Cost of quantum secret key

Karol Horodecki[1,2,3], Leonard Sikorski [1], Siddhartha Das[4], and Mark M. Wilde[3]

[1]Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland

[2]International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland

[3]School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA

[4]q4i, Centre for Quantum Science and Technology (CQST), Center for Security, Theory and Algorithmic Research (CSTAR), International Institute of Information Technology Hyderabad, Gachibowli 500032, Hyderabad, Telangana, India

arXiv:2402.17007v2 [quant-ph] 24 Apr 2026

In this paper, we develop the resource theory of quantum secret key. Operating under the assumption that entangled states with zero distillable key *do not* exist, we define the *key cost* of a quantum state, and device. We study its properties through the lens of a quantity that we call the *key of formation*. The main result of our paper is that the regularized key of formation is an upper bound on the key cost of a quantum state. The core protocol underlying this result is privacy dilution, which converts states containing ideal privacy into ones with diluted privacy. Next, we show that the key cost is bounded from below by the regularized relative entropy of entanglement, which implies the irreversibility of the privacy creation-distillation process for a specific class of states. We further focus on mixed-state analogues of pure quantum states in the domain of privacy, and we prove that a number of entanglement measures are equal to each other for these states, similar to the case of pure entangled states. The privacy cost and distillable key in the single-shot regime exhibit a yield-cost relation, and basic consequences for quantum devices are also provided. Importantly, our results presented here will remain valid even if entangled states with zero distillable key were shown to exist.

1 Introduction

Quantum mechanics is a rather surprising physical theory, as it is reversible in principle, contrary to our common experience. After an arbitrary quantum operation is applied to a system, if full access to its environment is available, the system's state can be set back to its initial form by a reversal operation. However, in practice, reversibility is usually not possible. The system, after an operation, typically becomes entangled with an inaccessible environment in an irreversible way. This irreversibility can be quantified in different ways in the resource-theoretic framework [1], which was first introduced and studied for the case of the resource theory of entanglement [2].

The origin of irreversibility is even more fundamental in the case of the resource of quantum secret key. In this setting, an eavesdropper or hacker will never give back a system that has leaked, even if it might be possible in practice. This fact was first noticed and studied in the classical scenario of secret key agreement (SKA) [3, 4]. There, the adversary has only a classical memory Z and eavesdrops on two honest parties, who possess classical random variables X and Y, respectively, and transform them by local (classical) operations and public communication. Inspired by an apparent correspondence between entanglement theory and SKA established in [5], it was proved that the cost of creating a distribution sometimes exceeds its distillable secure content in the SKA scenario [4] (see also [6, 7, 8, 9, 10] for related work). Key distillation for the quantum generalization of SKA has been studied in [11, 12, 13] via a mapping of tripartite distributions into pure tripartite states, as proposed in [14] [1].

Building a quantum internet infrastructure is one of the main visions of the quantum information community [15]. It is then important to understand the cost of the network's constituents, i.e., quantum states and channels with secure key. Indeed, since pure entanglement is not a precondition of quantum security [16, 17], we assert here that a secure key is a proper resource for quantifying the information-theoretic expense of the quantum-secured internet. Motivated by this, we initiate the study of the cost of a secret key and understanding the problem of irreversibility in the quantum cryptographic scenario.

In the most basic case of a point-to-point connection in the network, the two honest parties share a bipartite quantum state and process it by local oper-

Karol Horodecki: karol.horodecki@ug.edu.pl
Leonard Sikorski : leonard.sikorski@phdstud.ug.edu.pl
Siddhartha Das: das.seed@iiit.ac.in
Mark M. Wilde: wilde@cornell.edu

[1]The mapping of [14] is the following embedding of a classical distribution $P(x,y,z)$ into a Hilbert space: $\{P(x,y,z)\}_{x,y,z} \mapsto |\Psi\rangle_{XYZ} := \Sigma_{x,y,z}\sqrt{P(x,y,z)}|x,y,z\rangle$.

ations and classical communication (LOCC). Assuming the worst case, the quantum eavesdropper has access to a purifying system of a purification [18] of the state of the honest parties and obtains any classical communication and any system traced out by them during LOCC processing. The main question we pose in this setting is as follows: "How much private key is needed for the creation of an arbitrarily good approximation of n copies of a bipartite quantum state by LOCC for sufficiently large n?"

With this in mind, we depart from the above approach of exploring the embedding of SKA into the quantum scenario [2]. Instead, we develop the resource theory of key secure against a quantum adversary. It is important to note that the latter theory differs from the resource theory of entanglement. This is because there exist states that contain no distillable entanglement ($E_D = 0$) [19] but contain a strictly positive rate of distillable key K_D secure against a quantum adversary [16, 17].

While entanglement theory has been thoroughly studied [20] since its invention [2, 21], the resource theory of private key secure against a quantum adversary has yet to be developed fully from the resource-theoretic perspective. On the one hand, lower and upper bounds on the distillable key have been developed thoroughly, starting from the seminal protocols BB84 and E91 [22, 23] and their follow-ups [24, 25, 26, 27, 28, 29] in a number of cryptographic scenarios (cf. [30, 31]). Also, the aforementioned distillable key K_D has been shown to be an entanglement measure and studied in [16, 17, 32]. On the other hand, to our knowledge, the privacy cost has hitherto not been introduced nor studied in the fully quantum setup.

In this paper, we close this gap by defining and characterizing the key cost K_C, a fundamental quantity in the resource theory of privacy. The key cost is an upper bound on the distillable key secure against a quantum eavesdropper, and it indicates how much key one needs to invest when creating a quantum state. In order to characterize the key cost, we introduce and study another quantity, the *key of formation* K_F. Informally, K_F is equal to the minimum average amount of key content of a state, where the average is taken over all decompositions of the state into a finite mixture of pure states that are Schmidt-twisted [33, 34] (see (13) for a formal definition). One of our main results, relating the key cost and the key of formation, is encapsulated in the following inequality

$$K_C(\rho) \leq K_F^{\infty}(\rho), \tag{1}$$

where $K_F^{\infty}(\rho) \coloneqq \lim_{n\to\infty} \frac{1}{n} K_F(\rho^{\otimes n})$ (see Theorem 4).

[2] We consider, in fact, processing of an arbitrary pure state $|\psi\rangle_{ABE}$ (such that $\mathrm{Tr}_E |\psi\rangle\langle\psi|_{ABE} = \rho_{AB}$) by (quantum) local operations and public communication. The pure state $|\psi\rangle_{ABE}$ in our approach may not originate from any classical distribution via the Collins–Popescu mapping.

We note here that key cost and key of formation are analogous to the entanglement cost E_C and entanglement of formation E_F in entanglement theory [2], respectively. Furthermore, the aforementioned generalized private states form a class of states in the privacy domain that corresponds to the class of pure states in entanglement theory. Also, the inequality in (1) is partially analogous to the relation $E_F^{\infty}(\rho) = E_C(\rho)$ from entanglement theory [35, 36]. Although there are analogies between entanglement and private key [5, 14], we should note that there are important distinctions, some of which have led to profound insights into the nature of quantum information [37, 38, 39]. Additionally, the technicalities of dealing with privacy are more subtle and involved than when dealing with entanglement [16, 17]. For our specific problem considered here, i.e., to obtain (1), it was necessary for us to develop techniques beyond what is currently known in entanglement theory. Indeed, our main technical contribution here, for establishing (1), involves designing a protocol that dilutes privacy.

The applicability of the introduced quantities goes beyond the resource theory of (device-dependent) private key. Naturally, K_C is a novel entanglement measure. K_F and K_C are also applicable in a scenario in which security is independent of the inner workings of the devices (device-independent security [40]). Indeed, by the technique of [41], the *reduced* versions of K_C and K_F are novel measures of Bell nonlocality [42]. More importantly, the single-shot version of the reduced K_C, that is, the reduced single-shot key cost $K_C^{\varepsilon\downarrow}$, can be treated as the definition of the key cost of a device — a quantity that has not been considered so far.

