# Upper bounds on the leakage of private data and an operational approach to Markovianity

Karol Horodecki,[1,2] Michał Studziński,[3] Ryszard P. Kostecki,[1,2] Omer Sakarya,[1] and Dong Yang[4,5]

[1]*Institute of Informatics, National Quantum Information Centre in Gdańsk, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*

[2]*International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-952 Gdańsk, Poland*

[3]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre in Gdańsk, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*

[4]*Department of Informatics, University of Bergen, 5020 Bergen, Norway*

[5]*Laboratory for Quantum Information, China Jiliang University, 310018 Hangzhou, China*

(Received 22 July 2021; revised 11 October 2021; accepted 5 November 2021; published 19 November 2021)

We quantify the consequences of a private key leakage and private randomness generated during quantum key distribution. We provide simple lower bounds on the one-way distillable key after the leakage has been detected. We also show that the distributed private randomness does not drop by more than twice the number of qubits of the traced-out system. We further focus on irreducible private states, showing that their two-way distillable key is nonlockable. We then strengthen this result by referring to the idea of recovery maps. We further consider the action of a special case of side channels on some of the private states. Finally, we connect the topic of (non-)Markovian dynamics with that of hacking. In particular, we show that an invertible map is non-CP-divisible if and only if there exists a state whose the key witnessed by a particular privacy witness increases in time. This complements the recent result of J. Kołodyński *et al.* [Phys. Rev. A **101**, 020303(R) (2020)] where the log-negativity was connected with the (non-)Markovianity of the dynamics.

DOI: 10.1103/PhysRevA.104.052422

## I. INTRODUCTION

While the security of quantum key distribution is proven in theory, it usually lacks in practice. This is mainly because of (i) the imperfections in the production of the quantum key distribution (QKD) equipment and/or (ii) the active attacks of the eavesdropper known as Trojan horse attacks (THAs) [1,2]. The latter attacks, such as active inspection of the inner workings of the honest parties' device, can lead to a leakage of the secret key. Recently there has been taken effort to study the performance of QKD, which takes into account particular examples of the leakages [3,4] in the case of quantum key distribution as well as the measurement-device independent quantum key distribution.

In this paper, we consider a more drastic version of THA, according to which eavesdropper gets access to the very *raw* key of the honest parties' device. We then note that most of the up-to-date QKD protocols are using in practice one-way communication. (We consider here both device dependent [5] and independent [6,7] cases, see Ref. [8] and references therein.) Their performance is further based on protocols originating from the Devetak–Winter protocol [9]. We, therefore, focus on the lower bounds on the drop of the *raw* key that can be obtained via the latter protocol. It is a practically relevant problem since the raw key should be destroyed properly after key generation. Indeed, the part of the raw key, which does not form the final key, can be a source of potential leakage and thus should be irreversibly destroyed. Hence, we study how the incorrectly destroyed raw key can influence the security of the key.

Our findings are related to the *lockability* of a resource: the problem of how much a given resource drops down under action on (e.g., erasure of) a subsystem of a bipartite quantum state. There are two variants of the nonlockability of a resource. According to one of it, the resource should go down by less than the $S(a)$ upon the erasure of system $a$, where $S$ is the von Neumann entropy. We will call it a *strong nonlockability*. A weaker version states that there exists constant $c > 0$, independent of the dimension of the state under consideration, such that the resource does not go down by more than $cS(a)$ (or $c\log_2|a|$). We will call it a *nonlockability*.

Violation of the strong nonlockability was proven in Ref. [10] for the so called *accessible information*. The lockability of entanglement measures has been first considered in Ref. [11], where entanglement cost $E_C$ [12] was shown to be lockable, while the relative entropy $E_R$ of entanglement was shown to be nonlockable with $c = 2$. In Ref. [13], lockability of the squashed entanglement $E_{sq}$ was shown.

*a. Motivation.* Before showing the main results, we discuss three possible ways in which the eavesdropper can arrange local leakage, which come as a motivation for further studies.

It is known that the eavesdropper can monitor power consumption or the electromagnetic radiation of a working device [3]. One can also consider a drastic *hardware* THA. Every device which performs quantum key distribution, no matter how shielded, has an incoming fiber. This implies a hole in the shielding. It is then enough to set up a sufficiently strong radioactive source with an open-close mechanism. The bits of generating key can be stored in local memory and further leaked by an open-close mechanism outside via the presence of radiation (1) or lack of it (0) in a given slot of time. Monitoring the radioactivity implies directly the leakage of the key. Constant monitoring of radioactivity outside of the device could be a countermeasure to it.

Another attack can be considered in the case of device independent quantum key distribution. It was noticed in Ref. [14] that such a device can be used only once. If used twice, it can leak the key from its previous use by means, e.g., of the accept-abort mechanism. Hence, a device should be destroyed after a single use. This applies not only to the electronics or memory but also to the shielding. This is because shielding can contain a small memory that stores the data. Such an attack can be easily refuted by destroying of the device in the enough irreversible way.

The easiest way of attack is to set up software that copies the output of the device (a raw key) and distributes it to the eavesdropper. This can be noticed if the system hosting software is constantly monitored. However, noticing the attack does not always mean that it can be stopped, as exemplified by an important variant of this attack: a theft of data. The erasure of classical data happens when the *ransomware* (malicious software aimed at ransom) is used by the hackers. Ransomware encrypts the data, which are therefore practically lost unless the (former) owner pays a tribute.

The question is: how much of the security is still at hand after the leakage of the raw key has happened? The bounds obtained in the form of the order of leakage (denoted by constant $c$) considered in the introduction can help in *estimation* of the loss of data and lead to further shortening of the raw key to obtaining smaller yet still secure key. For example, in the case of a cloud-storage device exposed for a certain period of time, $\tau$ seconds, to an uncontrolled connection with a certain speed, $v$ megabits per second, one can conclude that no more than $cv\tau$ of megabits were exposed to the attack. (To detect which of the data happened to be copied or erased, one can use the trapdoor mechanism [15]).

*b. Main results.* We first consider one of quantum cryptography's fundamental resources, which is the randomness private against a quantum adversary. It is used, e.g., by protocols of generation of the secure key when the honest parties choose settings of measurements (see, e.g., Ref. [16] for review). We focus on a bipartite case introduced in Ref. [17]. There, two mutually trusting honest parties are distilling private randomness for each of them separately from many copies of a bipartite state $\rho_{AB}$ in the form of an ideal state $\frac{\mathbf{1}_A}{|A|} \otimes \frac{\mathbf{1}_B}{|B|} \otimes \rho_E$, where $\rho_E$ is the purifying system of $\rho_{AB}$. The operations which they use in this resource theory are (i) local unitary operations and (ii) sending quantum states via dephasing channel to the other party (this choice assures that the operations are free, i.e., do not create private randomness).

As the first main result, we show a lower bound on the drop of private randomness distillable in this scenario. Namely, for a bipartite state, under action of (local) unitary transformation followed by partial trace of a subsystem $a$, private randomness does not drop down by more than $S(a) + \log_2 |a|$, where $|a|$ is the dimension of $a$. In this scenario, one can also consider the rate of randomness obtained without operation (ii) and with or without borrowing local noise [17]. Our bound holds in all these cases.

Before turning to the problem of (non)lockability of the key secure against a quantum adversary, let us recall basic facts about the states containing ideal key, called private states [18,19]. A private state has two subsystems: system $AB$ is called the *key part* while system $A'B'$ is called a shield [19]. By definition, one can draw $\log_2 |AB|$ of the key via direct von-Neumann measurement on its key part. To test how much key drops down for a given private state, we need to control how much key it contains from the beginning. However, a private state can have the potentially large key contained in its shielding system $A'B'$. To avoid this problem, we focus on the so-called irreducible private states that have $\log_2 |AB|$ of key—exactly as much as it is directly accessible via the von-Neumann measurement on their key part.

As the first result related to the secure key, we show that the key of private states is nonlockable. Precisely, it cannot drop down by erasing system $a$ on one side of it, by more than $2S(a)$. In that, we partially address the open problem of whether the distillable key can be locked, as presented on the IQOQI list of open problems [20].

We then provide first simple bounds on the loss of the *raw* one-way distillable key secure against quantum adversary under erasure of data. By one-way distillable key, we mean the one obtained by utilizing one-way classical communication from Alice to Bob. By the raw key, we refer to the key generated via measurement on Alice's side on a quantum state shared by the honest parties. The raw key then is the bit string that the honest parties share before applying error correction and privacy amplification [21].[1]

As one of the main results, we show that the considered type of key is strongly nonlockable (see theorem 4). More precisely, it does not drop down by more than $\alpha$ upon the erasure of a system $a$. Similar results are obtained for the drop of the system at Bob's site: it does not drop down by more than $4\alpha$ upon the erasure of a system $b$ with its entropy scaling with the number of the raw key bits as $n\alpha$.

It is also natural to consider *copying* of the data by an adversary, which is a much easier attack than the one described above. In that case, we also observe the nonlockability of the one-way distillable key. It does not drop down by more than $2\alpha$.

Employing simple properties of the *smooth min and max entropies* [22], we also provide an alternative lower bound on the drop of the one-way key which reads, in the case considered above, $\log_2 |a|$.

*Bounds on the leakage of two-way distillable key for generalized private states via the fidelity of recovery.* The bounds presented above do not consider the fact that the system $a$ (or $b$ for Bob) can be almost uncorrelated with the rest of the state of the honest parties. In that case, the drop of the key should be less than the entropy of the copied or erased system. In particular, when the system $a$ is a product with the rest of the system, the drop of the key should be equal to zero.

[1] We note here that in this paper by (ideal) key, we mean the key for the one-time pad, i.e., uniformly random, perfectly correlated pair of bit-strings shared by two honest parties, known only to them. It can be represented by a state $\sum_{i=0}^{d-1} \frac{1}{d} |ii\rangle\langle ii|_{AB} \otimes \rho_E$, where $\rho_E$ represents the total knowledge of the quantum adversary.

To address this case, we use the concept known as *fidelity of recovery* [23], $F_R$. For arbitrary tripartite state $\rho_{aAB}$, fidelity of recovery is the maximum quantum fidelity of $\rho_{aAB}$ with the state $\tilde{\rho}_{AB\tilde{a}} = \Gamma_{A\to A\tilde{a}}(\rho_{AB})$ recovered by a local quantum map $\Gamma$ acting on system $A$, after erasure of the system $a$. It has been shown [23] that $F_R$ is lower bounded from below by a function $2^{-I(a:B|A)}$, where the conditional mutual information reads $I(a:B|A) := S(aA) + S(BA) - S(A) - S(ABa)$. While the latter relation is often treated as (in fact, suboptimal) lower bound on the quantum conditional mutual information, we focus here on the operational meaning of the fidelity of recovery. The conditional mutual information $I(a:B|A)$ quantifies, to some extent, how much the system $a$ is correlated with the remaining systems. The lower it is, the tighter bound we obtain.

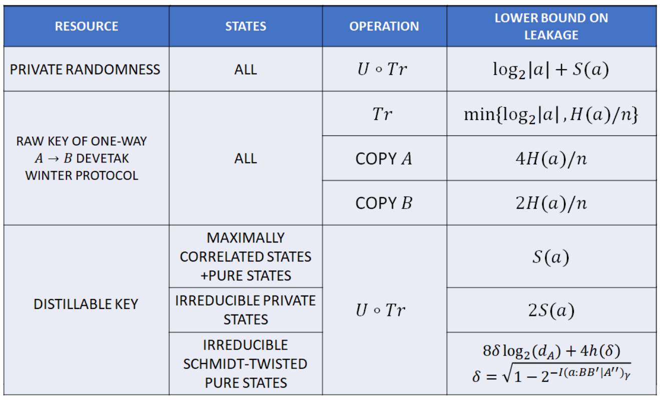
The above relationship allows us to show that the one-way distillable key achieved by i.i.d. operations can not drop down too much if $I(a:B|A)$ is low. By i.i.d., we mean that it is achieved by identical measurement operation and classical preprocessing on each copy of the input state, followed by error correction and privacy amplification [9]. Although such a quantity may be much lower than the distillable key for a general state, it is equal to the distillable key for certain generalization of private states called *irreducible Shmidt-twisted pure states*. Before stating the results, let us discuss this generalization. A private state can be seen as "twisted" singlet state $|\Psi_+\rangle$: $\gamma_{ABA'B'} = U|\Psi_+\rangle\langle\Psi_+|\otimes\sigma_{A'B'}U^\dagger$, where $\sigma_{A'B'}$ is an arbitrary state and $U = \sum_i |ii\rangle\langle ii|\otimes U_i$ is a control unitary transformation called twisting. We generalize this, by inserting a pure state $|\Phi\rangle$ in place of the singlet, and allow the unitary $U$ to control the Schmidt basis of $|\Phi\rangle$ that is a basis in which it can be written as $|\Phi\rangle = \sum_i \sqrt{\lambda_i}|ii\rangle$. The obtained state $\gamma'_{ABA'B'}$ we call the *irreducible Shmid-twisted pure state*, when $K_D(\gamma') = S(A)_\Phi$ that is the amount of key equals the entropy of the subsystem of the state $|\Phi\rangle\langle\Phi|$.

The following result encapsulates our findings: for any irreducible Schmidt-twisted pure states $\widetilde{\gamma}_{ABA'B'}$, after action $AA' \to A''a$ and partial trace of system $a$, there is

$$K_D(\widetilde{\gamma}_{A''BB'}) \geqslant K_D(\widetilde{\gamma}_{aA''BB'}) - (8\delta\log_2 d_A + 4h(\delta)) \qquad (1)$$

with $\delta = \sqrt{1 - 2^{-I(a:B|A)}}$ (see proposition 3), where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy. Note that the bound (1) generalizes result for pure states that the key is not lockable (see theorem 3). These and other results are presented in a unified way in Fig. 1.

