubit system associated with a mathematical graph $\mathcal{G} = \{\mathcal{V},\mathcal{E}\}$, composed of a set $\mathcal{V}$ of $3n+1$ vertices and a set $\mathcal{E}$ of edges $\{i,j\}$ connecting each vertex $i$ with some other $j$,

$$|\mathcal{G}\rangle = \bigotimes_{i,j\in\mathcal{E}} CZ_{ij}|\mathcal{G}_0\rangle, \tag{9}$$

where $3n+1$ qubits are initialized in the product state $|\mathcal{G}_0\rangle = \bigotimes_{i\in\mathcal{V}} |\psi_i\rangle$ with $|\psi_i\rangle = |0_i\rangle + |1_i\rangle$. Afterward, one applies a maximally entangling control-Z (CZ) gate to all pairs $\{i,j\}$ of qubits joined by an edge: $cz_{ij} = |0_i 0_j\rangle\langle 0_i 0_j| + |0_i 1_j\rangle\langle 0_i 1_j| + |1_i 0_j\rangle\langle 1_i 0_j| - |1_i 1_j\rangle\langle 1_i 1_j|$. If Alice takes no more than $n$ qubits from the graph system that is used to establish communication with Bob, who uses another $n$ qubits in this graph state, then they will be not able to set secure one-way communication by any means. This results from the fact that the state $\rho_{2n}^{AB}$ (with $n$ qubits on Alice's side and $n$ qubits on Bob's side) is symmetric extendible to a state $\rho_{3n}^{AB}$, which means that $K_{\rightarrow}(\rho_{2n}^{AB}) = 0$. A natural symmetric extension of $\rho_{2n}^{AB}$ is a state $\rho_{3n}^{AB} = \mathrm{Tr}_{B'}|\mathcal{G}\rangle\langle\mathcal{G}|$ resulting from tracing out an arbitrarily chosen qubit $B'$ from graph $\mathcal{G}$. However, if Alice takes $n$ qubits and Bob takes $n+1$ qubits from the graph system, the resulting state $\rho_{2n+1}^{AB}$ is no longer symmetric extendible. For example, for $n = 2$, this state has the spectral representation

$$\rho_{2n+1}^{AB} = \tfrac{1}{2}(|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|), \tag{10}$$

where $|\phi_0\rangle = |0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle$, $|\phi_1\rangle = |0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle$, and $\{|0\rangle_A = |00-01-10-11\rangle_A, |1\rangle_A = |00+01+10-11\rangle_A, |0\rangle_B = |001+010+100-111\rangle_B, |1\rangle_B = |000-011-101-110\rangle_B\}$. This state is isomorphic to a qubit bipartite state and meets the condition [23,24] for $\mathcal{C}^2 \otimes \mathcal{C}^2$ Bell-diagonal states to be symmetric extendible: $4\sqrt{\det(\rho_{AB})} \geqslant \mathrm{Tr}(\rho_{AB}^2) - \frac{1}{2}$. One can easily show the isomorphism of $\rho_{2n+1}^{AB}$ for any $n$ with a qubit bipartite state structure (10). Thus, for a one-way secret key of the state, $K_{\rightarrow}(\rho_{2n+1}^{AB}) \leqslant K_{\rightarrow} \downarrow (\rho_{2n+1}^{AB}) = 4$ holds, since after discarding one qubit $B'$ on Bob's side his system would become symmetric extendible.

## III. UPPER BOUND ON QUANTUM CHANNEL CAPACITY

The best known definition of the one-way quantum channel capacity $\mathcal{Q}_{\rightarrow}(\Lambda)$ [3,25] is expressed as an asymptotic regularization of coherent information: $\mathcal{Q}_{\rightarrow}(\Lambda) = \lim_{n\to\infty} \frac{1}{n} \sup_{\rho_n} I_c(\rho_n, \Lambda^{\otimes n})$ with parallel use of $N$ copies of the $\Lambda$ channel, where the one-copy formula is $\mathcal{Q}_{\rightarrow}^{(1)}(\Lambda) = \sup_{\rho} I_c(\rho,\Lambda)$. Coherent information for a channel $\Lambda$ and a source state $\sigma$ transferred through the channel is defined as $I_c(\sigma,\Lambda) = I^B(I\otimes\Lambda)(|\Psi\rangle\langle\Psi|)$, where $\Psi$ is a pure state with reduction $\sigma$, and coherent information of a bipartite state $\rho_{AB}$ shared between Alice and Bob is defined as $I^B(\rho_{AB}) = S(B) - S(AB)$. We use further the following notation: $I_c(A\rangle B) = I^B(\rho_{AB})$.