In large part, the quantum internet, when built, will be used to transfer classical data securely. Hence, the right choice of a quantum state with unit cost appears to be a state that has one bit of ideally secure key. Such states have been introduced already in [16, 17] and are called private bits. More generally, we can consider d-dimensional private states, called private dits. These states, denoted by $\gamma(\Phi^+)$, can be understood as a maximally entangled state

$$\Phi^+_{A_K B_K} \coloneqq \frac{1}{d_k} \sum_{i=0}^{d_k-1} |ii\rangle\langle jj|_{A_K B_K}, \tag{2}$$

where $d_k = \min\{|A_K|, |B_K|\}$ ($|A_K|$ denotes the dimension of the Hilbert space of A_K), which has become "twisted" with some arbitrary shared state $\rho_{A_S B_S}$ by means of a controlled-unitary

$$\tau_{A_K B_K A_S B_S} \coloneqq \sum_{i=0}^{d_k-1} |ii\rangle\langle ii|_{A_K B_K} \otimes U_i^{A_S B_S}, \tag{3}$$

leading to

$$\gamma_{d_k}(\Phi^+) \coloneqq \tau(\Phi^+_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger. \tag{4}$$

Since it has been shown (see [16, 17]), that a state contains at least $\log_2 d$ bits of secure key accessible by local (incomplete) von Neumann measurements if and only if it is of the above form, it is clear that the private states are resourceful states in the resource theory of private key. However, it is not clear which states are useless [1] (or "free" in the language of resource theory), from which no key can be obtained. So far, it is known that separable, i.e., disentangled states, are useless [43], while it remains open if entangled but key-undistillable states exist. This question is one of quantum information theory's most difficult open problems (see Problem 24 on the IQOQI Vienna list [44]). In this paper, we develop the resource theory of private key up to the current state of the art, i.e., under the assumption that there *do not exist* entangled but key-undistillable states.

2 Summary of results

2.1 Irreversibility of privacy

Informally, the *key cost* $K_C(\rho_{AB})$ of a quantum state ρ_{AB} is the minimal ratio of the number $\log_2 d_n$ of key bits, in the form of a private state $\gamma_{d_n}(\Phi^+)$, needed to create $\rho^{\otimes n}$ approximately, to the number n of copies, in the asymptotic limit of large n: it is equal to the minimal value of $\lim_{n\to\infty} \frac{\log_2 d_n}{n}$ such that the approximation error tends to zero. Based on this definition, we also quantify the cost of devices in terms of secret key [42] (see Section 11).

We now make several observations that are direct consequences of the definitions of the key cost and key of formation and facts known already in the literature. First, it is straightforward to see that $K_F \leq E_F$ because the set of pure states is a subset of the set of generalized private states and $K_C \leq E_C$ because a maximally entangled state is also a private state. Furthermore, if each of the local quantum systems A and B is either a qubit or qutrit, i.e., $|A| \in \{2,3\}$ and $|B| \in \{2,3\}$, then $K_F = E_F$. This is because, in this case, the shield systems $A_S B_S$ have trivial dimensions equal to one so that the generalized private states coincide with pure states. However, it is not clear if $K_C = E_C$ in this low-dimensional case. On the other hand in larger dimensions, we know that $K_C \neq E_C$ generally, as is the case for the so-called flower state [45]. This state is a $(2d_s)^2$-dimensional private state for which $K_C \leq 1$ by definition while $E_C \geq \log_2 d_s/2$ [46]. More importantly, by a standard approach, we prove that

$$K_C(\rho) \geq E_R^\infty(\rho), \tag{5}$$

(see Theorem 2), where the regularized relative entropy of entanglement is defined as [47]

$$E_R^\infty(\rho) \coloneqq \lim_{n\to\infty} \frac{1}{n} E_R(\rho^{\otimes n}), \tag{6}$$

$$E_R(\rho) \coloneqq \inf_{\sigma\in \mathrm{SEP}} \mathrm{Tr}[\rho(\log_2\rho - \log_2\sigma)], \tag{7}$$

with SEP denoting the set of all separable states of a given bipartite system. Furthermore, there are states $\widehat{\rho}$ for which an entanglement measure called *squashed entanglement* E_{sq} is strictly less than E_R^∞ [48, 49]. Since both E_R^∞ and E_{sq} are upper bounds on K_D [16, 32, 17, 50], this leads to a first example of irreversibility in the quantum cryptographic scenario

$$K_D(\widehat{\rho}) \leq E_{\mathrm{sq}}(\widehat{\rho}) \ll E_R^\infty(\widehat{\rho}) \leq K_C(\widehat{\rho}). \tag{8}$$

Hence, the resource of private key joins the family of resources for which irreversibility occurs [1].

2.2 The key cost

To quantify the investment in creating a state, we need to control how much private key a given private state possesses. A cogent choice is the class of irreducible private states, i.e., those for which $K_D(\gamma(\Phi^+_{d_k})) = \log_2 d_k$, such that there is no more key in this state than that contained in its key systems. This class has been characterized in [51] in the following way: if there are no entangled but key undistillable states, all irreducible private states are *strictly* irreducible (SIR) [34, 52], that is, taking the form

$$\gamma_{d_k,d_s}(\Phi_+) \coloneqq \frac{1}{d_k}\sum_{i,j=0}^{d_k-1} |ii\rangle\langle jj|_{A_K B_K} \otimes U_i \rho_{A_S B_S} U_j^\dagger, \tag{9}$$

where $U_i \rho_{A_S B_S} U_i^\dagger$ is a separable state for each i and $\rho_{A_S B_S}$ is an arbitrary $d_s \times d_s$ state. Since we study the key cost K_C up to the current state of the art, such that no entangled but key undistillable states are known to exist, we focus on the above class of strictly irreducible states in the definition of the key cost. Under this assumption, the definition of the key cost in the asymptotic regime is as follows:

Definition 1. *The asymptotic key cost $K_C(\rho)$ and one-shot key cost $K_C^\varepsilon(\rho)$ of a state ρ_{AB} are defined as*

$$K_C(\rho) \coloneqq \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}), \tag{10}$$

$$K_C^\varepsilon(\rho) \coloneqq \inf_{\substack{\mathcal{L}\in \mathrm{LOCC},\\ \gamma_{d_k,d_s}\in \mathrm{SIR}}} \left\{ \log_2 d_k : \frac{1}{2}\|\mathcal{L}(\gamma_{d_k,d_s}) - \rho\|_1 \leq \varepsilon \right\}, \tag{11}$$

where the infimum in (11) is taken over every LOCC channel $\mathcal{L}$ and every strictly irreducible private state γ_{d_k,d_s} with an arbitrarily large, finite shield dimension $d_s \geq 1$.

The choice of LOCC in the above definition is justified by the fact that, in the private key distillation scenario, it is known that the following two approaches are equivalent: (i) the distillation of dits

of privacy in the form $\frac{1}{d_k}\sum_{i=0}^{d_k-1}|ii\rangle\langle ii|\otimes\rho_E$ from a tripartite state $\psi_{ABE}^{\otimes n}$ via local operations and public communication (LOPC) and (ii) the distillation of private states $\gamma_{d_k,d_s}(\Phi^+)$ for some d_s, from $\rho_{AB}^{\otimes n}$ using LOCC [17, 16, 34]. While most of the following results hold for the asymptotic definition of the key cost, we prove a yield-cost relation in the one-shot scenario that bounds the one-shot distillable key from above by the one-shot key cost and a small correction factor

$$K_D^{\varepsilon_1}(\rho)\leq K_C^{\varepsilon_2}(\rho)+\log_2\left(\frac{1}{1-(\varepsilon_1+\varepsilon_2)}\right), \tag{12}$$

for $\varepsilon_1+\varepsilon_2<1$ and $\varepsilon_1,\varepsilon_2\in[0,1]$, where $K_D^{\varepsilon_1}$ is the single-shot version of the distillable key K_D (see Theorem 6). See [53, 54] for similar prior results.