*Attacks on private states.* It has been recently proposed [24] that certain private states can serve as a resource for the so called *hybrid quantum networks* (a variant of quantum network secure against unauthorized key generation). Therefore we also study special attacks on a particular class of private states. We consider several side channels, such as depolarising and amplitude-damping, acting on a shield of a private state. We focus on the private state that can be constructed from an operator $X$ being a (normalized) swap gate [see Eq. (8) in Sec. II]. The main insight is that the key drops down by the same amount, no matter how large the system shielding the key is. Therefore the larger the shield is, the more vulnerable to noise this particular private state becomes.



| RESOURCE | STATES | OPERATION | LOWER BOUND ON LEAKAGE |
|---|---|---|---|
| PRIVATE RANDOMNESS | ALL | $U\circ Tr$ | $\log_2\lvert a\rvert + S(a)$ |
| RAW KEY OF ONE-WAY $A\to B$ DEVETAK WINTER PROTOCOL | ALL | $Tr$ | $\min\{\log_2\lvert a\rvert, H(a)/n\}$ |
| | | COPY $A$ | $4H(a)/n$ |
| | | COPY $B$ | $2H(a)/n$ |
| DISTILLABLE KEY | MAXIMALLY CORRELATED STATES +PURE STATES | $U\circ Tr$ | $S(a)$ |
| | IRREDUCIBLE PRIVATE STATES | | $2S(a)$ |
| | IRREDUCIBLE SCHMIDT-TWISTED PURE STATES | | $8\delta\log_2(d_A) + 4h(\delta)$<br>$\delta = \sqrt{1 - 2^{-I(a:BB'\lvert A'')_\gamma}}$ |

FIG. 1. Summary of the main results. For either private randomness or private key and a given class of states, we provide lower bounds on the operation (unitary $U$ composed with partial trace, partial trace, and copying of a system, respectively) on system $a$ with the von-Neumann entropy $S(a)$ and dimension $|a|$. $I(a:BB'|A'')$ is the conditional mutual information.

*(Non)-Markovianity meets hacking.* We connect two topics, which are usually considered as quite far from each other: the leakage of the private key and the (non)-Markovianity of quantum dynamics. We consider states of the form $\rho_{ABA'B'} = p_+|\psi_+\rangle\langle\psi_+|_{AB}\otimes\rho_+^{A'B'} + p_-|\psi_-\rangle\langle\psi_-|_{AB}\otimes\rho_-^{A'B'}$, and let $X = \frac{1}{2}(p_+\rho_+^{A'B'} - p_-\rho_-^{A'B'})$. We argue that the distillable key of the so called *privacy squeezed state* of $\rho_{ABA'B'}$ exposed to hacking reads

$$K_D([\Lambda(\rho_{ABA'B'})]_{psq}) = 1 - h\big(\tfrac{1}{2} + ||(\Lambda_{A'}\otimes\mathbf{1}_{B'})X||_1\big), \qquad (2)$$

where $\Lambda(\rho_{ABA'B'}) = \Lambda_{A'}\otimes\mathbf{1}_{ABB'}(\rho_{ABA'B'})$, and $\Lambda_{A'}$ is a CPTP map acting on the system $A'$ of $\rho_{ABA'B'}$, which corresponds to action of hacking. Moreover $[\cdot]_{psq}$ is the so called *privacy squeezing* [19] [defined in Eq. (11)]. The privacy squeezing operation is considered here only as a mathematical tool rather than a physical map (although it can be physically realized). It allows to place a lower bound on the distillable key of a given quantum state. Indeed, we have $K_D(\rho) \geqslant K_D([\rho]_{psq})$ [19]. The result presented in Eq. (2) allows us not only to study the power of leakage of certain quantum channels, but also to connect the behavior of $||X||_1$ due to leakage under hacking with non-Markovianity of quantum dynamics. (We identify *Markovianity* with *CP divisibility* [25,26]). Using the results of Refs. [27,28], and in analogy to [29], we show that the non-Markovianity of (invertible or image nonincreasing) dynamics, given by a family $\{\Lambda_t \mid t \geqslant 0\}$ of CPTP maps acting on $A'$, is equivalent with

$$\frac{d}{dt}K_D([\Lambda_t(\rho)]_{psq}) > 0. \qquad (3)$$

## II. FACTS AND NOTATIONS

In this section, we invoke important facts and notation used throughout the paper. By $S(\rho_X)$ and $S(\rho_{XY})$, we will mean the von Neumann entropy of systems $X$ and $XY$, respectively. We will also write $S(X)$ and $S(XY)$ if the state is understood from the context. A bipartite state is called a maximally correlated state (MCS) if it is of the form

$$\rho_{AB} = \sum_{i,j} c_{ij} |ii\rangle\langle jj|_{AB}, \tag{4}$$

where $c_{ij}$ are arbitrary complex numbers. The classical-quantum (cq) state is any state of the form

$$\rho_{cq} = \sum_{i} p_i |i\rangle\langle i| \otimes \rho_i. \tag{5}$$

It is straightforward to check that

$$S(\rho_{cq}) = H(\{p_i\}) + \sum_i p_i S(\rho_i), \tag{6}$$

where $H$ denotes Shannon entropy of a distribution $\{p_i\}$.

The private states [18,19] have the form

$$\gamma_{ABA'B'} = \sum_{i,j} \frac{1}{d} |ii\rangle\langle jj|_{AB} \otimes U_i \sigma U_j^\dagger, \tag{7}$$

where $\sigma$ is an arbitrary state on $A'B'$ system. The private state $\gamma$ is called *irreducible* if $K_D(\gamma) = \log_2 d$, where $d$ is the dimension of the system $AB$ called the *key part*.

The class of irreducible private states is not characterized due to the fact that there can possibly exist states that have zero distillable key but are entangled [30]. Hence we also consider a well characterized, possibly strict subset of irreducible private states, called in [31] *strictly irreducible private states*. The operational meaning of this class is the following. Conditionally on measuring the key part of a strictly irreducible state in a standard basis, there always appears a separable state on their shielding system. Formally, the state (7) is called *strictly irreducible* iff the conditional states $U_i \sigma U_i^\dagger$ in Eq. (7) are separable (i.e., they are mixtures of product states) for all $i$. This feature assures that $K_D(\gamma) = \log_2 d$ where $d$ is the dimension of the key part [32]. In the case of a private bit, i.e., $d = 2$, the private state can be represented by a single operator $X$ with trace norm $||X||_1 = \mathrm{Tr}\sqrt{XX^\dagger}$ equal to $1/2$:

$$\begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix}. \tag{8}$$

In Ref. [31], it is shown how to use a one-way local operation and classical communication to transform any private bit represented by $X$ into a one represented by *Hermitian* $\tilde{X}$. Hence, in our considerations, we can focus on hermitian $X$.

The action of leakage via the map acting on the shielding system returns the following matrix:

$$\begin{bmatrix} \Lambda_{A'} \otimes \mathrm{I}_{ABB'} \sqrt{XX^\dagger} & 0 & 0 & \Lambda_{A'} \otimes \mathrm{I}_{ABB'} X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \Lambda_{A'} \otimes \mathrm{I}_{ABB'} X^\dagger & 0 & 0 & \Lambda_{A'} \otimes \mathrm{I}_{ABB'} \sqrt{X^\dagger X} \end{bmatrix}. \tag{9}$$

To express the connection of the leakage of the key and (non)-Markovianity, we will need to broaden the class of the interest to states of the form

$$\rho_{\text{block}} := p_+ |\psi_+\rangle\langle\psi_+| \otimes \rho_+ + p_- |\psi_-\rangle\langle\psi_-| \otimes \rho_- \tag{10}$$

(where $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$), which are private states when $\rho_+ \perp \rho_-$. Following Ref. [31], we will call them the *block states*. An important operation on them is the one that outputs the privacy squeezed state $\rho_{psq}$, i.e., the two-qubit bipartite state of the form

$$\rho_{psq} := \begin{bmatrix} \frac{p_+ + p_-}{2} & 0 & 0 & \frac{||p_+\rho_+ - p_-\rho_-||_1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{||p_+\rho_+ - p_-\rho_-||_1}{2} & 0 & 0 & \frac{p_+ + p_-}{2} \end{bmatrix}. \tag{11}$$

There is [19]

$$K_D(\rho_{\text{block}}) \geqslant K_D(\rho_{psq}), \tag{12}$$

where $K_D$ is a key distillable by LOCC operations, defined rigorously in Sec. II D. Due (12), the secure key content of the state $\rho_{psq}$ can be treated as a (nonlinear) witness of privacy for the state $\rho$ [33].

For a given pure state $|\Phi\rangle_{AB}$ let us consider its Schmidt decomposition $|\Phi\rangle_{AB} = \sum_i \lambda_i |e_i\rangle \otimes |f_i\rangle$, where $\lambda_i \geqslant 0$, and $\sum_i \lambda_i = 1$. A twisting operation in the Schmidt basis of a state $|\Phi\rangle_{AB}$ is given by

$$U = \sum_{i,j} |e_i f_j\rangle\langle e_i f_j|_{AB} \otimes U_{A'B'}^{(ij)}, \tag{13}$$

where for each $(ij)$, $U_{A'B'}^{(ij)}$ is some unitary operation. This leads to a concept of the *Schmidt-twisted pure state* $\widetilde{\gamma}_{ABA'B'}$, which is defined as

$$\begin{aligned} \widetilde{\gamma}_{ABA'B'} &:= U(|\Phi\rangle\langle\Phi|_{AB} \otimes \sigma_{A'B'})U^\dagger \\ &= \sum_{i,j} \lambda_i \lambda_j |e_i f_i\rangle\langle e_j f_j| \otimes U_i \sigma U_j^\dagger, \end{aligned} \tag{14}$$

where $\sigma$ is defined on systems $A'$ and $B'$ (for clarity, we suppressed subsystem indices). The Schmidt-twisted pure state $\widetilde{\gamma}_{ABA'B'}$ is called irreducible if it satisfies $K_D(\widetilde{\gamma}_{ABA'B'}) = S(A)_\Phi$. This means that its whole security content is accessible by a direct von Neumann measurement on its key part system $AB$.

Finally, for self-consistence of this manuscript, we define the Uhlmann fidelity [34,35] for two quantum states $\rho$ and $\sigma$:

$$F(\rho, \sigma) := (\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2. \tag{15}$$

This expression can be written in equivalent form $||\sqrt{\rho}\sqrt{\sigma}||_1^2$, where $||\cdot||_1$ denotes trace norm.

### A. Entanglement measures

Here, we introduce entanglement measures that are employed in this manuscript—the relative entropy of entanglement, distillable entanglement, and squashed entanglement.

*Definition 1.* The relative entropy of entanglement for an arbitrary density operator $\rho$ is defined as

$$E_R(\rho) := \inf_{\omega \in \mathcal{SEP}} D(\rho|\omega), \tag{16}$$

where the infimum runs over the set of separable states $\mathcal{SEP}$, and $D(\cdot|\cdot)$ denotes relative entropy, i.e., $D(\rho|\sigma) := \mathrm{tr}\rho \log_2 \rho - \mathrm{tr}\rho \log_2 \sigma$, for an arbitrary density operators $\rho, \sigma$.

*Definition 2.* For all bipartite states $\rho_{AB}$, we define one-way distillable entanglement

$$E_D^{\rightarrow} := \lim_{\epsilon\to 0}\lim_{n\to\infty}\sup_{\Lambda_{A\to B}}\{E : \Lambda(\rho^{\otimes n}) \approx_\epsilon \Phi_{AB}(2^{nE})\}, \tag{17}$$

where maps $\Lambda_{A\to B}$ are restricted to one-way *LOCC*, and $\Phi_{AB}(2^{nE})$ is maximally entangled state between $A$ and $B$ of Schmidt rank $2^{nE}$.

In the above expressions, we use the notation $\rho \approx_\epsilon \sigma$ for $||\rho - \sigma||_1 \leqslant \epsilon$ to compress the definitions.

*Definition 3.* The squashed entanglement [36] for an arbitrary bipartite sate $\rho_{AB}$ is defined as

$$E_{sq}(\rho_{AB}) := \inf_{\rho_{ABE}}\left\{\tfrac{1}{2}I(A;B|E) \mid \rho_{ABE} \text{ extension of } \rho_{AB}\right\}. \tag{18}$$

The infimum is taken over all extensions of $\rho_{AB}$, i.e., over all density operators $\rho_{ABE}$ with $\rho_{AB} = \mathrm{tr}_E\,\rho_{ABE}$. By $I(A;B|E) := S(AE) + S(BE) - S(ABE) - S(E)$ we denote the quantum conditional mutual information of $\rho_{ABE}$ [37]. $S(A) := S(\rho_A)$ is the von Neumann entropy of the underlying state.

### B. Min and max entropies and their smoothed versions

We begin from defining the min and max entropies (see Refs. [21,22,38] for the details). For a given bipartite state $\rho_{AB}$, they are given by

$$\begin{aligned} H_{\min}(A|B)_\rho &:= \sup_{\sigma_B}\sup\{\lambda\in\mathbb{R} : \rho_{AB} \leqslant 2^{-\lambda}\mathbf{1}_A\otimes\sigma_B\},\\ H_{\max}(A|B)_\rho &:= \max_{\sigma_B}\log_2 F(\rho_{AB}, \mathbf{1}_A\otimes\sigma_B), \end{aligned} \tag{19}$$

where $F(\rho,\sigma) = ||\sqrt{\rho}\sqrt{\sigma}||_1$ denotes fidelity between quantum states $\rho$ and $\sigma$. The $\epsilon$-smooth min and max entropies of $A$ conditioned on $B$ of the state $\rho_{AB}$ read, respectively,

$$\begin{aligned} H^\epsilon_{\min}(A|B)_\rho &:= \max_{\widetilde{\rho}_{AB}\in\mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|B)_{\widetilde{\rho}},\\ H^\epsilon_{\max}(A|B)_\rho &:= \min_{\widetilde{\rho}_{AB}\in\mathcal{B}^\epsilon(\rho_{AB})} H_{\max}(A|B)_{\widetilde{\rho}}, \end{aligned} \tag{20}$$

where $\mathcal{B}^\epsilon(\rho_{AB})$ is $\epsilon$-ball of states $\widetilde{\rho}_{AB}$ which are $\epsilon$-close to $\rho_{AB}$. For the further considerations, let us also remind here that the smooth entropies of the i.i.d. product state $\rho_{A^nB^n} = \rho_{AB}^{\otimes n}$ converge to conditional Shannon entropy $H_\rho(A|B)$ for $n\to\infty$. More precisely,

$$\begin{aligned} &\lim_{n\to\infty}\left\{\frac{1}{n}H^\epsilon_{\min}(A^n|B^n)_\rho\right\} \geqslant H(A|B)_\rho,\\ &\lim_{n\to\infty}\left\{\frac{1}{n}H^\epsilon_{\max}(A^n|B^n)_\rho\right\} \leqslant H(A|B)_\rho. \end{aligned} \tag{21}$$

### C. Key distillable by LOPC operations

For further purposes, we remind here the idea of the LOPC, local (quantum) operations, and public classical communication, with corresponding distillable key $C_D$ for tripartite quantum state $\rho = \rho_{ABE}$. In this scenario, three parties, Alice, Bob, and Eve, hold many systems in the same tripartite state $\rho$. Alice and Bob can process input states by quantum operations, each in their respective laboratory, and they communicate publicly classical messages, with copies also sent to eavesdropper Eve. For a more formal definition of LOPC operations, see definition 4.2 in Refs. [32,39]. Historically, its one-way version was defined first in Ref. [9], in a way equivalent to the following one, where $\rho \equiv \rho_{ABE}$,

$$K_{\rightarrow}(\rho) := \inf_{\epsilon>0}\limsup_{n\to\infty}\sup_{\Delta\in\mathrm{LOPC}_{\rightarrow}}\left\{\frac{\log_2 d}{n}\middle|\Delta(\rho^{\otimes n}) \approx_\epsilon \tau_d\right\}, \tag{22}$$

where $\mathrm{LOPC}_{\rightarrow}$ denotes the LOPC operations, in which the classical communication goes from $A$ to $B$ only, while $\tau_d = (1/d)\sum_{i=1}^{d-1}|ii\rangle\langle ii|\otimes\rho_E$ is a ccq-state with $\log_2 d$ secure bits, and $\approx_\epsilon$ denotes $\epsilon$-closeness in the trace norm $||\cdot||_1$.