*Observation 2.* For a bipartite state $\rho_{ABB'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'})$ shared between Alice and Bob ($B$ and $B'$ system), the following holds:

$$I_c(A\rangle BB') \leqslant I_c(A\rangle B) + 2S(B'). \tag{11}$$

*Proof.* One can easily observe that, for subadditivity of entropy $S(BB') \leqslant S(B) + S(B')$ and for the Araki-Lieb inequality $|S(AB) - S(B')| \leqslant S(ABB')$, the left-hand side can be bounded as follows: $S(BB') - S(ABB') \leqslant S(B) + S(B') - S(AB) + S(B') = I_c(A\rangle B) + 2S(B')$, which completes the proof. ■

Motivated by the reduced quantity of the secret key rate and the preceding observation, we further derive the reduced version of the quantum channel capacity and show that it is a good bound on quantum channel capacity.

*Definition 2.* For a one-way quantum channel $\Lambda_{BB'}: B(\mathcal{H}_{BB'}) \to B(\mathcal{H}_{\tilde{B}\tilde{B}'})$, the reduced one-way quantum channel capacity is defined as

$$\mathcal{Q}_{\rightarrow}^{(1)} \downarrow (\Lambda_{BB'}) = \inf_{\mathcal{U}} [\mathcal{Q}_{\rightarrow}^{(1)}(\mathcal{U}(\Lambda_B)) + \Delta_{\mathcal{Q}_{\rightarrow}}], \tag{12}$$

where $\mathcal{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve after action of the $\Lambda_{BB'}$ channel, that is, $\mathcal{U}(\Lambda_B(\rho_B)) = \mathrm{Tr}_{B'}\mathcal{U}\Lambda_{BB'}(\rho_{BB'})$. $\Delta_{\mathcal{Q}_{\rightarrow}} = 2\sup_{\rho_{BB'}} S(\mathrm{Tr}_B\mathcal{U}\Lambda_{BB'}(\rho_{BB'}))$ denotes the defect parameter related to the increase of entropy produced by the transfer of the $B'$-subsystem from Bob's side to Eve after the action of $\mathcal{U}$.

*Theorem 3.* For any one-way quantum channel $\Lambda_{BB'}: B(\mathcal{H}_{BB'}) \to B(\mathcal{H}_{\widetilde{B}\widetilde{B}'})$,

$$\mathcal{Q}_{\to}(\Lambda_{BB'}) \leqslant \mathcal{Q}_{\to} \downarrow (\Lambda_{BB'}) \tag{13}$$

holds, where $\mathcal{Q}_{\to} \downarrow (\Lambda_{BB'}) = \lim_n \mathcal{Q}^{(1)}_{\to} \downarrow (\Lambda^{\otimes n}_{BB'})/n$ denotes the reduced quantum capacity. In particular, for the identity operation $\mathcal{U} = id$ on Bob's side, one obtains $\mathcal{Q}_{\to}(\Lambda_{BB'}) \leqslant \mathcal{Q}_{\to}(\Lambda_B) + 2\sup_{\rho_{BB'}} S(\mathrm{Tr}_B \Lambda_{BB'}(\rho_{BB'}))$.

To prove this inequality for regularized quantum capacity and its reduced version, it is sufficient to derive the following lemma for the single-copy case in analogy to Lemma 1 for the one-way secret key rate.

*Lemma 2.* For any one-way quantum channel $\Lambda_{BB'}: B(\mathcal{H}_{BB'}) \to B(\mathcal{H}_{\widetilde{B}\widetilde{B}'})$, the following holds:

$$\mathcal{Q}^{(1)}_{\to}(\Lambda_{BB'}) \leqslant \mathcal{Q}^{(1)}_{\to} \downarrow (\Lambda_{BB'}). \tag{14}$$

*Proof.* The proof of this lemma is straightforward with the application of Observation 2 that, for a state $\rho_{BB'}$ maximizing coherent information on the left-hand side of the observation, the above formula also holds for a possible transfer of $B'$ to the environment. It is worth recalling that an action of the unitary operator on a state does not change its entropy and, as a result, does not change the coherent information for any partition of the system. ■