2.3 The key of formation

Private states can be naturally generalized to a class of states that correspond to pure bipartite states. This generalization is achieved when one twists a pure bipartite state ψ in such a way that τ controls the Schmidt bases of ψ, thereby obtaining generalized private states [34, 33], which need not be pure and are denoted by $\gamma(\psi)$. Below we focus on a subclass of the generalized private states, those which are *strictly irreducible*. They have a structure that assures irreducibility by construction; that is, they satisfy a condition analogous to the one from (9) characterising strictly irreducible private states. We use these states to define the key of formation of a bipartite state ρ_{AB} as an analog of the entanglement of formation

$$K_F(\rho_{AB}):=\inf_{\{p_k,\gamma(\psi_k)\}_{k=1}^{k_{\max}}}\sum_{k=1}^{k_{\max}}p_k S_{A_K}(\gamma(\psi_k)), \tag{13}$$

where

$$S_X(\rho_{XY}):=-\operatorname{Tr}[\rho_X\log\rho_X] \tag{14}$$

is the von Neumann entropy of the reduced state $\rho_X\equiv\operatorname{Tr}_Y[\rho_{XY}]$. Here $\sum_{k=1}^{k_{\max}}p_k\gamma(\psi_k)=\rho_{AB}$, and for each k, there exist unitary transformations $W_A^{(k)}\colon A\to A_KA_S$ for Alice and $W_B^{(k)}\colon B\to B_KB_S$ for Bob, such that the key can be obtained by measuring the systems A_KB_K directly with local von Neumann measurements in the Schmidt bases of ψ_k. The shield systems A_SB_S protect the key from the eavesdropper. Moreover, each state $\gamma(\psi_k)$ has the property that all of its key content is accessible in the A_KB_K systems via local von Neumann measurements. In particular, conditioned on the outcomes of this measurement, the systems A_SB_S remain separable; i.e., the state is strictly irreducible. In the definition above, $k_{\max}$ is arbitrarily large but finite. Based on [55], we prove that taking the infimum over $k_{\max}\leq|A|^2|B|^2+1$ suffices. The relation of the introduced quantities K_C, K_F, K_F^∞ to the well known entanglement measures such as distillable key, entanglement cost, entanglement of formation, etc., is represented in Figure 1.

2.4 The case of reversibility

The main result (1) along with the fact that $K_F(\rho)=\inf_{\{(p_k,\gamma(\psi_k))\}}\sum_k p_kK_D(\gamma(\psi_k))$, combined with other bounds, implies our second main result. Namely,

$$\begin{aligned}K_D(\gamma(\psi))=E_R(\gamma(\psi))=E_R^\infty(\gamma(\psi))=K_F^\infty(\gamma(\psi))=\\ K_F(\gamma(\psi))=K_C(\gamma(\psi))=S_A(\psi)=S_{A_K}(\gamma(\psi))\end{aligned} \tag{15}$$

(see Theorem 5). We note that these equalities are appealing, in analogy with what happens for pure states ψ in entanglement theory, for which the distillable entanglement, relative entropy of entanglement, and entanglement cost all coincide and are equal to the von Neumann entropy of the marginal of ψ. The difference is that system A_K is the full local subsystem for $\gamma(\psi)$ only when $\gamma(\psi)$ is itself a pure state, which is generically not the case.

More importantly, the analogy with entanglement theory is only partial. Indeed, the squashed entanglement [56] does not lie between the distillable key and the key cost (see detailed argument given in Remark 5). It is opposed to the fact that every proper entanglement monotone lies between the distillable entanglement and entanglement cost [57].

2.5 Dilution protocol

As mentioned, the core of the upper bound on K_C via (1) is a dilution protocol (DP). This protocol transforms a private state via LOCC into an approximation of a large number of copies of the desired generalized private state. Our idea behind this protocol is ultimately different from that of [58], where dilution of entanglement has been proposed using pure entanglement and quantum teleportation [2]. A key difference arises because private states have, in general, a low amount of pure entanglement. We partly follow the idea of coherence dilution [59], because generalized private states have a basis that is naturally distinguished by the fact that coherence in that basis assures secrecy of the key.

Our main statement regarding this dilution protocol is encapsulated in the following theorem (Theorem 3):

Theorem 1. *For every generalized private state $\gamma(\psi)$ with $|\psi\rangle=\sum_{a\in\mathcal{A}}\lambda_a|e_a\rangle|f_a\rangle$, and sufficiently large n, the state $\gamma(\psi)^{\otimes n}$ can be created by LOCC from $\gamma_{d_n}(\Phi^+)\otimes\Phi^+_{d'_n}$ with error less than 2ε in trace distance, and the number of key bits is equal to*

$$\log_2 d_n=\lceil n(S_{A_K}(\psi)+\eta)\rceil, \tag{16}$$

with $\log_2 d'_n=\lceil 4\delta n\rceil$, where $\eta,\varepsilon,\delta\to0$ as $n\to\infty$.

The idea of the proof is as follows. Both parties are allowed at the beginning of the protocol to share an arbitrary private state of their choice. We thus fix their initial private state to be $\gamma_{d_n}(\Phi_+)$ with $d_n:=|\mathcal{A}|^{\lceil n(S_{A_K}(\psi)+\eta)\rceil}$, that has a shield system in the same

state and rotated by the same twisting unitary as the target state we want to create, i.e.,

$$\gamma(\psi)^{\otimes n} = \sum_{\mathbf{s},\mathbf{s}'=\mathbf{0}}^{|\mathcal{A}|^{n-1}} \sqrt{\lambda_{\mathbf{s}}\lambda_{\mathbf{s}'}} |e_{\mathbf{s}} f_{\mathbf{s}}\rangle\langle e_{\mathbf{s}'} f_{\mathbf{s}'}| \otimes U_{\mathbf{s}} \widetilde{\rho}_{A_S B_S} U_{\mathbf{s}'}^{\dagger}. \tag{17}$$

Here

$$\mathbf{s} = (\mathbf{s}[1], \mathbf{s}[2], \ldots, \mathbf{s}[n]) \in \mathcal{A}^n, \tag{18}$$

$$U_{\mathbf{s}} = U_{\mathbf{s}[1]} \otimes U_{\mathbf{s}[2]} \otimes \cdots \otimes U_{\mathbf{s}[n]} \tag{19}$$

$$\widetilde{\rho}_{A_S B_S} = \rho_{A_S B_S}^{\otimes n}. \tag{20}$$

Alice creates a pure state $|\phi\rangle_{A''}^{\otimes n}$ with the same amplitudes as the state $|\psi\rangle^{\otimes n}$ and compresses it, so that it is stored in $\lceil n(S_{A_K}(\psi) + \eta)\rceil$ qubits. She then uses the controlled-XOR operation from A'' to A_K, measures A_K in the computational basis, and sends the result x to Bob. This operation is a coherently applied counterpart of one-time-pad encryption, an analog of quantum teleportation [14]. This part of the protocol is similar to what is used in [59], which is only the first part of our dilution protocol here.

The next part of the protocol proceeds as follows. After Bob corrects his key part B_K, shifting his system by x, the resulting state (after decompression on both sides) has the correct amplitudes, but the form of the shield systems is not yet correct. Up to a normalization factor, the overall state is as follows

$$\sum_{\mathbf{s},\mathbf{s}'} \sqrt{\lambda_{\mathbf{s}}\lambda_{\mathbf{s}'}} |\mathbf{s}\mathbf{s}\rangle\langle \mathbf{s}'\mathbf{s}'| \otimes U_{\beta_x(\mathbf{s})} \rho_{A_S B_S}^{\otimes n} U_{\beta_x(\mathbf{s}')}. \tag{21}$$

Here $\beta_x(\mathbf{s})$ is a certain automorphism on the so-called δ-typical sequences of length n, to which $\mathbf{s}$ also belongs (for details, see Section 7.4). The challenging task is then to (in a sense) invert β_x. To achieve this task, we design two algorithms: Permutation Algorithm (PA) followed by Phase Error Correction (PEC) and Inverting PA (IPA). The idea of PA is to permute the shield systems $A_S B_S$ in order to invert β_x in most positions, using the key and the system holding the pattern of errors as a control. This results in a string $\mathbf{s}_{\mathrm{cor}}$, which agrees with $\mathbf{s}$ in most positions. The remaining small amount of systems, for which there is still a phase error, i.e., $\mathbf{s}_{\mathrm{cor}}[i] \neq \mathbf{s}[i]$, are teleported to one side in the PEC procedure, corrected locally, and teleported back. This step consumes a nonzero but negligible amount of maximally entangled states. Finally, the Inverting PA procedure ensures that PA and PEC should not leave systems containing valuable information to Eve upon tracing them out. For details of the proof, see Sections 7.1–7.3.