The (two-way) distillable classical key between Alice and Bob from a quantum tripartite state $\rho \equiv \rho_{ABE}$ utilizing LOPC operations is given as [39]

$$C_D(\rho) := \inf_{\epsilon>0}\limsup_{n\to\infty}\sup_{\Delta\in\mathrm{LOPC}}\left\{\frac{\log_2 d}{n}\middle|\ \Delta(\rho^{\otimes n}) \approx_\epsilon \tau_d\right\}. \tag{23}$$

There is no closed formula known for $C_D$ for a general state. However, when one restricts the one-way LOCC communication in the distillation process, then there is a formula for the distillable key, called a one-way distillable key, given by Devetak and Winter [9]. We invoke here the theorem which encapsulates this rather complicated formula.

*Theorem 1 ([9], in formulation of [40]).* For every state $\rho_{ABE}$, $K_{\rightarrow} = \lim_{n\to\infty}\frac{K^{(1)}(\rho^{\otimes n})}{n}$, with $K^{(1)} = \max_{Q;T|X}(I(X:B|T) - I(X:E|T))$, where the maximization is over all POVMs $Q = (Q_x)_{x\in\mathcal{X}}$ and channels R such that $T = R(X)$, while the information quantities refer to the state $\omega_{TABE} = \sum_{t,x}R(t|x)P(x)|t\rangle\langle t|\otimes|x\rangle\langle x|\otimes Tr_A(\rho_{ABE}(Q_x)\otimes\mathbf{1}_{BE})$. The range of the measurement Q and the random variable $T$ may be assumed to be bounded as follows: $|T| \leqslant d_A^2$ and $|X| \leqslant d_A^2$ where $T$ can be taken as a (deterministic) function of $X$.

We have then, by definition that $K_{\rightarrow}(\rho_{ABE}) \leqslant C_D(\rho_{ABE})$, for any tripartite state $\rho_{ABE}$. This is by the fact that the class of protocols in definition of $K_{\rightarrow}$ is strictly less than in the case of $C_D$. In what follows, we will need a lower bound on $K_{\rightarrow}$, which bases on restricting operations in its definition to be identical on each copy of $\rho_{ABE}$. Namely, we define the one-way i.i.d. version of a one-way secure key, $K^{\mathrm{iid}}$, with $\{Q_x\}_{x\in\mathcal{X}}$ in the form $\hat{Q}_x^{\otimes n}$ and $T$ in the form $\hat{T}^{\times n}$. That is, the measurement on Alice's side is performed identically and independently on each copy of the state, rather than globally, and further classical information comes from a variable $\hat{T}$ that is identical on each copy.

*Definition 4.* For every state $\rho_{ABE}$, a one-way i.i.d. secure key reads

$$K^{\mathrm{iid}}(\rho_{ABE}) = \lim_{n\to\infty}\frac{1}{n}\max_{\hat{Q};\hat{T}|X}K_{\mathrm{DW}}([\hat{Q}_x(\rho_{ABE})]^{\otimes n}), \tag{24}$$

where $K_{\mathrm{DW}}(\rho_{XBE}) := I(X:B|\hat{T})_\rho - I(X:E|\hat{T})_\rho$, and the maximum in (24) is taken over POVMs of the form $\{\hat{Q}_x^{\otimes n}\}_{x\in\mathcal{X}}$, and channels $R$, such that $\hat{T}^{\times n} = R(X)$.

We have introduced the $K^{\mathrm{iid}}$, as it is easier to study its behavior than that of $K_{\rightarrow}$. While, as we show further, $K^{\mathrm{iid}}$ is to some extent nonlockable, $K_{\rightarrow}$ still can be lockable. We have finally $K^{\mathrm{iid}}(\rho_{ABE}) \leqslant K_{\rightarrow}(\rho_{ABE}) \leqslant C_D(\rho_{ABE})$, for any tripartite quantum state $\rho_{ABE}$.

### D. Key distillable by LOCC operations

Distillable key $K_D$ between Alice and Bob from a quantum bipartite state $\rho$ by means of two-way LOCC operations is given as [18,19]

$$K_D(\rho) := \inf_{\epsilon>0} \limsup_{n\to\infty} \sup_{\Delta\in\mathrm{LOCC}} \left\{ \frac{\log_2 d}{n} \middle| \Delta(\rho^{\otimes n}) \approx_\epsilon \gamma_d \right\}, \tag{25}$$

where $\gamma_d$ is a $d$-dimensional private state with $\log_2 d$ secure bits, and $\approx_\epsilon$ denotes $\epsilon$-closeness in the trace norm $|| \cdot ||_1$.

$K_D$ quantifies the amount of key secure against a quantum adversary who holds a purification of the state $\rho_{AB}$ can be obtained from asymptotically many copies of this state, in the form of a private state. Importantly, it can be shown [19,32] that for a pure tripartite state $\psi_{ABE}$ with corresponding state $\rho_{AB} = \mathrm{tr}_E\, \psi_{ABE}$, one has

$$C_D(\psi_{ABE}) = K_D(\rho_{AB}). \tag{26}$$

Therefore, in the worst case, that is when the adversary Eve holds a purifying system of $\rho_{AB}$, considering distillation of private states by LOCC operations or the ideal key states $\tau$ by LOPC operations yields the same rate. This allows us to interchange the use of $C_D$ and $K_D$ if needed.

## III. BOUND ON THE LEAKAGE OF PRIVATE RANDOMNESS

In this section, we focus on distributed scenario of private randomness distillation [17]. In this scenario, two honest parties share $n$ copies of a bipartite state $\rho_{AB}$. They use local unitary operations and dephasing channel to produce independent randomness private against Eve, who holds the purifying system and the environment of the dephasing channel. Depending on whether free or no local noise (in the form of a maximally mixed state) and free or no communication are allowed, we have four different settings for the distributed private randomness distillation. Theorem 2 in Ref. [17] shows the achievable rate regions (of private randomness distillable locally for each of the parties). For convenience and self-consistency of the paper, we restate it in the following. Here $R_G(\rho_{AB}) := \log_2 |A| + \log_2 |B| - S(\rho_{AB})$ stands for *global purity*, while $R_A$ is private randomness localizable by party $A$ in respective scenario (similarly for $B$).

*Theorem 2.* The achievable rate regions of $\rho_{AB}$ are the following:

(1) for no communication and no noise, $R_A \leqslant \log_2 |A| - S(A|B)_+$, $R_B \leqslant \log_2 |B| - S(B|A)_+$, and $R_A + R_B \leqslant R_G$, where $[t]_+ = \max\{0, t\}$;

(2) for free noise but no communication, $R_A \leqslant \log_2 |A| - S(A|B)$, $R_B \leqslant \log_2 |B| - S(B|A)$, and $R_A + R_B \leqslant R_G$;

(3) for free noise and free communication, $R_A \leqslant R_G$, $R_B \leqslant R_G$, and $R_A + R_B \leqslant R_G$;

(4) for free communication but no noise, $R_A \leqslant \log_2 |AB| - \max\{S(B), S(AB)\}$, $R_B \leqslant \log_2 |AB| - \max\{S(A), S(AB)\}$, and $R_A + R_B \leqslant R_G$.

Further the rate regions in settings (1), (2), and (3) are tight.

We consider then a local leakage at Alice's side, by a side channel consisting of local unitary $U_{A\to A'a}$ transformation of a system $A$ into a system $A'a$, followed by partial trace operation on system $a$, which implies leakage of this system to Eve. Before we get the proposition, we need an auxiliary technical fact.

*Fact 1.* For any two numbers $x$ and $y$,

$$\max\{0, x\} - \max\{0, y\} \leqslant |x - y|. \tag{27}$$

This can be checked directly by considering the two cases of $y \leqslant 0$ and $y > 0$. Now we are in position to formulate and prove the main result for this section.

*Proposition 1.* For a bipartite state $\rho_{AB}$ subjected to a side channel $\mathrm{tr}_a \circ U_{A\to A'a}$, there is

$$R_A(\rho_{AB}) - R_A(\rho_{A'B}) \leqslant \log_2 |a| + S(a), \tag{28}$$

in the four settings presented in theorem 2.

*Proof.* Setting (1) is reduced to setting (2) by noticing auxiliary fact 1. Then we have

$$\begin{aligned}
&R_A(\rho_{AB}) - R_A(\rho_{A'B}) &(29)\\
&\quad = \log_2 |A| - \max\{0, S(A|B)\}\\
&\qquad -[\log_2 |A'| - \max\{0, S(A'|B)\}] &(30)\\
&\quad = \log_2 |a| + \max\{0, S(A'|B)\} - \max\{0, S(A|B)\} &(31)\\
&\quad \leqslant \log_2 |a| + |S(A'|B) - S(A|B)| &(32)\\
&\quad = \log_2 |a| + |S(A'B) - S(A'aB)| &(33)\\
&\quad \leqslant \log_2 |a| + S(a), &(34)
\end{aligned}$$

where the first inequality comes from the auxiliary fact 1 and the last inequality from the subadditivity of entropy [41].

The proof for setting (3) is straightforward.

$$\begin{aligned}
&R_A(\rho_{AB}) - R_A(\rho_{A'B}) &(35)\\
&\quad = \log_2 |AB| - S(AB) - [\log_2 |A'B| - S(A'B)] &(36)\\
&\quad = \log_2 |a| + [S(A'B) - S(A'aB)] &(37)\\
&\quad \leqslant \log_2 |a| + S(a). &(38)
\end{aligned}$$

The proof for setting (4) can be reduced to setting (1) by noticing

$$\begin{aligned}
&R_A(\rho_{AB}) - R_A(\rho_{A'B}) &(39)\\
&\quad = \log_2 |AB| - \max\{S(B), S(AB)\}\\
&\qquad -[\log_2 |A'B| - \max\{S(B), S(A'B)\}] &(40)\\
&\quad = \log_2 |a| + \max\{0, S(A'|B)\} - \max\{0, S(A|B)\} &(41)\\
&\quad \leqslant \log_2 |a| + S(a). &(42)
\end{aligned}$$

#### Distillable key of maximally correlated states is strongly nonlockable

In the following theorem, we show that distillable key of a MCS is strongly nonlockable. A pure bipartite state is a special MCS in its Schmidt basis.

*Theorem 3.* For a maximally correlated state $\rho_{AB}$ defined through expression (4), after leakage of system $a$ from Alice to Eve the distillable key $K_D$ decreases by no more than S(a).

*Proof.* For a MCS $\rho_{AB}$, we have that $K_D(\rho_{AB}) = E_D(\rho_{AB}) = E_r(\rho_{AB}) = S(B) - S(AB)$. Suppose an isometry $U : A \to A'a$, and after the leakage of subsystem $a$ to Eve, then the shared state between Alice and Bob is $\rho_{A'B}$. By the Devetak-Winter protocol, we have $K_D(\rho_{A'B}) \geqslant S(B) - S(A'B)$

(this is the other direction of DW protocol). Therefore the loss of the distillable key can be upper bounded as follows,

$$K_D(\rho_{AB}) - K_D(\rho_{A'B}) \tag{43}$$
$$\leqslant S(B) - S(AB) - [S(B) - S(A'B)], \tag{44}$$
$$= S(A'B) - S(A'aB), \tag{45}$$
$$\leqslant S(a), \tag{46}$$

where we use $S(A'aB) = S(AB)$ since $U$ is an isometry, and subadditivity of the von Neumann entropy.

*Corollary 1.* The BB84 protocol [5], realized by means of the CSS codes, has a nonlockable rate.

*Proof.* In Ref. [42], it is shown, that such a protocol, if applied coherently, is equivalent to distillation of maximally entangled states. Hence, if the prepare-measure version of BB84 was lockable, i.e., the key upon tracing out some system $a$ would drop down by more than $S(a)$, so would be the drop of it for the coherent version. The latter is however forbidden by the theorem 3. ∎

In the next section, we generalize theorem 3 to Schmidt-twisted pure states $\widetilde{\gamma}_{ABA'B'}$ introduced in Eqs. (13) and (14).

## IV. LOWER BOUND FOR THE DROP OF GENERATED KEY UNDER LEAKAGE OF A SYSTEM

In this section, we investigate how much the generated key drops after leakage of a system. We start from Sec. IV A where we prove how much is the key rate drops for an irreducible private state when the system leaks from the shield part of Alice to Eve. Next, in Sec. IV B, we generalize the proof technique to all states and different types of leakage, such as erasure of a system or copying of a system. In turn, we prove the main result contained in theorem 4, saying that the raw key of a one-way Devetak-Winter protocol is nonlockable. In Sec. IV C by exploiting the concept of smooth min and max entropy, we show that the single-shot key rate is nonlockable. Finally, in Sec. IV D, we derive a lower bound on the loss of the two-way distillable key for the irreducible Schmidt-twisted pure states.

### A. Bound on the key drop by leakage from a irreducible private state

In this section, we provide a simple lower bound on the distillable key in the presence of leakage of subsystem $a$ from irreducible private states defined in Sec. II from the shield part, as well as from Alice's side in general. In all cases, we show that the key drops by no more than $2S(a)$. We start our considerations from the case of the leakage from the shield part.