Furthermore, one can complete the proof of the theorem in the asymptotic regime:

*Proof.* To prove the inequality of Theorem 3 asymptotically it suffices to notice that statements of Lemma 2 hold also for the arbitrarily chosen state $\rho_n = \rho^{\otimes n}$. Now we can prove that $\mathcal{Q}_{\to}(\Lambda_{BB'}) \leqslant \mathcal{Q}_{\to}(\Lambda_B) + \Delta_{\mathcal{Q}_{\to}}$. Let $\rho_n^{BB'}$ be a state maximizing $\mathcal{Q}_{\to}(\Lambda_{BB'})$ as an asymptotic regularization of coherent information; that is, $\mathcal{Q}_{\to}(\Lambda_{BB'}) = \lim_{n\to\infty} \frac{1}{n} I_c(\rho_n^{BB'}, \Lambda^{\otimes n}_{BB'})$, which one can represent as $I_c(A\rangle BB')$ for the aforementioned Choi-Jamiolkowski isomorphism between states and channels. Based on Observation 1, one can immediately derive for the maximizing state $\rho_n^{BB'}$: $\frac{1}{n} I_c(A\rangle BB') \leqslant \frac{1}{n}[I_c(A\rangle B) + 2S(\rho_n^{B'})]$, where $I_c(A\rangle B) = I_c(\mathrm{Tr}_{B'}\rho_n^{BB'}, \Lambda_B^{\otimes n})$ and $\rho_n^{B'} = \mathrm{Tr}_B \Lambda^{\otimes n}_{BB'}(\rho_n^{BB'})$. However, if there exists a state $\sigma_n^B$ for which $I_c(\sigma_n^B, \Lambda_B^{\otimes n}) > I_c(\mathrm{Tr}_{B'}\rho_n^{BB'}, \Lambda_B^{\otimes n})$, then it proves that the right-hand side of the inequality in the lemma can only be larger than in case of the chosen state $\rho_n^{BB'}$, which completes the proof. Finally, the aforementioned proof for key subadditivity of entropy can be applied to verify that, in the case of the regularized reduced secret key, its defect parameter cannot be larger than $\Delta_{\mathcal{Q}_{\to}} = 2\sup_{\rho_{BB'}} S(\mathrm{Tr}_B \mathcal{U}\Lambda_{BB'}(\rho_{BB'}))$, since for any state $\rho_{X_1\ldots X_n}$ and channel $\widetilde{\Lambda}$ there holds: $S(\widetilde{\Lambda}^{\otimes n}(\rho_{X_1\ldots X_n})) \leqslant \sum_i S(\widetilde{\Lambda}(\rho_{X_i}))$, which implies $\sup_{\rho_n^{BB'}} S(\mathrm{Tr}_B(\mathcal{U}\Lambda_{BB'})^{\otimes n}(\rho_n^{BB'})) \leqslant n \sup_{\rho_{BB'}} S(\mathrm{Tr}_B \mathcal{U}\Lambda_{BB'}(\rho_{BB'}))$. ■

*Example 3.* We use the aforementioned graph state from Example 2 and we search for the one-way channel capacity of a channel $\Lambda_{BB'}$, isomorphic due to the Choi-Jamiolkowski isomorphism, with a state $\rho^{ABB'}_{2n+1} = (I \otimes \Lambda_{BB'})|\Psi\rangle\langle\Psi|$. As above, after discarding the $B'$ 1-qubit system, the state would become symmetric extendible, which implies $Q_{\to}(\Lambda_B) = 0$. Therefore, we obtain $Q_{\to}(\Lambda_{BB'}) \leqslant 2$.

The power of the above results is especially visible in application of Theorem 3 to any channel reducible to an antidegradable channel for which the Choi-Jamiolkowski representation is symmetric extendible [23] or channels reducible to degradable channels which have known capacity [26].

## IV. DUAL PICTURE FOR ONE-WAY DISTILLABLE ENTANGLEMENT AND PRIVATE INFORMATION

Our results for the one-way secret key and quantum channel capacity lead immediately to a similar reduced formula for private information and one-way distillation quantities. The private capacity [7] $\mathcal{P}(\Lambda)$ of a quantum channel is equal to the regularization of private information, $\mathcal{P}^{(1)}(\Lambda) = \max_{X,\rho_x^A}[I(X,B) - I(X,E)]$, with maximization over classical random variables $X$ and input quantum states $\rho_x^A$ depending on the value of $X$. Absorbing $T$ into the variable $X$ in Theorem 1 leads to definitions for private information and private capacity [7]; thus, following Lemma 2, we can derive an upper bound on private information and private capacity via their reduced counterparts.