3 Summary of contents

We introduce all the necessary preliminaries in Section 4. In Section 5, we prove that the regularised relative entropy of entanglement is a lower bound on the key cost, which enables showing an example of the irreversibility of privacy creation-distillation process. In Section 6, we define the key of formation and prove some of its basic properties, including monotonicity under certain elementary LOCC operations. Section 7 contains a construction of a Privacy Dilution protocol, which dilutes twisted maximally entangled states to generalized private states. The rate at which privacy dilution can be performed using this protocol is given in the main theorem of this section. In Section 8, the Privacy Dilution protocol is used to prove that the regularized key of formation is an upper bound on the key cost. Section 9 contains proofs of several lemmas, including properties of generalized private states. The main theorem of this section states that the key of formation, the regularized key of formation, the key cost, the distillable key, and the relative and regularized relative entropy of entanglement are equal for strictly irreducible generalized private states. Section 10 shows the single-shot yield-cost relation, i.e., that the single-shot key cost is an upper bound (up to a factor) on the distillable key. Section 11 contains the definition of the key cost of a quantum device. It also introduces the device-independent key cost of a private state. The last section (Section 12) contains the proof of subadditivity of the key of formation.

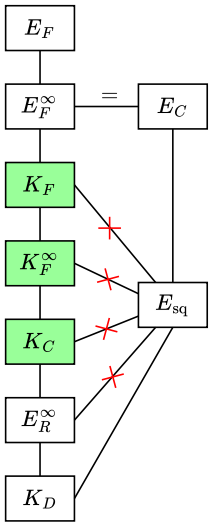


Figure 1: The diagram depicts relations between well known entanglement measures and the quantities K_C, K_F, and K_F^∞ introduced here (green boxes). A connection between two quantities corresponds to the fact that the higher one is no smaller that the lower one. Red cross means that connected quantities are incomparable. Note however, that the above diagram reduces for generalized private states, as quantities $K_F, K_F^\infty, K_C, E_R^\infty, K_D$ become equal for such states (see Theorem 5).

4 Preliminaries

Let us begin by providing some background on quantum information here and refer the reader to [60, 61] for more details. The dimension of any quantum system A is defined as the dimension of its Hilbert space $\mathcal{H}_A$. Let $|A| \coloneqq \dim(\mathcal{H}_A)$. The identity operator acting on the Hilbert space $\mathcal{H}_A$ is denoted as $\mathbb{1}_A$. The Hilbert space of a bipartite quantum system AB is $\mathcal{H}_{AB} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B$, and its dimension is $|AB| = |A||B|$. Let $\mathcal{B}_+(\mathcal{H}_A)$ denote the set of all positive semi-definite operators acting on $\mathcal{H}_A$. Quantum states are represented by density operators $\rho_A : \mathcal{H}_A \to \mathcal{H}_A$ and they satisfy following three criteria: (i) $\rho = \rho^\dagger$, (ii) $\rho \geq 0$, and (iii) $\mathrm{Tr}[\rho] = 1$. A pure state is a density operator of rank one, and a state that is not pure is called a mixed state. With slight abuse of nomenclature, we refer to both the pure state $\psi_A = |\psi\rangle\langle\psi|_A$ and its corresponding state vector $|\psi\rangle_A$, where $|\psi\rangle_A \in \mathcal{H}_A$, as pure states. Let $\mathcal{D}(\mathcal{H}_A)$ denote the set of all quantum states of the system A. Let $\mathrm{SEP}(A:B)$ denote the set of all separable states of a bipartite quantum system AB, i.e., $\rho_{AB} \in \mathrm{SEP}(A:B)$ if and only if we can express ρ_{AB} as

$$\rho_{AB} = \sum_x p_x \sigma_A^x \otimes \omega_B^x, \tag{22}$$

where $\sum_x p_x = 1$ and for each x we have $0 \leq p_x \leq 1$, $\sigma_A^x \in \mathcal{D}(\mathcal{H}_A)$, and $\omega_B^x \in \mathcal{D}(\mathcal{H}_B)$. A bipartite quantum state ρ_{AB} is called entangled if it is not separable, i.e., ρ_{AB} is entangled if $\rho_{AB} \notin \mathrm{SEP}(A:B)$.

A quantum channel $\mathcal{N}_{A\to B} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ is a completely positive, trace-preserving map. We use $\mathbb{1}_{A\to B} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ to denote an identity channel when $|A| = |B|$. The Choi state of a quantum channel $\mathcal{N}_{A\to B}$ is the output state $(\mathbb{1}_R \otimes \mathcal{N}_{A\to B})(\Phi_{RA}^+)$ of the channel $\mathbb{1} \otimes \mathcal{N}$ when the input state is a maximally entangled state

$$\Phi_{RA}^+ \coloneqq \frac{1}{d} \sum_{i,j=0}^{d-1} |ii\rangle\langle jj|_{RA}\,, \tag{23}$$

where $d = \min\{|R|, |A|\}$ is the Schmidt rank of Φ_{RA}^+ and $\{|i\rangle\}_i$ forms a set of orthonormal kets (vectors). An isometry is a linear map $U : \mathcal{H}_A \to \mathcal{H}_B$ such that $U^\dagger U = \mathbb{1}_A$ and $UU^\dagger = \Pi_B$, where Π_B is a projection on the support of $\mathcal{H}_B$. A positive-operator valued measure (POVM) is a set $\{\Lambda^x\}_x$ of positive semi-definite operators, i.e., $\Lambda^x \geq 0$ for each x, such that $\sum_x \Lambda^x = \mathbb{1}$. A quantum instrument Δ is a collection $\{\mathcal{M}^x\}_x$ of completely positive, trace-nonincreasing maps such that the sum map $\sum_x \mathcal{M}^x$ is a quantum channel

$$\Delta_{A'\to AX}(\cdot) = \sum_x \mathcal{M}_{A'\to A}^x(\cdot) \otimes |x\rangle\langle x|_X\,, \tag{24}$$

where quantum system X represents a classical register, because $\{|x\rangle\langle x|\}_x$ forms a set of orthogonal pure states, which are perfectly discriminable.

The fidelity of $\rho_A, \sigma_A \in \mathcal{B}_+(\mathcal{H}_A)$ is defined as [62]

$$F(\rho, \sigma) \coloneqq \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2, \tag{25}$$

where $\|\zeta\|_1 \coloneqq \mathrm{Tr}\sqrt{\zeta^\dagger\zeta}$ is the trace norm for an arbitrary bounded operator ζ.

An LOCC channel $\mathcal{L}_{A'B'\to AB}$ is a bipartite quantum channel that can be expressed in the separable form as $\sum_x \mathcal{E}_{A'\to A}^x \otimes \mathcal{F}_{B'\to B}^x$ where each $\mathcal{E}^x$ and $\mathcal{F}^x$ are completely positive, trace-nonincreasing maps such that the sum map $\mathcal{L}$ is a quantum channel [63, 61]. Here pairs A', A and B', B are held by two spatially separated parties, say Alice and Bob. However, note that not every separable channel is an LOCC channel [64]. Using only an LOCC channel, Alice and Bob can only create separable states. In what follows, LOCC will denote also the set of all local (quantum) operations and classical communication (LOCC) channels.

Let $\mathcal{B}$ be the set of all bipartite quantum states ρ_{AB} for all $|A|, |B| \geq 2$. A function $\mathbf{E} : \mathcal{B} \to \mathbb{R}$ is called an *entanglement monotone* if it is monotonic (nonincreasing) under the action of an arbitrary LOCC channel, i.e., $\mathbf{E}(\rho_{A'B'}) \geq \mathbf{E}(\mathcal{L}_{A'B'\to AB}(\rho_{A'B'}))$ where pairs of quantum systems A', A and B', B are held at spatially separated labs, say Alice and Bob, respectively. A direct consequence of this definition is that entanglement monotones are

1. Invariant under the action of local isometries,

$$\mathbf{E}(\rho_{A'B'}) = \mathbf{E}((U \otimes V)\rho_{A'B'}(U^\dagger \otimes V^\dagger)), \tag{26}$$

for all local isometries $U_{A'\to AE}$ and $V_{B'\to BF}$, and

2. Invariant under appending of quantum states via local operations,

$$\mathbf{E}(\rho_{AB}) = \mathbf{E}(\sigma_{A'} \otimes \rho_{AB} \otimes \omega_{B'}), \tag{27}$$

for all quantum states $\sigma_{A'}$ and $\omega_{B'}$ appended locally.