*Observation 1.* For an irreducible private state $\gamma_{AA'BB'}$, with $A' = aA''$, there is

$$K_D(\gamma_{AA''BB'}) \geqslant K_D(\gamma_{AA'BB'}) - 2S(a). \tag{47}$$

*Proof.* The distillable key of an irreducible private state $\gamma_{A A'BB'}$ reads $\log_2 d_k$. Let us then divide system $A'$ into $\hat{A}a$. The Devetak-Winter protocol applied to the key part (from Bob to Alice) reads

$$I(A:B)_\rho - I(B:Ea)_\rho = \log_2 d_k - I(B:E) - I(B:a|E), \tag{48}$$

where $I(B:a|E) = S(BE) + S(aE) - S(E) - S(BaE)$ is the conditional mutual information, which follows from the chain rule. From $I(X:Y) \leqslant 2\min\{S(X), S(Y)\}$ and the chain rule, we conclude that $I(B:a|E) \leqslant 2\min\{S(a), S(B), S(aE), S(BE)\} \leqslant 2S(a) \leqslant 2\log_2|a|$ [43]. This, due to $I(B:E) = 0$, as the state is the private state, proves our observation. ∎

Now, we will extend the statement of observation 1 to the leakage from the irreducible private state in a general way, not necessarily from its shield part. To do so, let us first prove the following technical lemma.

*Lemma 1.* For a cqq state $\rho_{XAaE} = \sum p_i |i\rangle\langle i|_X \otimes \rho^i_{AaE}$, after the leakage of system $a$ from Alice to Eve, the following holds:

$$[I(X:Aa) - I(X:E)] - [I(X:A) - I(X:aE)] \leqslant 2S(a). \tag{49}$$

*Proof.* The proof goes by straightforward calculations and strong subadditivity.

$$[I(X:Aa) - I(X:E)] - [I(X:A) - I(X:aE)] \tag{50}$$
$$= I(X:a|A) + I(X:a|E) \tag{51}$$
$$= S(a|A) - S(a|AX) + S(a|E) - S(a|EX) \tag{52}$$
$$= S(a|A) + S(a|E) - \sum_i p_i[S(a|E)_i + S(a|A)_i] \tag{53}$$
$$\leqslant 2S(a), \tag{54}$$

where the inequality comes from the facts that $S(a|A) \leqslant S(a)$, $S(a|E) \leqslant S(a)$, and $S(a|E)_i + S(a|A)_i \geqslant 0$ for each index $i$ which follows from the strong subadditivity. Namely, considering purification of $\rho_{aAE}$ to $|\psi_\rho\rangle_{aAEE'}$ we can write $S(a|EE') + S(a|A) = 0$, since $S(aEE') = S(A)$, and $S(EE') = S(aA)$. But using strong subadditivity we write $S(a|EE') \leqslant S(a|E)$, so $S(a|E) + S(a|A) \geqslant S(a|EE') + S(a|A) = 0$. This argumentation holds for every index $i$ in expression (50). ∎

*Proposition 2.* For an irreducible private state $\gamma_{AA'BB'}$, with $AA' = a\tilde{A}$, after the leakage of system $a$ from Alice to Eve, there is

$$K_D(\gamma_{\tilde{A}BB'}) \geqslant K_D(\gamma_{AA'BB'}) - 2S(a). \tag{55}$$

*Proof.* Denote $\gamma_{AA'BB'E}$ as the purification of $\gamma_{AA'BB'}$ when Eve's system $E$ is included. Consider then this state measured on $B$ in computational basis, producing a random variable $X$. Further notice that we have the following chain of (in)equalities:

$$K_D(\gamma_{AA'BB'}) = I(X:A) - I(X:E) \tag{56}$$
$$\leqslant I(X:AA') - I(X:E) \tag{57}$$
$$= I(X:\tilde{A}a) - I(X:E) \tag{58}$$
$$\leqslant I(X:\widetilde{A}) - I(X:aE) + 2S(a) \tag{59}$$
$$\leqslant K_D(\gamma_{\widetilde{A}BB'}) + 2S(a). \tag{60}$$

The first equality is due to the fact that $\gamma$ is irreducible, hence $K_D(\gamma_{ABA'B'}) = \log_2 d_k = I(X:A) = I(X:A) - I(X:E)$, as $I(X:E) = 0$ due to privacy from Eve of the system $B$ under measurement. The first inequality is due to data processing inequality [44] implying $I(X:A) \leqslant I(X:AA')$. We next observe that the unitary transformation does not change the mutual information, hence $I(X:AA') = I(X:\tilde{A}a)$. Finally we note that

$$I(X:\tilde{A}a) - I(X:E) - [I(X:\tilde{A}) - I(X:aE)] \leqslant 2S(a), \tag{61}$$

where the inequality is due to lemma 1 by identifying $A$ with $\tilde{A}$. This finishes the proof. ∎

The upper bounds on the key in observation 1 and proposition 2 are tight, which implies that $K_D$ is not strongly nonlockable in general. The example comes from a variant of the superdense coding protocol.

*Example 1.* Consider the private state $\gamma_{AA'B}$ where $B'$ is a trivially one-dimensional subsystem and the purification of the state with Eve's system $E$ is of the form

$$\frac{1}{\sqrt{4}}\sum_{i=0}^{3} |ii\rangle_{AB} \otimes \left(\sigma^i_{A'} \otimes I_E\right) |\Phi\rangle_{A'E}\,, \tag{62}$$

where $\sigma^i_{A'}$ are the Pauli unitary operators acting on the subsystem $A'$ and $|\Phi\rangle_{A'E} = \frac{1}{\sqrt{2}}(|00\rangle_{A'E} + |11\rangle_{A'E})$. A simple observation is that $K_D(\gamma_{AA'B}) = 2$ and after the leakage of the shielding qubit $A'$ to Eve, $K_D = 0$.

The same holds if the leakage takes place on system $B'$, unless it is given to Eve. Hence, given that the leakage happens only on the shielding system of an irreducible private state, the key drops down by at most twice the entropy of the system, and in some cases, it can equal to 2.

### B. The raw key of a one-way Devetak-Winter protocol is nonlockable

We now generalize the result from Sec. IV A to all states that are the output of key-generation protocol. In practice, they differ from private states considered above. This is because the process of key generation is usually not coherent. In that we also narrow to one-way key distillation. We will first need the following observation.

*Observation 2.* For a cq state $\rho_{x(XY)}$,

$$I(x:Y|X) \leqslant H(x). \tag{63}$$

*Proof.* It is convenient to rewrite $I(x:Y|X)$ as

$$I(x:Y|X) = S(x|X) - S(x|YX). \tag{64}$$

The state $\rho_{x(XY)}$ is separable in cut $x:(XY)$, hence $S(x|YX) \geqslant 0$ [12]. We can thus neglect this term, obtaining an upper bound

$$I(x:Y|X) \leqslant S(x|X). \tag{65}$$

Since $\rho_{x(X)}$ is also a cq state, we can further expand $S(x|X)$ as

$$S(x|X) = H(x) + \sum_x p(x) S(\rho_{X|x}) \\ -S\left(\sum_x p(x)\rho_{X|x}\right) \leqslant H(x), \tag{66}$$

where the last inequlity is due to concavity of the von Neumann entropy.

*Lemma 2.* For a state $\rho_{aABET}$, there is

$$I(A:B|T) - I(A:Ea|T) \\ \geqslant I(Aa:B|T) - I(aA:E|T) - cS(a), \tag{67}$$

with $c = 2$. Moreover, when state $\rho_{a(ABET)}$ is a cq state, then the bound holds for $c = 1$.

*Proof.* The first part of the lemma is obtained by direct calculations. Namely, we have the following:

$$I(Aa:B|T) - I(Aa:E|T) - [I(A:B|T) - I(A:Ea|T)] \\ = -S(a|ABT) + S(a|ET) \leqslant 2S(a). \tag{68}$$

To show the second part of the statement, when we deal with a cq state, it is enough to notice that $S(a|ABT) \geqslant 0$. ∎

We have considered above a drop of a system on the side of a sender of one-way communication during key distillation via Devetak-Winter protocol [9]. We now show that similar result holds for the party who, in their protocol, receives only the data.

*Corollary 2.* For a state $\rho_{ABbET}$, there is

$$I(A:B|T) - I(A:Eb|T) \\ \geqslant I(A:Bb|T) - I(A:E|T) - cS(b), \tag{69}$$

with $c = 4$. Moreover, if the state $\rho_{b(ABET)}$ is a cq state, then the bound holds for $c = 2$.

*Proof.* The proof follows from the following chain of inequalities:

$$I(A:B|T) - I(A:Eb|T) \pm I(b:A|BT) \tag{70}$$

$$= I(A:Bb|T) - I(A:Eb|T) - I(b:A|BT) \tag{71}$$

$$\geqslant I(A:Bb|T) - I(A:Eb|T) - 2S(b) \tag{72}$$

$$= I(A:Bb|T) - I(A:E|T) - I(b:A|ET) - 2S(b) \tag{73}$$

$$\geqslant I(A:Bb|T) - I(A:E|T) - 4S(b). \tag{74}$$

We first focus on the case $c = 4$. The first equality comes from the chain rule, while the first inequality from bound on $I(b:A|BT)$. Similarly, the second equality follows from the chain rule, and following inequality from bounding the term $I(b:A|ET)$. Regarding the case $c = 2$, we note that when system $b$ is classical, then both terms $I(b:A|ET)$ and $I(b:A|BT)$ are bounded by $S(b)$ by observation 2, which proves the thesis. ∎

Owing to the fact that the raw key is classical, it is also realistic to assume that the leakage will be through copying rather than the theft of data. We therefore consider this case below.

*Corollary 3.* For a state $\rho_{AaBET}$, there is

$$I(Aa:B|T) - I(Aa:Ea|T) \\ \geqslant I(Aa:B|T) - I(Aa:E|T) + cS(a), \tag{75}$$

with $c = 2$.

*Proof.* To prove expression (75), we write the following chain of inequalities:

$$I(Aa:B|T) - I(Aa:Ea|T) \pm I(Aa:E|T) \tag{76}$$

$$= I(Aa:B|T) - I(Aa:E|T) - I(a:Aa|ET) \tag{77}$$

$$\geqslant I(Aa:B|T) - I(aA:E|T) - 2S(a). \tag{78}$$

The first equality follows from the chain rule, and further we bound the term $I(a:Aa|ET)$. ∎

To conclude about the nonlockability of the raw key obtained in the one-way protocol we base on the main result of Devetak and Winter in Ref. [9], invoked in Sec. II C.

Let $\mathcal{P}$ be a part of the protocol of one-way key distillation after Alice have performed measurement $Q_x$, i.e., after producing a state of the form $Q_x(\rho_{ABE}^{\otimes n}) = \omega_{TABE}^{(n)} = \sum_{t,x} R(t|x)P(x)|t\rangle\langle t| \otimes |x\rangle\langle x| \otimes Tr_A(\rho_{ABE}(Q_x) \otimes \mathbf{1}_{BE})$. It consists of an error correction and a privacy amplification operations applied to the state $\omega_{TXBE}$ [21] and $\mathcal{P}$ is the part of total protocol, which generates the key from the *raw key* at Alice's side. Let also the rate of $\mathcal{P}$ be denoted as $\kappa$. In the above theorem, the state of the raw key is represented by $\omega_{TXBE}^{(n)}$. We assume also that system of Alice is represented by $A \equiv Xx$, where $x$ will be given to Eve in the process of leakage. We have then an immediate result.

*Theorem 4.* The raw key of a one-way Devetak-Winter protocol is nonlockable: for any state $\omega_{T(Xx)BE}^{(n)}$ generated by measurement $Q_x$ on $n$ copies of $\rho_{AaBE}$, and for any random variable $T = R(X)$, there is $\kappa(\mathcal{P}(\omega_{T(Xx)BE}^{(n)})) \geqslant \kappa(\mathcal{P}(\omega_{TXB(Ex)}^{(n)})) - H(x)/n$.

*Proof.* Let us denote the states where the raw key is presented, in both cases, when the system $x$ is with Alice and Eve by $\omega_{TXxBE}^{(n)}$ and $\omega_{TXB(Ex)}^{(n)}$, respectively. Denoting by $\mathcal{P}$ the one-way key distillation protocol applied to both states, we evaluate its rates $\kappa$ as

$$\kappa\big(\mathcal{P}\big(\omega_{TXxBE}^{(n)}\big)\big) = \frac{1}{n}[I(Xx:B|T) - I(Xx:E|T)], \tag{79}$$

$$\kappa\big(\mathcal{P}\big(\omega_{TXB(Ex)}^{(n)}\big)\big) = \frac{1}{n}[I(X:B|T) - I(X:Ex|T)]. \tag{80}$$

Applying the statement from lemma 2, and using the fact that $x$ is classically correlated with the rest of the systems, we can write

$$\kappa\big(\mathcal{P}\big(\omega_{TXB(Ex)}^{(n)}\big)\big) \geqslant \kappa\big(\mathcal{P}\big(\omega_{TXxBE}^{(n)}\big)\big) - \frac{H(x)}{n}. \tag{81}$$

Hence, whenever entropy $H(x)$ scales linearly with number of copies $n$, i.e., when $H(x) = \alpha n$, where $\alpha$ is a constant, the raw key drops by constant factor. However, when the dependence is sublinear in $n$, the resulting raw key does suffer from the leakage. ■

The same statement as in theorem 4 can be made in the case of system leakage $b$ from Bob to Eve, or of copying the system $a$ from Alice to Eve. Denoting by $(\omega_{TX(Bb)E}^{(n)}, \omega_{TXB(Eb)}^{(n)})$ and $(\omega_{TXxBE}^{(n)}, \omega_{TXxB(Ex)}^{(n)})$ the pairs of states containing the raw key in the case of leakage of Bob's system and of copying, respectively, we formulate the following.

*Observation 3.* The raw key of a one-way Devetak-Winter protocol is nonlockable in the case of system leakage from Bob to Eve and of copying a system from Alice to Eve. In particular, the raw key rates before and after the process of leakage (copying) satisfy, respectively:

$$\kappa\big(\mathcal{P}\big(\omega_{TX(Bb)E}^{(n)}\big)\big) \geqslant \kappa\big(\mathcal{P}\big(\omega_{TXB(Eb)}^{(n)}\big)\big) - 4S(b)/n, \tag{82}$$

$$\kappa\big(\mathcal{P}\big(\omega_{T(Xx)BE}^{(n)}\big)\big) \geqslant \kappa\big(\mathcal{P}\big(\omega_{TXxB(Ex)}^{(n)}\big)\big) - 2S(x)/n. \tag{83}$$

Whenever entropies $S(x)$ and $S(b)$ scale linearly or sublinearly with $n$ the raw key drops down by a constant factor or does not change in the limit of large $n$.