*Definition 3.* For a one-way quantum channel $\Lambda_{BB'}: B(\mathcal{H}_{BB'}) \to B(\mathcal{H}_{\widetilde{B}\widetilde{B}'})$, the reduced private information is defined as

$$\mathcal{P}^{(1)} \downarrow (\Lambda_{BB'}) = \inf_{\mathcal{U}}[\mathcal{P}^{(1)}(\mathcal{U}(\Lambda_B)) + \Delta_P], \tag{15}$$

where $\mathcal{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve; that is, $\mathcal{U}(\Lambda_B(\rho_B)) = \mathrm{Tr}_{B'}\mathcal{U}\Lambda_{BB'}(\rho_{BB'})$. $\Delta_P = 4S(\rho_{B'})$ denotes the defect parameter related to an increase of entropy produced by the transfer of the $B'$-subsystem from Bob's side to Eve after the action of $\mathcal{U}$.

*Theorem 4.* For a one-way quantum channel $\Lambda_{BB'}: B(\mathcal{H}_{BB'}) \to B(\mathcal{H}_{\widetilde{B}\widetilde{B}'})$,

$$\mathcal{P}(\Lambda_{BB'}) \leqslant \mathcal{P} \downarrow (\Lambda_{BB'}) \tag{16}$$

holds, where $\mathcal{P} \downarrow (\Lambda_{BB'}) = \lim_n \mathcal{P}^{(1)} \downarrow (\Lambda^{\otimes n}_{BB'})/n$ denotes the reduced private capacity. In particular, for the identity operation $\mathcal{U} = id$ on Bob's side, one obtains $\mathcal{P}(\Lambda_{BB'}) \leqslant \mathcal{P}(\Lambda_B) + 4S(\rho_{B'})$.

The proof can be conducted in analogy to Theorem 2 and Lemma 2, however, because the regularization of reduced private information it is crucial to derive the following lemma for a one-copy case.

*Lemma 3.* For every one-way quantum channel $\Lambda_{BB'}: B(\mathcal{H}_{BB'}) \to B(\mathcal{H}_{\widetilde{B}\widetilde{B}'})$, the following holds:

$$\mathcal{P}^{(1)}(\Lambda_{BB'}) \leqslant \mathcal{P}^{(1)} \downarrow (\Lambda_{BB'}). \tag{17}$$

*Proof.* To prove this lemma, it suffices to absorb variable $T$ into $X$ in Theorem 1 for the definition of private information and to conduct the proof in analogy to the proof of Lemma 1 for a channel $\Lambda_{BB'}$ and a chosen state $\rho$ sent through it. ■

We can now propose a new bound on distillation of entanglement by means of a one-way LOCC. This result is based on the observation [7] that one-way distillable entanglement $D_{\to}$ of a state $\rho_{AB}$ can be represented as the regularization of a one-copy formula, $D^{(1)}_{\to}(\rho_{AB}) = \max_{\mathbf{T}} \sum_{l=1}^{L} \lambda_l I_c(A\rangle B)_{\rho_l}$, where the maximization is over quantum instruments $T = (T_1, \ldots, T_L)$ on Alice's system, $\lambda_l = \mathrm{Tr}T_l(\rho_A)$, $T_l$ is assumed to have one Kraus operator $T_l(\rho) = A_l \rho A_l^{\dagger}$, and $\rho_l = \frac{1}{\lambda_l}(T_l \otimes id)\rho_{AB}$. Based on the results of Observation 2 and Lemma

2, we derive a general formula for the bound on one-way distillable entanglement applying the reduced quantity.