We also need fundamental results from classical information theory (see, e.g., [65, 66]). Consider a random variable X with probability distribution $\{p_X(x)\}_{x\in\mathcal{X}}$, where $\mathcal{X}$ is a finite alphabet. Let x^n be a sequence drawn from $\mathcal{X}$. The empirical probability mass function of x^n, also called its type, is given by

$$\pi(x|x^n) \coloneqq \frac{|\{i : x_i = x\}|}{n} \text{ for } x \in \mathcal{X}. \tag{28}$$

For $\delta \in (0, 1)$, we define the strongly δ-typical set as

$$T_n^\delta(X) \coloneqq \{x^n : |\pi(x|x^n) - p(x)| \leq \delta p(x)\ \forall x \in \mathcal{X}\}. \tag{29}$$

The size $\left|T_n^\delta(X)\right|$ of the strongly δ-typical set is approximately $2^{nH(X)}$, where

$$H(X) \coloneqq -\sum_{x\in\mathcal{X}} p_X(x) \log_2 p_X(x) \tag{30}$$

is the Shannon entropy of X [67]; to be more precise, for all sufficiently large n

$$(1-\delta)2^{n[H(X)-\eta(\delta)]} \leq \left|T_n^\delta(X)\right| \leq 2^{n[H(X)+\eta(\delta)]}, \quad (31)$$

where $\eta(\delta) \coloneqq \delta H(X)$, so that $\eta(\delta) \to 0$ as $\delta \to 0$. The probability that a randomly selected sequence x^n belongs to the strongly δ-typical set $T_n^\delta(X)$ converges to one in the asymptotic limit $n \to \infty$; i.e.,

$$\lim_{n\to\infty} \Pr(X^n \in T_n^\delta(X)) = 1. \quad (32)$$

We will often use shorthand notations or suppress system labels and identity operations for simplicity, whenever the meaning is clear from the context.

4.1 Entropies and generalized divergence

The quantum entropy, also called von Neumann entropy, of a quantum system A in a state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ is defined as

$$S(A)_\rho \coloneqq S(\rho_A) = -\operatorname{Tr}[\rho_A \log_2 \rho_A]. \quad (33)$$

For the sake of readability, we may use the notation $S_A(\rho)$ instead of the above. It is known that the quantum entropy satisfies the inequalities $0 \leq S(\rho_A) \leq \log_2 |A|$. The conditional quantum entropy, also called the conditional von Neumann entropy, $S(A|B)_\rho$ of a bipartite quantum state ρ_{AB} conditioned on quantum system B is given by

$$S(A|B)_\rho \coloneqq S(AB)_\rho - S(B)_\rho. \quad (34)$$

It is known that the conditional quantum entropy can be negative for an entangled state ρ_{AB} [68].

The quantum mutual information $I(A;B)_\rho$ of a quantum state ρ_{AB} is defined as

$$I(A;B)_\rho \coloneqq S(A)_\rho + S(B)_\rho - S(AB)_\rho. \quad (35)$$

The quantum conditional mutual information $I(A;B|C)_\rho$ is the mutual information between A and B conditioned on C

$$I(A;B|C)_\rho \coloneqq S(A|C)_\rho + S(B|C)_\rho - S(AB|C)_\rho. \quad (36)$$

Both the quantities $I(A;B)_\rho$ and $I(A;B|C)_\sigma$ for all quantum states ρ_{AB} and σ_{ABC}, respectively, are always non-negative [69]. The squashed entanglement $E_{\mathrm{sq}}(\rho_{AB})$ of a bipartite quantum state ρ_{AB} is defined as [56]

$$E_{\mathrm{sq}}(\rho_{AB}) \coloneqq \inf_{\substack{\rho_{ABE}:\\ \operatorname{Tr}_E[\rho_{ABE}]=\rho_{AB}}} \frac{1}{2} I(A;B|E)_\rho, \quad (37)$$

where the infimum is taken over every state ρ_{ABE} that is an extension of ρ_{AB}.

A function $\mathbf{D} : \mathcal{D}(\mathcal{H}_A) \times \mathcal{D}(\mathcal{H}_A) \to \mathbb{R}$ is called a generalized divergence [70] if it satisfies the data-processing inequality for all quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$ and an arbitrary quantum channel $\mathcal{N}_{A\to B}$

$$\mathbf{D}(\rho\|\sigma) \geq \mathbf{D}(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)). \quad (38)$$

It directly follows from the above definition that any generalized divergence remains invariant under the following two operations [71]: the action of an isometry U and appending of quantum states, i.e.,

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(U\rho U^\dagger\|U\sigma U^\dagger), \quad (39)$$
$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(\rho\otimes\omega\|\sigma\otimes\omega), \quad (40)$$

for an arbitrary isometric operator U and an arbitrary quantum state ω. Examples include the quantum relative entropy [72], defined for quantum states ρ, σ as

$$D(\rho\|\sigma) \coloneqq \operatorname{Tr}[\rho(\log_2\rho - \log_2\sigma)], \quad (41)$$

when $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma)$ and otherwise $D(\rho\|\sigma) \coloneqq +\infty$. Another example is the sandwiched Rényi relative entropy [73, 71], which is denoted as $\widetilde{D}_\alpha(\rho\|\sigma)$ and defined for states ρ, σ, and $\alpha \in (0,1)\cup(1,\infty)$ as

$$\widetilde{D}_\alpha(\rho\|\sigma) \coloneqq \frac{1}{\alpha-1}\log_2 \operatorname{Tr}\left[\left(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right)^\alpha\right], \quad (42)$$

but it is set to $+\infty$ for $\alpha \in (1,\infty)$ if $\operatorname{supp}(\rho) \nsubseteq \operatorname{supp}(\sigma)$. The sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ of two states is nonincreasing under the action of a quantum channel $\mathcal{N}$ for all $\alpha \in [\frac{1}{2},1)\cup(1,\infty)$ [74, 75], i.e.,

$$\widetilde{D}_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)). \quad (43)$$

It is also monotone in α [73]; that is,

$$\widetilde{D}_\alpha(\rho\|\sigma) \geq \widetilde{D}_\beta(\rho\|\sigma) \quad (44)$$

for all $\alpha, \beta \in (0,1)\cup(1,\infty)$ such that $\alpha \geq \beta$.

In the limit $\alpha \to 1$ the sandwiched Rényi relative entropy converges to the quantum relative entropy, and in the limit $\alpha \to \infty$, it converges to the max-relative entropy [73], which is defined as [76, 77]

$$D_{\max}(\rho\|\sigma) \coloneqq \inf\{\lambda \in \mathbb{R} : \ \rho \leq 2^\lambda\sigma\}, \quad (45)$$

and if $\operatorname{supp}(\rho) \nsubseteq \operatorname{supp}(\sigma)$ then $D_{\max}(\rho\|\sigma) \coloneqq +\infty$. It is also known that $I(A;B)_\rho = D(\rho_{AB}\|\rho_A\otimes\rho_B)$, where ρ_A and ρ_B are reduced states of $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$.

Another generalized divergence is the ε-hypothesis-testing divergence [78, 79], defined as

$$D_h^\varepsilon(\rho\|\sigma) \coloneqq -\log_2 \inf_{\Lambda:0\leq\Lambda\leq\mathbb{1}}\{\operatorname{Tr}[\Lambda\sigma] : \ \operatorname{Tr}[\Lambda\rho] \geq 1-\varepsilon\}, \quad (46)$$

for $\varepsilon \in [0,1]$ and density operators ρ and σ. The ε-hypothesis testing relative entropy for $\varepsilon = 0$ reduces to the min-relative entropy, i.e.,

$$D_{\min}(\rho\|\sigma) \coloneqq D_h^{\varepsilon=0}(\rho\|\sigma) = -\log_2 \operatorname{Tr}[\Pi_\rho\sigma], \quad (47)$$

where Π_ρ denotes the projection onto the support of ρ (see [80, Appendix A-3] for a proof of this equality).

Some other well-known generalized divergences include the trace distance $\|\rho-\sigma\|_1$ and the negative of fidelity $-F(\rho,\sigma)$.