### C. Single-shot key rate approach after leakage system to Eve

By the result of Ref. [22], one can deduce how much smooth min entropy $H_{\min}^{\epsilon}$ drops after the leakage of system $x$ to Eve (see Sec. II B for definitions).

*Lemma 3 (Adaptation of lemma 5 from Ref. [22]).* A The smooth min entropy $H_{\min}^{\epsilon}$ is nonlockable. It means that after leakage of a system $x$ to Eve, the following inequality holds:

$$H_{\min}^{\epsilon}(Xx|E) \leqslant H_{\min}^{\epsilon}(X|Ex) + \log_2|x|, \tag{84}$$

where $|x|$ denotes dimension of the system $x$.

Using the above result, one can show that the single-shot key rate is nonlockable. Namely, before and after leakage of a system $x$ to Eve, the key rates are respectively:

$$K^{(1)}(\rho_{(Xx)BE}) = H_{\min}^{\epsilon}(xX|E) - H_{\max}^{\epsilon}(xX|B),$$
$$\widetilde{K}^{(1)}(\rho_{XB(Ex)}) = H_{\min}^{\epsilon}(X|Ex) - H_{\max}^{\epsilon}(X|B). \tag{85}$$

Applying data processing theorem [22] to the expression of (85) we have that $H_{\max}^{\epsilon}(xX|B) \leqslant H_{\max}^{\epsilon}(X|B)$. Thanks to this, we conclude that the key drops by no more than $\log_2|x|$.

Finally, by observing that, in the limit $n \to \infty$, the min and max entropies converge to the conditioned Shannon entropy (21), we can conclude that the right-hand side of (84) gives $n\log_2|x|$. Whenever system $x$ is of $n$ qubits, and $S(x) > \frac{1}{4}n$ holds, this bound is smaller than the bound $4S(x)$ discussed in observation 3.

### D. Lower bound on the loss of the distillable key for the irreducible Schmidt-twisted pure states

The bounds shown in the previous sections are independent of the correlations of the erased system $a$ with the rest of the system. However, it is intuitive that the less $a$ is correlated the smallest should be drop of the key upon loss of $a$. This motivates us to search for a bound which is dependent on these correlations.

To show that the key sometimes does not leak too fast, we propose a particular strategy to be taken after erasure of subsystem of the state. It is based on the so called *fidelity of recovery* [23,45].

As we will see, this approach will lead us to a bound on a two-way distillable key for private states. Namely, after the loss of a subsystem $a$ of a system $Aa$, Alice is applying the best map $\Gamma_{A\to A\tilde{a}}$ that recovers $a$ in some form $\tilde{a}$. She then applies the same one-way protocol on system $A\tilde{a}$. Denoting by $F(\rho_{AaBE}, \widetilde{\rho}_{A\tilde{a}BE})$ the Uhlmann fidelity between quantum states [46], the fidelity of recovery reads

$$F_R(a;BE|A) := \sup_{\Gamma_{A\to A\tilde{a}}} F(\rho_{AaBE}, \Gamma_{A\to A\tilde{a}}(\rho_{ABE})), \tag{86}$$

where $\rho_{AaBE}$ with $\rho_{ABE} = \mathrm{tr}_a\rho_{AaBE}$, and we suppressed identity $\mathbf{1}_{BE}$ in the action of recovery map $\Gamma_{A\to A\tilde{a}}(\rho_{ABE}) \equiv (\mathbf{1}_{BE} \otimes \Gamma_{A\to A\tilde{a}})(\rho_{ABE}) = \widetilde{\rho}_{A\tilde{a}BE}$. We will call $\rho_{A\tilde{a}BE}$ a recovered state. It is proven that there is an appealing lower bound on the formula (86) in terms of the conditional mutual information [23,45]:

$$F_R(\rho_{AaBE}) \geqslant 2^{-I(a:BE|A)}. \tag{87}$$

This allows us for estimating closeness of single copy one-way secure key $K_{\to}^{(1)}$ between state $\rho_{AaBE}$ and its recovered version $\widetilde{\rho}_{A\tilde{a}BE}$. In what follows, we use lemma V.3 of Ref. [40] for the case of triparite states (for biparite states it needs correction, see lemma 4 presented in Appendix).

*Observation 4.* For any state $\rho_{AaBE}$ and its recovered version $\widetilde{\rho}_{A\tilde{a}BE} = \Gamma_{A\to A\tilde{a}}(\rho_{ABE})$, where $\rho_{ABE} = \mathrm{tr}_a \rho_{AaBE}$, and $\Gamma_{A\to A\tilde{a}}$ is recovery map, the following relation holds:

$$|K_{\to}^{(1)}(\widetilde{\rho}_{A\tilde{a}BE}) - K_{\to}^{(1)}(\rho_{AaBE})| \leqslant 8\delta \log_2 d_{Aa} + 4h(\delta), \tag{88}$$

with $\delta = \sqrt{1 - 2^{-I(a:BE|A)}}$ and $h(\cdot)$ denoting the binary Shannon entropy.

This observation follows directly from the Fuchs–van de Graaf inequality [47], which for two arbitrary states $\rho, \sigma$ reads $\frac{1}{2}||_1 \rho - \sigma|| \leqslant \sqrt{1 - F(\rho, \sigma)}$, and the fact that (not regularized) one-way distillable key is asymptotically continuous (see lemma V.3 in Ref. [40]). We use fidelity which is calculated for a map $\Gamma_{A\to A\tilde{a}}$ maximising the fidelity of recovery in (86).

The above considerations hold for one copy of the state $\rho_{A\tilde{a}BE}$. Now we shall discuss and find an upper bound for the regularized version, $K_{\to} = \lim_n \frac{1}{n} K_{\to}^{(1)}(\rho^{\otimes n})$. The above reasoning cannot be applied straightforwardly to this case, because the closeness of $\rho$ and $\sigma$ in trace norm $\frac{1}{2}||\rho - \sigma||_1$ does not imply their closeness after taking many copies, when one considers $\frac{1}{2}||\rho^{\otimes n} - \sigma^{\otimes n}||_1$.

Nevertheless, we can extend the above result to a class of *Schmid-twisted irreducible private states*. Let us recall that the one-way i.i.d. version of a secure key, $K^{\mathrm{iid}}$, is the key distillable by one-way communication via first measuring and postprocessing it in an i.i.d. way on Alice's side. That is, the measurement $Q_x$ on Alice's side is performed identically and independently on each copy of the state, rather than globally, and further classical information comes from a variable $\hat{T}$ that is identical on each copy (see Sec. II C for a full definition).

We can now prove the result inspired by observation 4 in the case of $K^{\mathrm{iid}}$.

*Theorem 5.* Let $K^{\mathrm{iid}}$ be one-way i.i.d. version of secure key, as in definition 4. Denoting the original state by $\rho_{aABE}$, the following inequality holds:

$$K^{\mathrm{iid}}(\rho_{ABE}) \geqslant K^{\mathrm{iid}}(\rho_{aABE}) - (4\delta \log_2(d_a d_A d_B^2) + 4h(\delta)), \tag{89}$$

where $\delta = \sqrt{1 - 2^{-I(a:BE|A)}}$, $I(a : BE|A)$ is a conditional mutual information calculated on respective systems, and $h(\cdot)$ denotes the binary Shannon entropy.

*Proof.* Let $\hat{Q}_x^*$ be the optimal measurement realizing $K^{\mathrm{iid}}(\rho_{AaBE})$, where $\rho_{AaBE} = |\psi_{AaBE}\rangle\langle\psi_{AaBE}|$, and let $\widetilde{\rho}_{\tilde{a}ABE}$ be the state after application of the recovery map $\Gamma_{A\to A\tilde{a}}$ to the state $\rho_{ABE} = \mathrm{tr}_a \rho_{aABE}$. As we have argued below observation 4, there is $||\widetilde{\rho}_{\tilde{a}ABE} - \rho_{AaBE}||_1 \leqslant \delta$, and the same holds for this pair of states after application of the measurement $\hat{Q}_x^*$, so $||\widetilde{\rho}'_{\tilde{a}ABE} - \rho'_{XABE}||_1 \leqslant \delta$, where $\rho'_{XABE} = \hat{Q}_x^*(\rho_{aABE})$, with $X$ denoting the outcome of the measurement. Now, applying definition 4 to our case, one has

$$K^{\mathrm{iid}}(\rho_{aABE}) = \lim_{n\to\infty} \frac{1}{n} \max_{\hat{T}|X} K_{\mathrm{DW}}([Q_x^*(\rho_{aABE})]^{\otimes n}) \tag{90}$$

$$= \lim_{n\to\infty} \frac{1}{n} \max_{\hat{T}|X} (I(X : B|\hat{T})_{\rho'^{\otimes n}} - I(X : E|\hat{T})_{\rho'^{\otimes n}}) \tag{91}$$

$$= \max_{\hat{T}|X} (I(X : B|\hat{T})_{\rho'} - I(X : E|\hat{T})_{\rho'}) \tag{92}$$

$$= I(X : B|\hat{T}^*)_{\rho'} - I(X : E|\hat{T}^*)_{\rho'}. \tag{93}$$

To obtain the second line, we use $K_{\mathrm{DW}}(\rho_{XBE}) = I(X : B|\hat{T})_\rho - I(X : E|\hat{T})_\rho$. To obtain the third line, we exploit the additivity of the conditional mutual information. To get the last line, we introduce the quantity $\hat{T}^*$ attaining the maximum value of $\hat{T}$. On the other hand, by similar lines, there is

$$K^{\mathrm{iid}}(\widetilde{\rho}_{\tilde{a}ABE}) \geqslant I(X : B|\hat{T}^*)_{\widetilde{\rho}'} - I(X : E|\hat{T}^*)_{\widetilde{\rho}'}, \tag{94}$$

where $\hat{T}^*$ is the value of $\hat{T}$ that attains maximum in the formula for $K^{\mathrm{iid}}(\rho_{aABE})$, and $X$ is the outcome of measurement $\hat{Q}_x^*$ on $\widetilde{\rho}_{\tilde{a}ABE}$. Finally, to prove expression (89), we write the following chain of inequalities:

$$K^{\mathrm{iid}}(\rho_{ABE}) \geqslant K^{\mathrm{iid}}(\tilde{\rho}_{\tilde{a}ABE}) \tag{95}$$

$$\geqslant I(X : B|\hat{T}^*)_{\widetilde{\rho}'} - I(X : E|\hat{T}^*)_{\widetilde{\rho}'} \tag{96}$$

$$\geqslant I(X : B|\hat{T}^*)_{\rho'} - I(X : E|\hat{T}^*)_{\rho'} - (4\delta \log_2 d_B + 4\delta \log_2(d_a d_A d_B) + 4h(\epsilon)) \tag{97}$$

$$\geqslant K^{\mathrm{iid}}(\rho_{aABE}) - (8\delta \log_2 d_B + 4\delta \log_2(d_a d_A) + 4h(\delta))$$

$$= K^{\mathrm{iid}}(\rho_{aABE}) - (4\delta \log_2 (d_a d_A d_B^2) + 4h(\delta)). \tag{98}$$

The first inequality follows from the fact that the operation of recovery, since it is local, does not increase the amount of the key. To obtain the third line we use the fact that closeness of states $\widetilde{\rho}'$ and $\rho'$ in the trace norm implies closeness of the corresponding conditional mutual information. First, we expand $I(X : B|\hat{T}^*)_{\widetilde{\rho}'}$ and $I(X : B|\hat{T}^*)_{\rho'}$ with respect to Bob, using mutual entropies:

$$|I(X : B|\hat{T}^*)_{\widetilde{\rho}'} - I(X : B|\hat{T}^*)_{\rho'}| = |S(B|\hat{T}^*)_{\widetilde{\rho}'} - S(B|\hat{T}^*)_{\rho'}| + |S(B|X\hat{T}^*)_{\widetilde{\rho}'} - S(B|X\hat{T}^*)_{\rho'}| \leqslant 4\delta \log_2 d_B + 2h(\delta). \tag{99}$$

For functions $I(X : E|\hat{T}^*)_{\widetilde{\rho}'}$ and $I(X : E|\hat{T}^*)_{\rho'}$, we expand with respect to Eve's system,

$$|I(X : E|\hat{T}^*)_{\widetilde{\rho}'} - I(X : E|\hat{T}^*)_{\rho'}| \leqslant |S(E|\hat{T}^*)_{\widetilde{\rho}'} - S(E|\hat{T}^*)_{\rho'}| + |S(E|X\hat{T}^*)_{\widetilde{\rho}'} + S(E|X\hat{T}^*)_{\rho'}| \leqslant 4\delta \log_2 d_E + 2h(\delta). \tag{100}$$

The state $\rho_{aABE}$ is pure, which implies that the dimension $d_E$ is upper bounded by $d_a d_A d_B$. This follows from observation that, in the cut $aAB : E$, the Schmidt decomposition cannot have more terms than $\mathrm{rank}(\rho_{aAB}) \leqslant \dim(\mathcal{H}_a \otimes \mathcal{H}_A \otimes \mathcal{H}_B) = d_a d_A d_B$. This allows us to rewrite (100) as

$$|I(X : E|\hat{T}^*)_{\widetilde{\rho}'} - I(X : E|\hat{T}^*)_{\rho'}| \leqslant 4\delta \log_2(d_a d_A d_B) + 2h(\delta) = 4\delta \log_2 d_B + 4\delta \log_2(d_a d_A) + 2h(\delta). \tag{101}$$

Now, combining expressions (99) and (101), we get (98) finishing the proof.

*Observation 5.* Inequality (89) in theorem 5 can be rewritten in terms of dimension $d_X$ of the space of measurements $X$:

$$K^{\mathrm{iid}}(\rho_{ABE}) \geqslant K^{\mathrm{iid}}(\rho_{aABE}) - (8\delta \log_2 d_X + 4h(\delta)), \tag{102}$$

where $X$ is generated from $aA$ via iid measurement $\hat{Q}_x^*: aA \to X$.

One can prove this statement by writing expressions (99) and (100) with respect to space of outcomes $X$, and by similar lines as in the proof of theorem 5 one gets the statement. As we will see, this observation is of the great importance when one considers private states with $d_X = d_A$, since considered measurements are the von Neumann measurements, which do not increase respective dimension. This significantly reduces the value of the factor in Eq. (89).