*Definition 4.* For a bipartite state $\rho_{ABB'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'})$ shared between Alice and Bob ($B$ and $B'$ system), the reduced one-way distillable entanglement is defined as

$$D^{(1)}_{\rightarrow} \downarrow (\rho_{ABB'}) = \inf_{\mathcal{U}} \left[ D^{(1)}_{\rightarrow}(\mathcal{U}(\rho_{AB})) + \Delta_{D_{\rightarrow}} \right], \qquad (18)$$

where $\mathcal{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve; that is, $\mathcal{U}(\rho_{AB}) = \mathrm{Tr}_{B'}(I \otimes \mathcal{U})\rho_{ABB'}$. $\Delta_{D_{\rightarrow}} = 2S(\rho_{B'})$ denotes the defect parameter related to the increase of entropy produced by the transfer of the $B'$-subsystem from Bob's side to Eve after the action of $\mathcal{U}$.

*Theorem 5.* For a bipartite state $\rho_{ABB'} \in B(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'})$ shared between Alice and Bob ($B$ and $B'$ system),

$$D_{\rightarrow}(\rho_{ABB'}) \leqslant D_{\rightarrow} \downarrow (\rho_{ABB'})$$

holds, where $\Delta_{D_{\rightarrow}} = 2S(\rho_{B'})$ and $D_{\rightarrow} \downarrow (\rho_{ABB'}) = \lim_n D^{(1)}_{\rightarrow} \downarrow (\rho^{\otimes n}_{ABB'})/n$ denotes the regularized version of reduced one-way distillable entanglement for one copy. In particular, for the identity operation $\mathcal{U} = id$ on Bob's side, one obtains $D_{\rightarrow}(\rho_{ABB'}) \leqslant D_{\rightarrow}(\rho_{AB}) + 2S(\rho_{B'})$.

The proof of this theorem can be conducted in analogy to the previous proofs for bounds on one-way secret keys and quantum channel capacity. The left inequality is an immediate implication of the following lemma for the one-copy formula.

*Lemma 4.* For every bipartite state $\rho_{ABB'}$, the following holds:

$$D^{(1)}_{\rightarrow}(\rho_{ABB'}) \leqslant D^{(1)}_{\rightarrow} \downarrow (\rho_{ABB'}). \qquad (19)$$

*Proof.* It suffices to use the results of Observation 2 to notice that, for a chosen set of instruments T on Alice's side for calculation of $D^{(1)}_{\rightarrow}(\rho_{ABB'})$, the inequality holds as an extension of the inequality from Observation 2 by multiplicands $\lambda_l$ on the left and right sides. However, if in case of calculating $D^{(1)}_{\rightarrow}(\rho_{AB})$ there exists a set T$'$ that maximizes $D_{\rightarrow}(\rho_{AB})$ better than T, then the right-hand side of the inequality can be only greater. ■

It is crucial to notice that the "defect" parameters $\Delta$ for the reduced quantities are subadditive and, hence, can be exploited in the case of composite systems and regularization.

*Corollary.* For the reduced quantities of $\{K_{\rightarrow}, \mathcal{P}, \mathcal{Q}_{\rightarrow}, D_{\rightarrow}\}$, for composite systems, $\Delta_X(\rho \otimes \sigma) \leqslant \Delta_X(\rho) + \Delta_X(\sigma)$ and $\Delta_Y(\Lambda \otimes \Gamma) \leqslant \Delta_Y(\Lambda) + \Delta_Y(\Gamma)$ hold, where $X = \{K_{\rightarrow}, D_{\rightarrow}\}$ and $Y = \{\mathcal{Q}_{\rightarrow}, \mathcal{P}\}$ stand for states for channels, respectively.

To prove the above corollary, it suffices to use the subadditivity of entropy for composite systems since Bob can act with a unitary operation before he discards some part of his subsystem. This property of the parameters enables regularization in the asymptotic regime of the reduced quantities for large systems $\rho^{\otimes n}$.