4.2 Private states and generalized private states

A tripartite key state γ_{ABE} contains $\log_2 d_k$ bits of secret key, shared between A and B, against an eavesdropper possessing E, if there exists a state σ_E such that

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{d_k} \sum_{i=0}^{d_k-1} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E \quad (48)$$

for a projective measurement channel $\mathcal{M}(\cdot) = \sum_i |i\rangle\langle i| (\cdot) |i\rangle\langle i|$, where $\{|i\rangle\}_{i=0}^{d_k-1}$ forms an orthonormal basis. The quantum systems A and B are maximally classically correlated, and the key value is uniformly random and independent of E.

A (perfect) bipartite private state $\gamma(\Phi^+)$ containing at least $\log_2 d_k$ bits of secret key has the following form [17, 16, 34]

$$\gamma_{A_K A_S B_K B_S}(\Phi^+) = \tau(\Phi^+_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger, \quad (49)$$

where $\Phi^+_{A_K B_K}$ is a maximally entangled state of Schmidt rank d_k and the state $\rho_{A_S B_S}$ of the shield systems gets twisted by $\tau_{A_K B_K A_S B_S}$, which is a controlled-unitary operation given as

$$\tau_{A_K B_K A_S B_S} = \sum_{i=0}^{d_k-1} |ii\rangle\langle ii|_{A_K B_K} \otimes U^i_{A_S B_S}, \quad (50)$$

where $U^i_{A_S B_S}$ is an arbitrary unitary operator for each i. It is understood that A_K, A_S are held by Alice and B_S, B_S are held by Bob, both being safe against a quantum adversary.

A special class of private states for which $K_D(\gamma(\Phi^+)) = \log_2 d_k$ (i.e., there is no more key in this state than that contained in its key systems) are called irreducible private states. This class has been characterized in [51] in the following way: if there are no entangled but key undistillable states, all irreducible private states are strictly irreducible (SIR) [34, 52], that is, taking the form

$$\gamma_{d_k,d_s}(\Phi_+) \coloneqq \frac{1}{d_k} \sum_{i,j=0}^{d_k-1} |ii\rangle\langle jj|_{\text{key}} \otimes U_i \rho_{\text{shield}} U_j^\dagger, \quad (51)$$

where $U_i \rho_{\text{shield}} U_i^\dagger$ is a separable state for each i and ρ_{shield} is an arbitrary state defined over the Hilbert space of dimension $d_s \times d_s$.

Private states $\gamma(\Phi^+)$ can be naturally generalized to a class of states in which $\Phi^+_{A_K B_K}$ is replaced with an arbitrary pure bipartite state $\psi_{A_S B_S}$, i.e.,

$$\gamma_{A_K A_S B_K B_S}(\psi) = \tau(\psi_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger, \quad (52)$$

where $\tau_{A_K A_S B_K B_S}$ is a controlled-unitary operation (twisting unitary) defined earlier that twists the state $\psi_{A_K B_K}$ of the key system with the state $\rho_{A_S B_S}$ of the shield system. These states $\gamma(\psi)$ have been called Schmidt-twisted pure states in [33, 34]. They are, however, pure if and only if $\rho_{A_S B_S}$ is pure; else, they are mixed. Therefore, we will refer to them here as *generalized private states*. These states are of the following form

$$\gamma_{A_K A_S B_K B_S}(\psi) \coloneqq \widetilde{\tau}(\psi_{A_K B_K} \otimes \rho_{A_S B_S})\widetilde{\tau}^\dagger, \quad (53)$$

where

$$\psi_{A_K B_K} = |\psi\rangle\langle\psi|_{A_K B_K}, \quad (54)$$

$$|\psi\rangle_{A_K B_K} = \sum_{i=0}^{d_k-1} \sqrt{\mu_i} |e_i f_i\rangle_{A_K B_K}, \quad (55)$$

is a pure bipartite state of Schmidt-rank d_k and a twisting unitary

$$\widetilde{\tau}_{A_K A_S B_K B_S} = \sum_{i=0}^{d_k-1} |e_i f_i\rangle\langle e_i f_i|_{A_K B_K} \otimes U^i_{A_S B_S} \quad (56)$$

has control in the orthonormal bases $\{|e_i\rangle\}_i$ and $\{|f_i\rangle\}_i$, while the state ρ is arbitrary. In [33], a class of generalized private states $\gamma(\psi)$ called *irreducible generalized private states* (called there Schmidt-twisted pure states) were introduced. We relax this class here, by allowing all states that are locally unitarily equivalent to the generalized private states to fall into the same class of generalized private states.

Definition 2. *A generalized private state $\gamma(\psi)_{AB}$ is called irreducible if there exists a unitary transformation*

$$W_{AB} \coloneqq W_{A \to A_K A_S} \otimes W_{B \to B_K B_S}, \quad (57)$$

such that the following two conditions are satisfied:

$$W_{AB}\gamma(\psi)_{AB}W^\dagger_{AB} = \sum_{i,j} \sqrt{\mu_i \mu_j} |e_i f_i\rangle\langle e_j f_j|_{A_K B_K} \otimes U_i \rho_{A_S B_S} U_j^\dagger, \quad (58)$$

and

$$S_{A_K}(W_{AB}\gamma(\psi)W^\dagger_{AB}) = K_D(\gamma(\psi)). \quad (59)$$

We further define strictly irreducible generalized private states.

Definition 3. *The generalized private state, equivalent up to local unitary transformations to a state*

$$\gamma_{A_K B_K A_S B_S}(\psi) = \sum_{i,j} \sqrt{\mu_i \mu_j} |e_i f_i\rangle\langle e_j f_j|_{A_K B_K} \otimes U_i \rho_{A_S B_S} U_j^\dagger \quad (60)$$

is called strictly irreducible if $\rho_i = U_i \rho_{A_S B_S} U_i^\dagger \in \text{SEP}(A_S : B_S)$ for each i. We denote the set of all strictly irreducible generalized private states as GSIR.

5 Irreversibility of privacy creation and distillation

Before we state the main result of this section, we introduce our definition of the asymptotic key cost $K_C(\rho)$ and one-shot key cost $K_C^\varepsilon(\rho)$ of a bipartite quantum state ρ_{AB}.

Definition 4. *The asymptotic key cost $K_C(\rho)$ and one-shot key cost $K_C^\varepsilon(\rho)$ of a state ρ_{AB} are defined as*

$$K_C(\rho) \coloneqq \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}), \tag{61}$$

$$K_C^\varepsilon(\rho) \coloneqq \inf_{\substack{\mathcal{L}\in\mathrm{LOCC},\\ \gamma_{d_k,d_s}\in\mathrm{SIR}}} \left\{ \begin{array}{c} \log_2 d_k : \\ \frac{1}{2}\left\|\mathcal{L}(\gamma_{d_k,d_s}) - \rho\right\|_1 \leq \varepsilon \end{array} \right\}, \tag{62}$$

where the infimum is taken over every LOCC channel $\mathcal{L}$ and every strictly irreducible private state γ_{d_k,d_s} with arbitrarily large, finite shield dimension $d_s \geq 1$.

To exhibit irreversibility in the privacy distillation-creation process, we use standard techniques to prove that the regularized relative entropy of entanglement bounds the key cost from below.

Theorem 2. *For every bipartite state ρ_{AB}, the following bound holds*

$$K_C(\rho) \geq E_R^\infty(\rho), \tag{63}$$

where $E_R^\infty(\rho) \coloneqq \lim_{n\to\infty} \frac{1}{n} E_R(\rho^{\otimes n})$ and $E_R(\rho) \coloneqq \inf_{\sigma\in\mathrm{SEP}} D(\rho\|\sigma)$.

Proof. We follow here some standard arguments used in quantum resource theories. Let us begin by giving the basic idea of the proof. We first note that the relative entropy of entanglement of an irreducible private state γ_k is bounded from above by k, i.e., $E_R(\gamma_k) \leq k$ (see Theorem 2 in [51]). We then note that under the action of an LOCC channel $\mathcal{L}$ that approximately generates the target state $\rho^{\otimes n}$, the relative entropy does not increase, and for a separable state σ, $\mathcal{L}(\sigma) = \sigma' \in \mathrm{SEP}$. Furthermore, asymptotic continuity of the relative entropy of entanglement corresponds to the following inequality

$$\left|E_R(\mathcal{L}(\gamma_k)) - E_R(\rho^{\otimes n})\right| \leq f(\varepsilon, d, n), \tag{64}$$

where

$$f(\varepsilon, d, n) \coloneqq \varepsilon \log_2 d^n + g(\varepsilon), \tag{65}$$

$$g(\varepsilon) \coloneqq (\varepsilon+1)\log_2(\varepsilon+1) - \varepsilon\log_2\varepsilon. \tag{66}$$

Regularization of the considered quantity by n finishes the proof.