We know that any Schmidt-twisted pure state $\widetilde{\gamma}_{ABA'B'}$ can be written as $U(\psi_{AB} \otimes \sigma_{A'B'})U^{\dagger}$, where its explicit form is presented in (14). In this class, one can consider a subclass of irreducible Schmidt-twisted pure states. The whole secret content of these states is accessible via systems $A$ and $B$. Irreducible private states [30] are a special case of these states. An irreducible private state $\gamma$ with $2^k \otimes 2^k$ dimensional key part satisfies $K_D(\gamma) = k$. From theorem 5 and observation 5 we have the following proposition:

*Proposition 3.* For an irreducible Schmidt-twisted pure state $\widetilde{\gamma}_{ABA'B'}$ with $AA' = aA''$, there is

$$K_D(\widetilde{\gamma}_{A''BB'}) \geqslant K_D(\widetilde{\gamma}_{aA''BB'}) - [8\delta \log_2 d_A + 4h(\delta)], \tag{103}$$

with $\delta = \sqrt{1 - 2^{-I(a:BB'|A'')_{\gamma}}}$.

*Proof.* We apply the statement of observation 5 to a pure state $\widetilde{\gamma}_{aA''BB'E}$ with measurement $Q_x^*$, which is composition of the unitary $U : aA'' \to AA'$ with the von Neumann measurement on system $A$ in the computational basis, obtaining

$$K_D^{\text{iid}}(\widetilde{\gamma}_{A''BB'E}) \geqslant K_D^{\text{iid}}\big(\psi_{\widetilde{\gamma}_{aA''BB'E}}\big) - [8\delta \log_2 d_A + 4h(\delta)]. \tag{104}$$

The following chain of equalities holds:

$$\begin{aligned} K_D^{\text{iid}}\big(\psi_{\widetilde{\gamma}_{aA''BB'E}}\big) &= K_D^{\text{iid}}\big(\psi_{\widetilde{\gamma}_{ABA'B'E}}\big) \\ &= C_D\big(\psi_{\widetilde{\gamma}_{ABA'B'E}}\big) = K_D\big(\widetilde{\gamma}_{ABA'B'}\big) = K_D\big(\widetilde{\gamma}_{aA''BB'}\big). \end{aligned} \tag{105}$$

The first equality holds since the unitary operation producing different cut of the Alice's systems $AA' \leftrightarrow aA''$ does not change the amount of the key. Furthermore,

$$K^{\text{iid}}\big(\psi_{\widetilde{\gamma}_{ABA'B'E}}\big) \leqslant C_D\big(\psi_{\widetilde{\gamma}_{ABA'B'E}}\big) = S(A)_{\psi}, \tag{106}$$

where $C_D$ denotes the rate of key distilled by means of LOPC operations, see Sec. II C and Ref. [9] ($\psi$ denotes $\psi_{\widetilde{\gamma}_{ABA'B'E}}$). The inequality in (106) is obtained because we work with a restricted class of protocols, while the equality follows from the fact that from irreducible private state we obtain exactly $S(A)_{\psi}$ of the key. Next, we notice that, for irreducible Schmidt-twisted pure states, the inequality (106) is saturated, $K^{\text{iid}}(\psi_{\widetilde{\gamma}_{ABA'B'E}}) = C_D(\psi_{\widetilde{\gamma}_{ABA'B'E}})$, because one achieves rate of $C_D(\psi_{\widetilde{\gamma}_{ABA'B'E}}) = S(A)_{\psi}$ via the measurement, which is tensor power of the von Neumann measurement on the key part $A$, while variable $T$ is null here (no communication is needed for obtaining the key). Due to Ref. [32], $C_D(\psi_{\widetilde{\gamma}_{ABA'B'E}}) = K_D(\widetilde{\gamma}_{ABA'B'})$. Applying the unitary producing different cut of the Alice's systems $AA' \leftrightarrow aA''$, we obtain the last equality in (105). To prove the left-hand side of (103), we observe that

$$C_D\big(\psi_{\widetilde{\gamma}_{A''BB'E}}\big) \geqslant K_D^{\text{iid}}\big(\widetilde{\gamma}_{A''BB'E}\big). \tag{107}$$

Finally, using expression (26) from Sec. II C, stating that, for a pure tripartite state $\psi_{ABE}$ with corresponding state $\rho_{AB} = \operatorname{tr}_E \psi_{ABE}$, one has $C_D(\psi_{ABE}) = K_D(\rho_{AB})$, we obtain the statement. ■

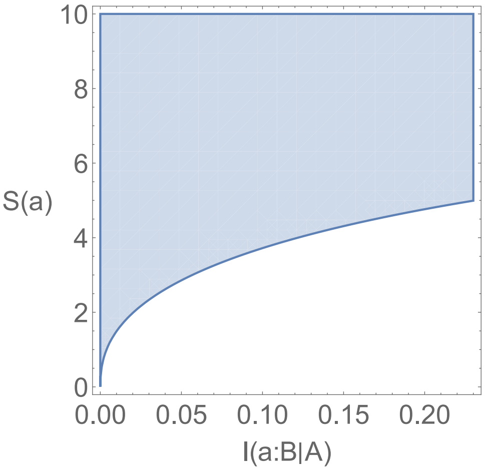


FIG. 2. A comparison of the bounds given in theorem 5, with $\delta = \sqrt{1 - 2^{-I(a:B|A)}}$, and in observation 1. The blue region corresponds to the case when $8\delta \log_2 d_A + 4h(\delta) \leqslant 2S(a)$ with $d_A = 2$. However, the quantities $S(a), I(a:B|A)$ are not independent, so not all pairs $(I(a:B|A), S(a))$ in the blue region are achievable. In other words, if a point is achievable, then it has to satisfy plotted relation, and otherwise we do not take it into account.

It is tempting to ask how the bound from theorem 5 compares with the bound from proposition 2. In Fig. 2, we ask whether $8\delta \log_2 d_A + 4h(\delta) \leqslant 2S(a)$, with $\delta = \sqrt{1 - 2^{-I(a:BB'|A'')_{\gamma}}}$.

## V. PARTIAL NONLOCKING FOR PRODUCT OF TWO STATES

As we have mentioned earlier, it is an open problem if a two-way distillable key drops down by more than $S(CD)$ upon the erasure of subsystems $CD$ of some bipartite state $\rho_{AC:BD}$. An easy subcase of this problem is when the subsystem $CD$ is a *product* with the rest of the system $AB$. That is, we consider the consequences of the following transformation:

$$\rho_{AB} \otimes \sigma_{CD} \to \rho_{AB}. \tag{108}$$

It looks at first that the drop of a key should be $K_D(\sigma_{CD})$. However, it need not be the case. The problem that arises here stems from the fact that $K_D$ may be superadditive on tensor product (this is known for the private capacity of quantum channels [48]). This is why it is not clear how much the key of $\rho_{AB}$ increases upon adding auxiliary system $\sigma_{CD}$.

We argue now that the increase can be controlled.

*Observation 6.* For a tensor product of biparite states $\rho_{AB} \otimes \rho_{CD}$, there is

$$\begin{aligned} K_D(\rho_{AB} \otimes \sigma_{AB}) - K_D(\rho_{AB}) &\leqslant \min\{E_R(\rho_{AB}), E_{sq}(\rho_{AB})\} - K_D(\rho_{AB}) \\ &\quad + \min\{S(\sigma_C), S(\sigma_D)\}, \end{aligned} \tag{109}$$

where $E_R(\rho) := \inf_{\sigma \in SEP} D(\rho, \sigma)$, with $D(\rho, \sigma) := \operatorname{tr}\rho \log_2 \rho - \operatorname{tr}\rho \log_2 \sigma$, is the relative entropy of entanglement [49], while $E_{sq}(\rho_{AB}) := \inf\{\frac{1}{2} I(A:B|E) \mid \rho_{AB} = \operatorname{tr}_E \rho_{ABE}\}$ is the squashed entanglement [36].

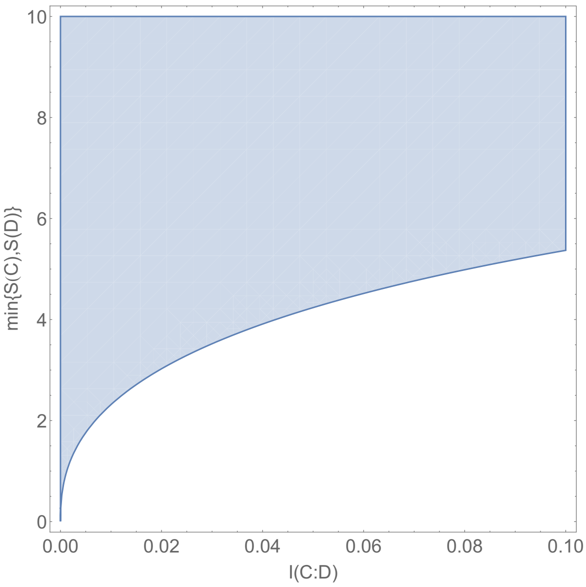


FIG. 3. A comparison of the bounds given in theorem 5, with $\delta = \sqrt{1-2^{-I(C:D)}}$, and through corollary 4. The blue region corresponds to the case when $8\delta\log_2 d_A + 4h(\delta) \leqslant \min\{S(\sigma_C), S(\sigma_D)\}$ with $d_A = 2$.

*Proof.* By noticing $K_D \leqslant \min\{E_R, E_{sq}\}$, we observe that

$$K_D(\rho_{AB}\otimes\sigma_{AB}) - K_D(\rho_{AB}) \leqslant \min\{E_R(\rho_{AB}\otimes\sigma_{AB}), E_{sq}(\rho_{AB}\otimes\sigma_{AB})\} - K_D(\rho_{AB}). \tag{110}$$

We further note that $E_R$ is subadditive and $E_{sq}$ is additive on tensor product of the state. This leads to

$$K_D(\rho_{AB}\otimes\sigma_{AB}) - K_D(\rho_{AB}) \leqslant \min\{E_R(\rho_{AB}) + E_R(\sigma_{AB}), E_{sq}(\rho_{AB}) + E_{sq}(\sigma_{AB})\} - K_D(\rho_{AB}). \tag{111}$$

Finally, we have $\max\{E_R, E_{sq}\} \leqslant E_C$ where $E_C$ is an *entanglement cost* [12], which satisfies $E_C \leqslant \min\{S(\sigma_C), S(\sigma_D)\}$.

*Corollary 4.* For a strictly irreducible private state $\gamma_{ABA'B'}$ and any state $\sigma_{CD}$, there is $K_D(\gamma_{ABA'B'}\otimes\sigma_{CD}) - K_D(\gamma_{ABA'B'}) \leqslant \min\{S(\sigma_C), S(\sigma_D)\}$.

*Proof.* Follows from the fact that strictly irreducible private states satisfy $E_R(\gamma_{ABA'B'}) = K_D(\gamma_{ABA'B'})$ [30]. ■

We note, that similar corollary holds for the *maximally correlated states* of the form $\sum_{i,j} b_{ij}|ij\rangle\langle ij|$. For these states $E_D = K_D = E_R$ [12].

The system $CD$ can be viewed as a subsystem of the shield $A'B'$. In that case, observation 1 applies. The above bound is tighter than the latter one, however it holds for a subclass of private states, and for a special case in which system $CD$ is a product with $ABA'B'$.

Furthermore, the bound given in theorem 5 applies in this case with $\delta = \sqrt{1-2^{-I(C:BB'D|AA')}} = \sqrt{1-2^{-I(C:D)}}$. In Fig. 3, we compare the range of applicability of the latter bound with the one given in corollary 4.

We now propose a weaker, but more general bound.

*Observation 7.* For a bipartite state $\rho_{A:BC}$ there is

$$K_D(\rho_{A:BC}) - K_D(\rho_{AB}) \leqslant I(A:C|B) + E_R^\infty(\rho_{AB}) - K_D(\rho_{AB}), \tag{112}$$

where $E_R^\infty(\rho) := \lim_{n\to\infty}\frac{1}{n}E_R(\rho^{\otimes n})$.

*Proof.* We upper bound $K_D(\rho_{A:BC})$ by $E_R^\infty(\rho_{A:BC})$ [18,19]. We then add and subtract $E_R^\infty(\rho_{AB})$. Lemma 1 of Ref. [50,51] allows to upper bound the difference $E_R^\infty(\rho_{A:BC}) - E_R^\infty(\rho_{A:B})$ by $I(A:C|B)$, which proves the thesis. ■

As an immediate corollary, we have that, for the state $\rho_{A:BC}$ such that the leftover state satisfies $E_R(\rho_{AB}) = K_D(\rho_{AB})$, the upper bound on the loss of key is $I(A:C|B)$.

## VI. EXAMPLES OF ACTION OF SIDE CHANNELS FOR SOME PRIVATE STATES

A motivation for this section is given by the fact that certain private states, as well as states with a positive partial transposition that approximate them, are candidates for the *hybrid quantum network* design [24]. This design ensures that unauthorized key generation will be impossible in quantum networks. It is therefore important to know how the distillable key of the latter states behaves under specific side channels.

The findings of Sec. IV ensure us that, upon the erasure of a single qubit of the shield (and hence upon any channel on it), the distillable key of a private state does not decrease by more than twice the entropy of the qubit (see proposition 2). In this section, we concentrate on upper bounds on the drop of a key. Namely, we consider special private states and channels and show the behavior of a key under the latter.

The main result of this section is an observation that the action on just one qubit of the shield of a certain private state can decrease the key by half, irrespectively of the dimension of the shield (which varies in some range). This means that the protection of the state is not a monotonically increasing function of the number of qubits in the shield.

We consider attacks on state $\gamma_V$, given by (8) with $X = V = \frac{1}{2d_s^2}\sum_{i=0,j=0}^{d_s-1}|ij\rangle\langle ji|$ being the (normalized to half) swap operator. Specifically, we consider three values of local dimension of the shield: $d_s = 2, 4, 8$, and an attack by the *bit-flip* channel, specified as an operation $\Lambda_{bf}(\rho) := \alpha(\sigma_x^{A'}\otimes\mathbf{1}_{ABB'})\rho(\sigma_x^{A'}\otimes\mathbf{1}_{ABB'}) + (1-\alpha)\rho$, where $\sigma_x^{A'}$ is the Pauli matrix applied to system $A'$. We upper bound the value of key by $E_R(\rho)$ [18]. As a specific state $\sigma$ we choose the state $(1-p)\sigma_{att} + p\frac{\mathbf{1}}{(2d_s)^2}$, where $\sigma_{att} = \Lambda_{bf}(\frac{1}{2}(|00\rangle\langle 00|\otimes\frac{\mathbf{1}}{d_s} + |11\rangle\langle 11|\otimes\frac{\mathbf{1}}{d_s}))$. The minimal value of an upper bound reached by this operation reads 0.5. The result is shown on Fig. 4.