*Example 4: Activable multiqubit bound entangled states.* As an example illustrating this bound, we consider an activated bound entangled state $\rho_{II}$ [27], which is distillable if the parties (Alice and Bob) form two groups containing between 40% and 60% of all parties of the system in the state $\rho_{II}$. If Alice or Bob possess less than 40% of the system or if the system is shared between more than two parties, then the state becomes undistillable. This state for a large amount of particles can manifest features characteristic of "macroscopic entanglement" with no "microscopic entanglement." For a definition of the state, let us consider the family $\rho_N$ of $N$-qubit states: $\rho = \sum_{\sigma=\pm} \lambda_0^{\sigma} |\Psi_0^{\sigma}\rangle\langle\Psi_0^{\sigma}| + \sum_{k\neq 0} \lambda_k (|\Psi_k^{+}\rangle\langle\Psi_k^{+}| + |\Psi_k^{-}\rangle\langle\Psi_k^{-}|)$, where $|\Psi_k^{\pm}\rangle = \frac{1}{\sqrt{2}}(|k_1 k_2 \cdots k_{N-1} 0\rangle \pm |\bar{k}_1 \bar{k}_2 \cdots \bar{k}_{N-1} 1\rangle)$ are Greenberger-Horne-Zeilinger-like states with $k = k_1 k_2 \cdots k_{N-1}$ being a chain of $N-1$ bits and $k_i = 0,1$ if $\bar{k}_i = 1,0$; thus, the state is parametrized by $2^{N-1}$ coefficients. Let us consider now a bipartite splitting $\mathcal{P}$ where Alice takes $0.6N$ qubits and Bob takes the other $0.4N$ qubits. We can immediately show that $D_{\rightarrow}(\rho_{II}) \leqslant -2(\lambda_0^{\pm} + 2\sum_k \lambda_k) \log_2(\lambda_0^{\pm} + 2\sum_k \lambda_k)$ since, for Bob transferring one qubit to the environment, we obtain the undistillable state $D_{\leftrightarrow}(\rho_{N-1}) = 0$. It is noticeable that, even for a large macroscopic system with $N \to \infty$, $D_{\rightarrow}(\rho_{II}) \leqslant -2(\lambda_0^{\pm} + 2\sum_k \lambda_k) \log_2(\lambda_0^{\pm} + 2\sum_k \lambda_k)$. It can be easily shown that with the same method it is possible to achieve an upper bound on the one-way quantum channel capacity $Q_{\rightarrow}$.

## V. CONCLUSIONS

In this paper we proposed reduced versions of quantum quantities: a reduced one-way quantum key, distillable entanglement, and reduced corresponding capacities. We showed that in some cases these quantities may provide bounds on the nonreduced versions, drastically simplifying their estimations. It is evident especially for states of large systems, as supported by examples. The open problem is whether they can be applied to a nonadditivity problem of quantum channel capacities and quantum secure keys [11,26]. Furthermore, it is not known if they have analogs in general quantum networks or whether the bounds can be improved by better estimation of defect parameters.

## ACKNOWLEDGMENTS

The authors thank Michal Horodecki for critical comments on this paper. This work was supported by Ministry of Science and Higher Education Grant No. N202 231937 and by European Commission project Q-ESSENCE. Part of this work was performed at the National Quantum Information Center of Gdansk.

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

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

[3] H. Barnum, E. Knill, and M. A. Nielsen, IEEE Trans. Inf. Theory **46**, 1317 (2000).

[4] H. Barnum, M. A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).

[5] I. Devetak and A. Winter, Proc. R. Soc. London A **461**, 207 (2005).
[6] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).
[7] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[8] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 200501 (2005).
[9] K. Horodecki *et al.*, IEEE Trans. Inf. Theory **55**, 1898 (2009).
[10] R. Renner and S. Wolf, Lect. Notes Comput. Sci. Eng. **2656**, 562 (2003).
[11] G. Smith and J. Yard, Science **321**, 1812 (2008).
[12] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[13] A. S. Holevo, Tamagawa Univ. Res. Rev. **4**, 1 (1998).
[14] A. S. Holevo, Probl. Inf. Transm. (USSR) **9**, 177 (1973).
[15] M. Christland, A. Ekert *et al.* Lect. Notes Comput. Sci. **4392**, 456 (2007).
[16] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[17] M. L. Nowakowski and P. Horodecki, J. Phys. A **42**, 135306 (2009).
[18] M. L. Nowakowski (unpublished).
[19] T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).
[20] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
[21] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[22] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
[23] G. O. Myhr and N. Lütkenhaus, Phys. Rev. A **79**, 062307 (2009).
[24] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lutkenhaus, Phys. Rev. A **79**, 042329 (2009).
[25] C. H. Bennett, D. P. Di Vincenzo, J. Smolin, and W. K.Wootters, Phys. Rev. A **54**, 3824 (1996).
[26] G. Smith, J. A. Smolin, and A. Winter, IEEE Trans. Inf. Theory **54**, 4208 (2008).
[27] W. Dür and J. I. Cirac, Phys. Rev. A **62**, 022302 (2000).