We state these steps formally now. Consider that

$$\log_2 d_k \geq E_R(\gamma_{d_k}) \tag{67}$$

$$\geq E_R(\mathcal{L}(\gamma_{d_k})) \tag{68}$$

$$\geq E_R(\rho^{\otimes n}) - f(\varepsilon, d, n), \tag{69}$$

where we have applied [51, Theorem 2] for the first inequality, LOCC monotonicity of the relative entropy of entanglement for the second inequality, and asymptotic continuity of the relative entropy of entanglement [81, Corollary 8] for the third. Since the above inequalities hold for each $\mathcal{L} \in \mathrm{LOCC}$ and $\gamma_{d_k} \in \mathrm{SIR}$ such that $\frac{1}{2}\left\|\mathcal{L}(\gamma_{d_k}) - \rho^{\otimes n}\right\|_1 \leq \varepsilon$ and K_C^ε is defined to be the infimum of $\log_2 d_k$ over all such $\mathcal{L}$ and γ_{d_k}, then we conclude that

$$K_C^\varepsilon(\rho^{\otimes n}) \geq E_R(\rho^{\otimes n}) - f(\varepsilon, d, n). \tag{70}$$

After dividing by n and applying the definition of key cost and the regularized relative entropy of entanglement, we conclude that

$$K_C(\rho) = \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}) \geq E_R^\infty(\rho). \tag{71}$$

This concludes the proof. □

As an important consequence, it follows that the process of privacy creation is irreversible. Indeed in [48] (see also [49]) it was shown that there are states $\widehat{\rho}$ satisfying $E_{\mathrm{sq}} \ll E_R^\infty$, where E_{sq} is the squashed entanglement measure defined in (37). We then have

$$K_D(\widehat{\rho}) \leq E_{\mathrm{sq}}(\widehat{\rho}) \ll E_R^\infty(\widehat{\rho}) \leq K_C(\widehat{\rho}), \tag{72}$$

which implies that $K_D(\widehat{\rho}) \ll K_C(\widehat{\rho})$. The above inequality is the first example of irreversibility in the case of privacy.

Remark 1. *We note here that a simplified version of the definition of K_C is to consider only those states that take the form of the so-called Bell private states [52] whenever they are strictly irreducible. A Bell private state takes the form*

$$\sum_i p_i \left|\Phi_i\right\rangle\!\left\langle\Phi_i\right|_{A_K B_K} \otimes \rho^{(i)}_{A_S B_S} \tag{73}$$

where $\rho^{(i)}_{A_S B_S}$ are arbitrary, yet mutually orthogonal states on $A_S B_S$, and the states $|\Phi_i\rangle\langle\Phi_i|$ are Bell states of local dimension d_k generated from $|\Phi\rangle = \frac{1}{\sqrt{d_k}}\sum_{i=0}^{d_k-1}|ii\rangle$ by the local rotations

$$X^m Z^j = \left(\sum_{l'=0}^{d_k-1} |m\oplus l'\rangle\!\langle l'|\right)\left(\sum_{l=0}^{d_k-1} e^{2\pi i j l/d_k}|l\rangle\!\langle l|\right). \tag{74}$$

This simplification comes from the fact (see [52, Lemma 1]) that a one-way LOCC channel can reversibly transform any private state to a Bell private state.

Remark 2. *The existence of entangled but zero distillable key states would result in a redefinition of the key cost to a novel quantity, say K'_C, which is smaller than our key cost K_C, since it would be based on taking the infimum over a larger class of private states, those with conditional states that are not necessarily separable.*

6 Key of formation

Here, we generalize the notion of entanglement of formation to the case of the key of formation. We will need a notion corresponding to a pure state in the domain of private states. For this purpose, we consider irreducible generalized private states $\gamma_{A_K A_S B_K B_S}(\psi)$ (see Eq. (53)). We denote such a state by $\gamma(\psi)$, where ψ is the pure state under consideration.

We note that subsystem $A_K B_K$, i.e., the key part of a private state, is not the same for different private states as they can differ by some product $W_{A_K A_S} \otimes W_{B_K B_S}$ of local unitary transformations, and the key part of one private state can be of a different dimension than the one for the other private state. For this reason, by the *key* A_K (similarly B_K), we will mean the one from which after a von Neumann measurement in some product basis $\{|e_i\rangle\}_i$ ($\{|f_i\rangle\}_i$) the whole key of the generalized private state given in Eq. (53) is obtained. The key of formation is then defined as follows:

Definition 5. *The key of formation of a bipartite state ρ is defined as*

$$K_F(\rho) \coloneqq \inf_{\left\{ \begin{array}{c} \sum_{k=1}^{K} p_k \gamma(\psi_k) = \rho, \\ \gamma(\psi_k) \in \mathrm{GSIR} \end{array} \right\}} \sum_{k=1}^{K} p_k S_{A_K}[\gamma(\psi_k)], \tag{75}$$

where $\gamma(\psi_k)$ is a strictly irreducible generalized private state and $S(\cdot)$ denotes the von Neumann entropy. Additionally, the infimum is taken over finite, yet arbitrarily large K.

The definition provided above directly parallels the definition of the entanglement of formation, but it is applicable to the private key resource theory developed here. Intuitively, K_F quantifies the minimal average amount of (i) directly accessible, (ii) ideally secure correlations, where the minimum runs over the set of states having this property. Here, by "directly accessible," we mean the correlations that can be generated by two local, in general incomplete, von Neumann measurements. Furthermore, we consider ideally secure correlations, i.e., decoupled from the purifying system of a purification of ρ held by the eavesdropper, yet possibly biased. They generalize notion of secret key, which has the outcomes of the mentioned von Neumann measurements necessarily equally likely. Generalized private states satisfy the above two properties (i)-(ii); thus, they are a natural choice in the definition. However, we need to narrow this class of states to irreducible ones only, since, without this requirement, the proposed definition would be trivially equal to zero. Indeed, all the secret correlations could be considered as a part of the shield subsystem, which is not taken into account in the definition. Finally, we decided to consider only strictly irreducible generalized private states because this class is precisely characterized in [33].

Let us note that the defined key of formation has an operational interpretation. Namely, it quantifies the minimal average amount of ideally secure, directly accessible correlations required to generate a state by sampling from its ensemble.

As a first step, we show that in the above definition, the infimum can be taken over ensembles with at most $(|A||B|)^2+1$ elements. This technical result is crucial in proving the main result in Theorem 4.

Lemma 1. *For a state ρ_{AB}, the infimum in Definition 5 of $K_F(\rho_{AB})$ can be taken on ensembles with a number of elements at most $(|A| \times |B|)^2 + 1$.*

Proof. We closely follow the idea of Proposition 3 in [55]. Consider a decomposition of ρ_{AB} into a finite number of states, as $\rho_{AB} = \sum_{k=1}^{K} p_k \gamma(\psi_k)$, with $K > D+1$ and $D \coloneqq (|A| \times |B|)^2$. We aim to find a decomposition $\rho_{AB} = \sum_{k=1}^{D+1} q_k \widetilde{\gamma}(\psi_k)$, where $\{q_k\}_k$ is a probability distribution. One can construct a polytope $C(S)$, which is the convex hull of the set

$$S \coloneqq \{(\gamma(\psi_k), S_{A_K}(\gamma(\psi_k))\}_{k=1}^{K}. \tag{76}$$

The set $C(S)$ is convex by definition and a proper subset of $\mathbb{R}^D$. This holds because private states are spanned by Hermitian operators and have unit trace, and one more parameter corresponds to the value of $S_{A_K}(\gamma(\psi_k))$. Now, by definition

$$y \coloneqq \left(\sum_{k=1}^{K} p_k \gamma(\psi_k), \sum_{k=1}^{K} p_k S_{A_K}(\gamma(\psi_k)) \right) \in C(S). \tag{77}$$

It is then important to note that the extremal points of $C(S)$ are contained within the set S. Hence by Caratheodory's theorem, there exist at most $D+1$ extremal points $\{(\widetilde{\gamma}(\psi_j), S_{A_K}(\widetilde{\gamma}(\psi_j))\}_{j=1}^{D} \subseteq S$ in $C(S)$ such that $y = \sum_{j=1}^{D+1} q_j (\widetilde{\gamma}(\psi_j), S_{A_K}(\widetilde{\gamma}_j))$, which implies the statement of the lemma. □

Note that, while we show above that the infimum in the definition of K_F can be taken over ensembles of bounded size, it remains open to determine if the infimum is attained. In what follows, we will use that K_F, constructed by the convex-roof method, is a convex function. We prove it below for the sake of the completeness of the presentation.