For the same state, we consider the action of *depolarizing* channel, specified by

$$\Lambda_{\rm dep}(\cdot) = \left(1-\frac{3\alpha}{4}\right)\mathbf{1}(\cdot) + \frac{\alpha}{4}\sigma_x(\cdot)\sigma_x + \frac{\alpha}{4}\sigma_y(\cdot)\sigma_y + \frac{\alpha}{4}\sigma_z(\cdot)\sigma_z. \tag{113}$$

The maximal drop of the relative entropy of entanglement (and hence the key) reads 0.18872, for $\alpha = 1$. Resulting plot is depicted on Fig. 5.

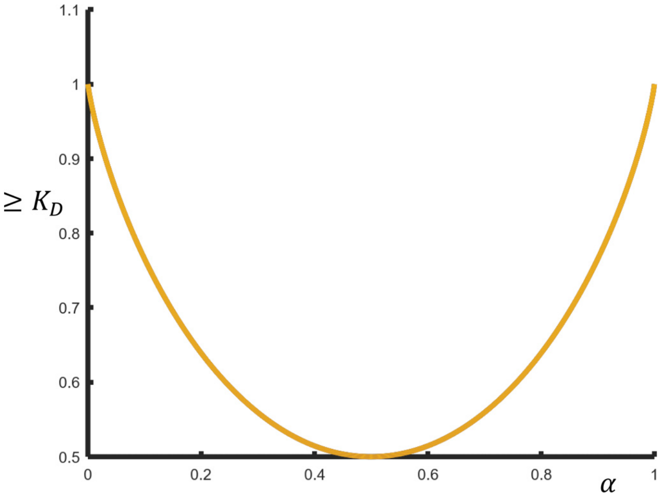


FIG. 4. Upper bound on the relative entropy of entanglement (and hence on $K_D$) of the state $\gamma_V$, after acting with the bit-flip channel on a qubit of its shield. The same plot is obtained for $d_s = 2,\ 4,\$ and 8, hence larger shield is no more shielding than smaller one.

Next, we check the action of the *amplitude damping* channel, $\mathcal{N}_\alpha(\cdot) = M_1(\alpha)(\cdot)M_1(\alpha)^\dagger + M_2(\alpha)(\cdot)M_2(\alpha)^\dagger$, which is specified by parameter $\alpha \in [0, 1]$ and the following two Kraus operators:

$$M_1(\alpha) = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\alpha} \end{bmatrix}, \quad M_2(\alpha) = \begin{bmatrix} 1 & \sqrt{\alpha} \\ 0 & 0 \end{bmatrix}. \tag{114}$$

The minimal value reached in this case is also 0.18872, and the results are the same for $d_s = 2,\ 4,\$ and 8. They are plotted on Fig. 6.

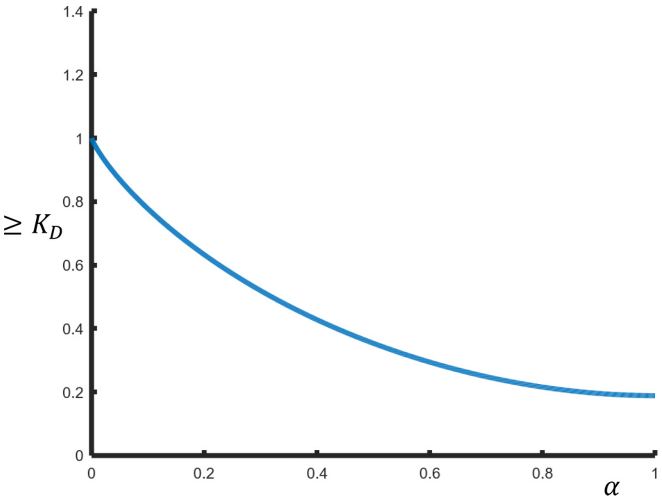


FIG. 5. Upper bound on the relative entropy of entanglement of the state $\gamma_V$ (and hence $K_D$), after acting with depolarizing channel on a qubit of its shield. The same plot is obtained for $d_s = 2,\ 4,\$ and 8.

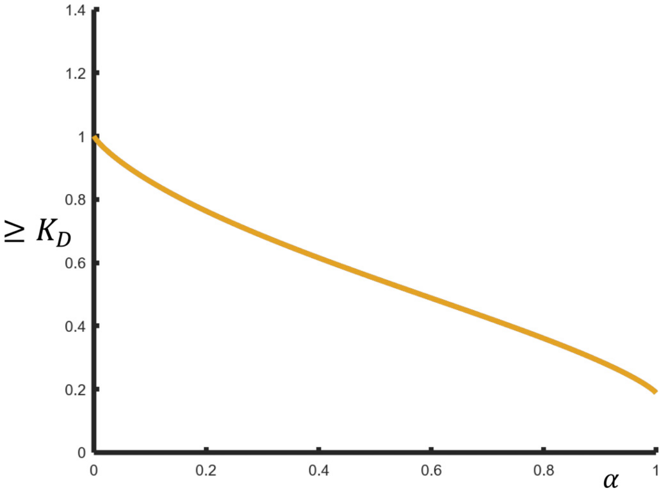


FIG. 6. Upper bound on the relative entropy of entanglement of the state $\gamma_V$ (and hence $K_D$), after acting with amplitude damping channel on a qubit of its shield. The same plot is obtained for $d_s = 2,\ 4,\$ and 8.

## VII. CONNECTION OF LEAKAGE WITH THE NON-MARKOVIANITY OF DYNAMICS

In this section, we reveal the connection between the problem of (non)-Markovianity of a quantum dynamics and that of hacking. We will see that a dynamics is markovian, then for all block states, their key witnessed by certain nonlinear privacy witness does not increase in time under the dynamics.

Given a family $\{\Lambda_t \mid t \geqslant 0\}$ of CPTP maps (interpreted as a temporal dynamics of a system), there is a range of different (generally inequivalent) conditions that can be imposed on this family, to make it called (by, generally, different authors) a "quantum Markovian dynamics" (see, e.g., Refs. [25,52] for review and comparison). Among those conditions, *CP-divisibility*, introduced in Ref. [25] and further studied in Ref. [26], is defined as existence of a CPTP map $V_{t,s}$ such that $\Lambda_t = V_{t,s}\Lambda_s\ \forall t \geqslant s$. In this paper, we fix a terminological choice, identifying Markovianity with CP divisibility.

In what follows, we will construct an analog of a recent result by Kołodyński *et al.* [29], who found that an entanglement measure known as *negativity* is an indicator of non-Markovianity. The authors of Ref. [29] provide examples of tripartite states and show that the invertible map is non-Markovian iff there exist a specially designed tripartite state whose negativity increases in time. (The *invertibility* of $\Lambda_t$ is understood everywhere here as left invertibility, i.e., $\exists!\ \Lambda_t^{-1}$ such that $\Lambda_t^{-1} \circ \Lambda_t = \mathbf{1}$). More precisely, in Ref. [29], there were considered block states of the form (using notation of the latter paper):

$$\begin{aligned} \tau_t^{ABC} = {} & p_1\big(\Lambda_t^A \otimes \mathbf{1}^{B_1}\big)\big(\rho_1^{AB_1}\big) \otimes |\psi_+\rangle\langle\psi_+|^{B_2C} \\ & + p_2\big(\Lambda_t^A \otimes \mathbf{1}^{B_1}\big)\big(\rho_2^{AB_1}\big) \otimes |\psi_-\rangle\langle\psi_-|^{B_2C}, \end{aligned} \tag{115}$$

where $\rho^{ABC} := \tau_{t=0}^{ABC}$ for $\Lambda_{t=0} = \mathbf{1}$. It is shown there that the negativity $E_N$ [53–55], computed in the cut $C : B_1B_2A$, witnesses non-Markovianity of dynamics.

*Theorem 6 (Theorem 2 of Ref. [29]).* For any invertible non-Markovian evolution $\{\Lambda_t \mid t \geqslant 0\}$ there exists a quantum state $\rho_{ABC}$ such that

$$\frac{d}{dt}{E_N}^{AB|C}\left(\tau_t^{ABC}\right) > 0 \tag{116}$$

for some $t > 0$. For single-qubit evolutions $\Lambda_t$, the statement also holds for noninvertible dynamics.

We observe that these states, treated as *bipartite*, are block states, and in special cases also private states. This motivates us to study the connection between the topic of privacy and non-Markovianity.

The proof of a result of Ref. [29] is based on a theorem in Ref. [27], which states that CP-divisibility for a family $\{\Lambda_t \mid t \geqslant 0\}$ of *invertible* CPTP maps is equivalent to a condition $\frac{d}{dt}||(\Lambda_t \otimes \mathbf{1})X||_1 \leqslant 0\ \forall X \in \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H})$ with $X = X^\dagger$, and $\mathcal{B}(\mathcal{H})$ denotes space of all bounded operators on $\mathcal{H}$. In [28] this result has been extended to noninvertible families of CPTP maps satisfying $\mathrm{im}(\Lambda_t) \subseteq \mathrm{im}(\Lambda_s)\ \forall t > s$ (i.e., *image nonincreasing*), and we will use this extension below.

In what follows, we first show the behavior of the privacy witness under an attack of a hacker. Hacker acts on the system $A'$, and her attack is represented by operation $\Lambda_{A'}$. As we will see, the privacy witness degrades monotonically with the decrease of $||(\Lambda_{A'} \otimes \mathbf{1}_{B'})\frac{1}{2}(p_+\rho_+ - p_-\rho_-)||_1$.

*Proposition 4 (Nonlinear privacy witness).* Let $\rho_{ABA'B'} = p_+|\psi_+\rangle\langle\psi_+|_{AB} \otimes \rho_+^{A'B'} + p_-|\psi_-\rangle\langle\psi_-|_{AB} \otimes \rho_-^{A'B'}$, $\Lambda_{A'}$ a CPTP map acting on system $A'$ of $\rho_{ABA'B'}$, $[\Lambda(\rho)]_{psq}$ be the privacy-squeezed state of $\Lambda(\rho) = \Lambda_{A'} \otimes \mathbf{1}_{ABB'}(\rho_{ABA'B'})$ . Then

$$K_D([\Lambda(\rho)]_{psq}) = 1 - h\left(\tfrac{1}{2} + ||(\Lambda_{A'} \otimes \mathbf{1}_{B'})X||_1\right), \tag{117}$$

where $X = \frac{1}{2}(p_+\rho_+^{A'B'} - p_-\rho_-^{A'B'})$.

*Proof.* For the first inequality, we upper bound the amount of key of $[\Lambda(\rho)]_{psq}$ via the relative entropy of entanglement. We note that the state under consideration is Bell-diagonal, of the form $q_+|\psi_+\rangle\langle\psi_+| + q_-|\psi_-\rangle\langle\psi_-|$. Thus its relative entropy of entanglement reads $1 - h(p_{\max})$, where $p_{\max}$ is the maximal probability of a Bell state in the mixture [56]. In our case $\frac{1}{2}(q_+ - q_-) = ||(\Lambda_{A'} \otimes \mathbf{1}_{B'})X||_1 =: c$, hence $q_+ = \frac{1}{2} + c$ and $q_- = \frac{1}{2} - c$. Since $c \geqslant 0$, $q_+ \geqslant q_-$, and so

$$K_D([\Lambda(\rho)]_{psq}) \leqslant E_R([\Lambda(\rho)]_{psq}) = 1 - h\left(\tfrac{1}{2} + c\right). \tag{118}$$

To see the lower bound we note that

$$K_{\mathrm{DW}}([\Lambda(\rho)]_{psq}) \leqslant K_D([\Lambda(\rho)]_{psq}), \tag{119}$$

where $K_{\mathrm{DW}}$ is the rate of Devetak-Winter protocol [9]. The lower bound follows then from corollary 1 of Ref. [57], which states that $K_{\mathrm{DW}}(\rho_{psq}) \geqslant 1 - H(\alpha + \gamma, \alpha - \gamma, \beta, \beta)$, where $\alpha = (p_+ + p_-)/2 = 1/2$, $\beta = 0$ and $\gamma = ||(\Lambda_{A'} \otimes \mathbf{1}_{B'})X||_1$. Hence the assertion follows. ■

Hence, the key of privacy squeezed state of an $\rho$ attacked by $\Lambda_{A'}$ is a privacy witness of $\Lambda_{A'}(\rho)$, and is monotonically strictly decreasing with the decrease of $||(\Lambda_{A'} \otimes \mathbf{1}_{B'})X||_1 \in [0, \frac{1}{2}]$, for hermitian $X$ representing the state.

To uncover the connection between hacking and (non)-Markovianity, we observe the following.

(1) The rate of any protocol of key distillation from a quantum state $\rho$ quantifies the resource (how much key can be gained from a given state). Hence, as the time passes, it can only stay the same (e.g., as a result of local unitary transformation on $\rho$), or decrease (e.g., as a result of the action of the local partial trace of a subsystem of $\rho$).

(2) The (invertible or image nonincreasing) dynamics $\{\Lambda_t \mid t \geqslant 0\}$ (acting on the system $A'$) is markovian iff the map $\Lambda_t \otimes \mathbf{1}_{B'}$ either preserves the trace norm of $X$ or decreases it for all hermitian $X$ and all $t > 0$ [27,28].

Using proposition 4 and equality of dimensions of $A'$ and $B'$, we can formulate an analog of theorem 2 of [29].

*Theorem 7.* An invertible or image nonincreasing dynamics $\{\Lambda_t \mid t \geqslant 0\}$ is non-Markovian iff there exists a block state (10) and $t > 0$ such that

$$\frac{d}{dt}K_D([\Lambda_t(\rho)]_{psq}) > 0. \tag{120}$$

*Proof.* From Refs. [27,28], we have an equivalence of CP-divisibility with $\frac{d}{dt}||(\Lambda_t \otimes \mathbf{1}_{B'})X||_1 \leqslant 0$ for all $X$ and all $t > 0$. This, combined with equivalence of $\frac{d}{dt}||(\Lambda_t \otimes \mathbf{1}_{B'})X||_1 > 0$ with $\frac{d}{dt}h(\frac{1}{2} + ||(\Lambda_t \otimes \mathbf{1}_{B'})X||_1) < 0$, and with proposition 4, completes the proof. ■

The above theorem establishes a link with an operational quantity, the *witnessed distillable key* (WDK), rather than with a theoretical measure of entanglement, such as the negativity $E_N$. It can be interpreted as follows: non-Markovian dynamics implies the flow of privacy from environment to the system.

Interestingly, WDK is not an entanglement measure. Indeed, to make WDK zero for a block state, it is enough that $||p_+\rho_+ - p_-\rho_-||_1 = 0$, which is true for $X = p_+\rho_+ - p_-\rho_-$ being a zero matrix. This implies $p_+ = p_- = \frac{1}{2}$ and $\rho_+ = \rho_- \equiv \rho$. In this case the block state takes form $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes \rho$. However, if $\rho$ is entangled, then WDK is zero, while the block state is clearly entangled as a product of separable and entangled state. It would be interesting to extend this result to other operational entanglement measures, possibly via the approach of [31]. Finally we note, that WDK is the inherently nonlinear witness of non-Markovianity. In that, this approach is complementary to that of considered earlier in [58], where *linear* witness of a slightly different notion of non-Markovianity, has been proposed.

## VIII. DISCUSSION

We have provided bounds on the leakage of private randomness and private key. We have shown that the private randomness in distributed setting can not drop down by more than $S(a) + \log_2 |a|$ upon unitary transformation followed by the erasure of a system $a$. It would be interesting to consider a more general case, in which a POVM is performed by the hacker. In this case, the difficulty rests in controlling the amount of private randomness that can be added to the system. Indeed, every POVM can be considered as von Neumann measurement on the embedded system. However, embedding implies attaching a pure state, i.e., the state with private randomness, which we would like to avoid in the resource-theoretic approach.

Regarding private key, we have proved its nonlockability for the first nontrivial class of mixed states—the class of irreducible private states. Let us note here that the assumption that the state is irreducible is not restrictive. Indeed, a nonirreducible private state can have an arbitrary state on the shield.

Hence nonlocking for the general private state is as hard as the still open problem of nonlockability of the key for any state. We have shown that the bound on leakage [that reads $2S(a)$] is tight. We then provided a refinement of this result, which reflects the fact, that less correlated qubits affect the drop of key by less amount, dependent on the value of $I(a:B|A)$. We have done it for generalized private states called *irreducible Schmid-twisted pure states*. It is an interesting open problem if the same would hold for the class of twisted pure states. Another open problem which arises concerns one-way distillable key by means of communication from $A$ to $B$. Our upper bounds for the leakage differ in the case when the leakage affects the system $A$ and from the case when it affects system $B$. It is an open problem if they need to differ, that is whether one-way distillable key from $A$ to $B$ drops down by a different number for some state when the same leaking channel acts on system $A$ from the case when it acts on system $B$.

We have also considered the effect of the leakage via exemplary side channels. For the considered private state, we observed that the key drops down by the same amount irrespectively of the size of the shield. This means that it is not the case that the larger is shield, the more protected is the key of this private states. Designing private states which are immune to the qubit loss on the shield (and having low distillable entanglement) would be a good step towards the hybrid quantum network provided in Ref. [24].

Still, however, a major theoretical problem rests in answering the question of how much the key drops down under the erasure of a system of an arbitrary quantum state. As we argue, it remains open even in the case when the system is in tensor product with the rest of the state under consideration.

Finally, we proved a connection between the (non)-Markovianity of quantum dynamics and hacking. We have found an operational quantity which is a nonlinear private key witness, $K_D([\rho]_{psq})$, the key of a privacy-squeezed state. In this context, it would be interesting to find an operational entanglement measure, the behavior of which corresponds to (non)-Markovianity of dynamics. It is also interesting if other variants of the definition of (non)-Markovianity can be connected to a secret key extraction (see Ref. [58] in this context).

## ACKNOWLEDGMENTS

K.H. acknowledges Marcus Grassl and Anindita Bera for enlightening discussions. K.H., O.S., and R.P.K. acknowledge support by the National Science Centre grant Sonata Bis 5 (Grant No.: 2015/18/E/ST2/00327). D.Y. was supported by the NSFC (Grants No. 11375165 and No. 11875244) and by the NFR Project No. ES564777. We acknowledge partial support by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. MAB/2018/5, co-financed by EU within Smart Growth Operational Programme). The "International Centre for Theory of Quantum Technologies" project (Contract No. MAB/2018/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

## APPENDIX

Here we partially recover lemma V.3 of Ref. [40]. The problem with the original statement of this lemma is: when two states $\rho_{AB}$ and $\widetilde{\rho}_{AB}$ are close in trace norm, it does not imply that the state $\rho_{AE}$ and $\widetilde{\rho}_{AE}$ are so (here $\rho_{ABE}$ is an extension of $\rho_{AB}$ to system $E$). However this holds true, yet with a worse factor, given the extension $\rho_{ABE}$ is pure.

In what follows, we use the fidelity defined by $F(\rho,\sigma) := ||\sqrt{\rho}\sqrt{\sigma}||_1^2$. Before showing a restatement of the aforementioned lemma, we show that if two bipartite states are close, so are their purifications (this technique was used before in Ref. [19], which we recall here for the completeness of the presentation).

Let $||\rho_{AB}-\widetilde{\rho}_{AB}||\leqslant\delta$. By the Fuchs-van de Graaf inequality [47], we have

$$\sqrt{F(\rho_{AB},\widetilde{\rho}_{AB})}\geqslant 1-\frac{\delta}{2}. \tag{A1}$$

On the other hand, by the Uhlmann theorem [34], $F(\rho_{AB},\widetilde{\rho}_{AB})=\max_{\phi_{\widetilde{\rho}_{AB}}}|\langle\psi_{\rho_{AB}}|\phi_{\widetilde{\rho}_{AB}}\rangle|^2$ and $|\langle\psi_{\rho_{AB}}|\phi_{\widetilde{\rho}_{AB}}\rangle|^2=F(\psi_{\rho_{AB}},\phi_{\widetilde{\rho}_{AB}})$, where $\psi_{\rho_{AB}}$ and $\phi_{\widetilde{\rho}_{AB}}$ are purifications of $\rho_{AB}$ and $\widetilde{\rho}_{AB}$ respectively. Applying again the Fuchs-van de Graaf inequality, we obtain

$$\begin{aligned}&|||\psi_{\rho_{AB}}\rangle\langle\psi_{\rho_{AB}}|-|\phi_{\widetilde{\rho}_{AB}}\rangle\langle\phi_{\widetilde{\rho}_{AB}}|||_1\\&\leqslant\sqrt{1-\left(1-\frac{\delta}{2}\right)^2}\leqslant\sqrt{2\delta}.\end{aligned} \tag{A2}$$

Lemma 4 (below) recovers the content of lemma V.3 of Ref. [40] for the case of system $E$ purifying systems $AB$. (By notation $K^{\rightarrow}(\rho_{AB})$ we mean $K^{\rightarrow}(|\psi_{\rho_{AB}}\rangle)$, where $\mathrm{tr}_E|\psi_{\rho_{ABE}}\rangle\langle\psi_{\rho_{ABE}}|=\rho_{AB}$).

*Lemma 4.* For bipartite states $\rho_{AB}$ and $\widetilde{\rho}_{AB}$ satisfying $||\rho_{AB}-\widetilde{\rho}_{AB}||_1\leqslant\delta$ with $\delta\leqslant\frac{1}{2}$, there is

$$\begin{aligned}|K^{\rightarrow}(\rho_{AB})-K^{\rightarrow}(\widetilde{\rho}_{AB})|\leqslant&(4\delta+4\sqrt{2\delta})\log_2 d_A\\&+2h(\delta)+2h(\sqrt{2\delta}).\end{aligned} \tag{A3}$$

*Proof.* Following Ref. [40], we consider difference of conditional entropies: $K^{\rightarrow}(\rho)=-S(A|BT)+S(A|ET)$, where $T$ is generated via measurement on system $A$. Hence,

$$||\rho_{ABT}-\widetilde{\rho}_{ABT}||_1\leqslant\delta, \tag{A4}$$

since the trace norm does not increase under CPTP maps. Further, from (A2), there is $||\rho_{AE}-\widetilde{\rho}_{AE}||_1\leqslant\sqrt{2\delta}$ and, by the same argument,

$$||\rho_{AET}-\widetilde{\rho}_{AET}||_1\leqslant\sqrt{2\delta}. \tag{A5}$$

We have then

$$\begin{aligned}|K^{\rightarrow}(\rho_{AB})-K^{\rightarrow}(\widetilde{\rho}_{AB})|\leqslant&|S(\widetilde{A}|\widetilde{BT})-S(A|BT)|\\&+|S(A|ET)-S(\widetilde{A}|\widetilde{ET})|.\end{aligned} \tag{A6}$$

We further bound the two terms in right-hand side (r.h.s.) using theorem by Alicki and Fannes [59], which states that if two states $\rho_{AB}$ and $\sigma_{AB}$ satisfy $\epsilon=||\rho_{AB}-\sigma_{AB}||_1$, then

$$|S(A|B)-S(\widetilde{A}|\widetilde{B})|\leqslant 4\epsilon\log_2 d_A+2h(\epsilon), \tag{A7}$$

where $d_A$ is dimension of system $A$ and $h(\cdot)$ is the binary Shannon entropy. Applying the above inequality to (A6), we obtain

$$|K^{\rightarrow}(\rho_{AB}) - K^{\rightarrow}(\widetilde{\rho}_{AB})| \leqslant + 4\delta \log_2 d_A + 2h(\delta) + 4\sqrt{2\delta}\log_2 d_A + 2h(\sqrt{2\delta}), \tag{A8}$$

only if $\sqrt{2\delta} \leqslant \frac{1}{2}$, and hence $\delta \leqslant \frac{1}{2}$. Here we use the fact that $h(x)$ is strictly increasing for $x \in [0, \frac{1}{2}]$, so that $h(||\rho_{AB} - \widetilde{\rho}_{AB}||_1) \leqslant h(\sqrt{2\delta})$. ■

It is important to note that quantum purification is the worst extension from the cryptographic point of view because it allows an eavesdropper to create any other extension by local operation. Hence, the above result is important from a cryptographic point of view.

[1] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).

[2] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Sci. Rep. **7**, 8403 (2017).

[3] W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).

[4] W. Wang, K. Tamaki, and M. Curty, Sci. Rep. **11**, 1678 (2021).

[5] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society Press, New York, Bangalore, India, 1984), pp. 175–179.

[6] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[7] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[8] R. Arnon-Friedman, Reductions to IID in device-independent quantum information processing, arXiv:1812.10922.

[9] I. Devetak and A. Winter, Proc. R. Soc. London A **461**, 207 (2005).

[10] R. König, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502 (2007).

[11] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 200501 (2005).

[12] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[13] M. Christandl and A. Winter, IEEE Trans. Inf. Theory **51**, 3159 (2005).

[14] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).

[15] B. van der Vecht, X. Coiteux-Roy, and B. Skoric, arXiv:2006.02476 [quant-ph].

[16] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, Rep. Prog. Phys. **80**, 124001 (2017).

[17] D. Yang, K. Horodecki, and A. Winter, Phys. Rev. Lett. **123**, 170501 (2019).

[18] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[20] P. Horodecki, Lockable entanglement measures, Problem 25 at the IQOQI list of open problems, https://oqp.iqoqi.univie.ac.at/open.

[21] R. Renner, Security of quantum key distribution, Ph.D. thesis, ETH Zurych, 2005.

[22] J. M. Renes and R. Renner, IEEE Trans. Inf. Theory **58**, 1985 (2012).

[23] O. Fawzi and R. Renner, Commun. Math. Phys. **340**, 575 (2015).

[24] O. Sakarya, M. Winczewski, A. Rutkowski, and K. Horodecki, Phys. Rev. Research **2**, 043022 (2020).

[25] M. M. Wolf and J. I. Cirac, Commun. Math. Phys. **279**, 147 (2008).

[26] A. Rivas, S. F. Huelga, and M. B. Plenio, Phys. Rev. Lett. **105**, 050403 (2010).

[27] D. Chruściński, A. Kossakowski, and Á. Rivas, Phys. Rev. A **83**, 052128 (2011).

[28] D. Chruściński, A. Rivas, and E. Størmer, Phys. Rev. Lett. **121**, 080407 (2018).

[29] J. Kołodyński, S. Rana, and A. Streltsov, Phys. Rev. A **101**, 020303(R) (2020).

[30] K. Horodecki, P. Ćwikliński, A. Rutkowski, and M. Studziński, New J. Phys. **20**, 083021 (2018).

[31] M. Christandl and R. Ferrara, Phys. Rev. Lett. **119**, 220506 (2017).

[32] K. Horodecki, General paradigm for distilling classical key from quantum states—On quantum entanglement and security, Ph.D. thesis, University of Warsaw, 2008.

[33] K. Banaszek, K. Horodecki, and P. Horodecki, Phys. Rev. A **85**, 012330 (2012).

[34] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[35] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[36] M. Christandl and A. Winter, J. Math. Phys. **45**, 829 (2004).

[37] N. J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997).

[38] M. Tomamichel, *Quantum Information Processing with Finite Resources, Mathematical Foundations*, Springer Briefs in Mathematical Physics, Vol. 5 (Springer, Cham, 2016).

[39] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Theory of Cryptography*, edited by S. P. Vadhan (Springer, Berlin, Heidelberg, 2007), pp. 456–478.

[40] M. L. Nowakowski, J. Phys. A: Math. Theor. **49**, 385301 (2016).

[41] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).

[42] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[43] M. Shirokov, J. Math. Phys. **58**, 102202 (2017).

[44] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[45] K. P. Seshadreesan and M. M. Wilde, Phys. Rev. A **92**, 042321 (2015).

[46] A. Uhlmann, Ann. Phys. **497**, 524 (1985).

[47] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[48] K. Li, A. Winter, X. B. Zou, and G. C. Guo, Phys. Rev. Lett. **103**, 120501 (2009).

[49] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[50] F. G. S. L. Brandão, M. Christandl, and J. Yard, Commun. Math. Phys. **306**, 805 (2011).

[51] F. G. S. L. Brandão, M. Christandl, and J. Yard, Commun. Math. Phys. **316**, 287 (2012).

[52] L. Li, M. J. W. Hall, and H. M. Wiseman, Phys. Rep. **759**, 1 (2018).

[53] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).

[54] J. Eisert, Entanglement in quantum information theory, Ph.D. thesis, University of Potsdam, 2006.

[55] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).

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

[57] M. Christandl, R. Ferrara, and K. Horodecki, Phys. Rev. Lett. **126**, 160501 (2021).

[58] M. Banacki, M. Marciniak, K. Horodecki, and P. Horodecki, Information backflow may not indicate quantum memory, arXiv:2008.12638 [quant-ph].

[59] R. Alicki and M. Fannes, Note on multiple additivity of minimal Renyi entropy output of the Werner-Holevo channels, arXiv:quant-ph/0407033 [quant-ph].