Lemma 2. *K_F is a convex function.*

Proof. Let $\sum_k^K p_k \rho_k$ be a convex mixture of quantum states and let $\eta_1, \ldots, \eta_K > 0$. Since K_F is by the definition an infimum over ensembles into generalized strictly irreducible private states, then for each ρ_k there exist an ensemble $\{(q_{kl}, \gamma_{kl})\}_l$ such that $\sum_l q_{kl}\gamma_{kl} = \rho_k$ and $\sum_l q_{kl} S_{A_K}[\gamma_{kl}] \leq K_F(\rho_k) + \eta_k$. Now observe that $\sum_{k,l} p_k q_{kl} \gamma_{kl}$ is a valid decomposition into generalized strictly irreducible private states

of the state $\sum_k^K p_k\rho_k$. Again, since K_F is an infimum we obtain

$$K_F\left(\sum_k p_k\rho_k\right) \leq \sum_{k,l} p_k q_{kl} S_{A_K}[\gamma_{kl}]$$
$$\leq \sum_k p_k(K_F(\rho_k)+\eta_k) = \sum_k p_k K_F(\rho_k) + \sum_k p_k\eta_k. \tag{78}$$

Since it holds true for every $\eta_1,\ldots,\eta_K > 0$, it follows that

$$K_F\left(\sum_k p_k\rho_k\right) \leq \sum_k p_k K_F(\rho_k), \tag{79}$$

concluding the proof. □

6.1 Monotonicity of the key of formation under some elementary operations

In this section, we prove that K_F is monotonic under certain LOCC operations. We note first that it is easy to observe that the key of formation does not increase after local measurements on pure states.

Observation 1. *K_F does not increase on pure states under LOCC.*

Proof. We note that, for a pure state, $K_F = K_D = E_F$ by definition. Since E_F is an LOCC monotone, we have

$$E_F(\psi_{AB}) \geq \sum_k p_k E_F(\sigma_{AB}^k), \tag{80}$$

where ψ_{AB} is a pure state, k is an outcome of the LOCC operation, p_k is the probability of outcome k, and σ_{AB}^k is a state given that outcome k was obtained. Combining the above statements, we obtain

$$K_F(\psi_{AB}) = E_F(\psi_{AB}) \tag{81}$$
$$\geq \sum_k p_k E_F(\sigma_{AB}^k) \tag{82}$$
$$\geq \sum_k p_k K_F(\sigma_{AB}^k). \tag{83}$$

Here the equality comes from the fact that $|\psi\rangle$ is pure; hence it cannot be expressed as a mixture of a non-pure members ensemble such as non-pure generalized private states. The first inequality follows from the monotonicity of E_F under LOCC. The second inequality follows from the definition, i.e., $K_F \leq E_F$ for all states. □

We note, however, that in general, E_F can be much larger than K_F for a private state. To give an example, consider the state provided in [45] and recalled explicitly below

$$\gamma_{2,d_s} = \frac{1}{2}\begin{bmatrix} \sigma & 0 & 0 & \frac{1}{d_s}U^T \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{d_s}U^* & 0 & 0 & \sigma \end{bmatrix}, \tag{84}$$

where

$$U = \sum_{i,j=0}^{d_s-1} u_{ij}|ii\rangle\langle jj|, \tag{85}$$

$$\sigma = \frac{1}{d_s}\sum_{i=0}^{d_s-1} |ii\rangle\langle ii|, \tag{86}$$

with the matrix $\sum_{ij} u_{ij}|i\rangle\langle j|$ a unitary transformation. In [46], it was shown that the above state satisfies

$$E_C(\gamma_{2,d_s}) \geq \frac{\log_2 d_s}{2}, \tag{87}$$

while (as this state is a strictly irreducible private state), from Corollary 1, its asymptotic key cost equals $\log_2 d_k = 1$. Hence, whenever $d_s > 4$, the entanglement cost exceeds the key cost of this state. Now, since $E_F \geq E_F^\infty = E_C$, we have that for the above state $E_F(\gamma_{2,d_s}) > K_F(\gamma_{2,d_s})$ for $d_s \geq 4$. Due to this strict inequality holding, we cannot prove monotonicity of K_F for mixed states by the same approach given in the proof of Observation 1.

We do not provide a general proof of monotonicity under LOCC operations. However, here we present partial results. In [20], it is stated that any convex-roof type measure, to which K_F belongs, is monotonic under LOCC if and only if it is monotonic under local measurements on average. However for the sake of completeness, we show here explicitly the proofs of monotonicity of K_F under all other elementary operations, including adding a local auxiliary state, local partial trace, and random unitary channels.

Observation 2. *If K_F is non-increasing under the action of some operation $\Lambda \in$ LOCC on strictly irreducible generalized private states, then it is non-increasing under the action of Λ.*

Proof. Let ρ be an arbitrary bipartite state. Since K_F is equal to the infimum over ensembles of ρ into strictly irreducible generalized private states, then for all $\eta > 0$, there exists an ensemble $\{(p_i,\gamma_i)\}_i$ such that

$$\eta + K_F(\rho) \geq \sum_i p_i K_F(\gamma_i). \tag{88}$$

Let $\Lambda \in$ LOCC. Suppose that $K_F(\gamma) \geq K_F(\Lambda(\gamma))$ for each strictly irreducible generalized private state γ. Then the following chain of inequalities holds

$$\eta + K_F(\rho) \geq \sum_i p_i K_F(\gamma_i) \tag{89}$$
$$\geq \sum_i p_i K_F(\Lambda(\gamma_i)) \tag{90}$$
$$\geq K_F\left(\sum_i p_i \Lambda(\gamma_i)\right) \tag{91}$$
$$= K_F\left(\Lambda\left(\sum_i p_i\gamma_i\right)\right) \tag{92}$$

$$= K_F(\Lambda(\rho)). \tag{93}$$

For the second inequality, we applied the assumption that K_F does not increase under the action of LOCC on generalized private states. Since the inequality $\eta + K_F(\rho) \geq K_F(\Lambda(\rho))$ holds for all $\eta > 0$, then we conclude that $K_F(\rho) \geq K_F(\Lambda(\rho))$. □

Observation 3. *K_F is invariant under local unitary transformations.*

Proof. Let us fix $\kappa > 0$, and let $\{(p_i, \gamma(\psi_i))\}_i$ be an arbitrary ensemble decomposition of ρ_{AB} in terms of generalized private states, such that

$$\sum_i p_i S_{A_K}(\gamma(\psi_i)) = K_F(\rho) + \kappa. \tag{94}$$

Let us note that Definition 3 for strict irreducibility of each $\gamma(\psi_i)$ implies that for each i there exists a unitary transformation of the form

$$W_{AB}^{(i)} \coloneqq W_{A\to A_K A_S}^{(i)} \otimes W_{B\to B_K B_S}^{(i)}, \tag{95}$$

such that

$$W_{AB}^{(i)} \gamma(\psi_i)_{AB} {W_{AB}^{(i)}}^\dagger = \sum_{l,m} \sqrt{\mu_l^{(i)} \mu_m^{(i)}} |e_l^{(i)} f_l^{(i)}\rangle\langle e_m^{(i)} f_m^{(i)}|_{A_K B_K} \otimes U_l^{(i)} \rho_{A_S B_S}^{(i)} U_m^{(i)\dagger}, \tag{96}$$

where $|\psi_i\rangle = \sum_l \mu_l^{(i)} |e_l^{(i)}\rangle|f_l^{(i)}\rangle$, the operator $U_l^{(i)}$ is a unitary transformation for each l and i, and $\rho_{A_S B_S}^{(i)}$ is a quantum state for each i. Moreover

$$S_{A_k}(W_{AB}^{(i)} \gamma(\psi_i) {W_{AB}^{(i)}}^\dagger) = K_D(\gamma(\psi_i)). \tag{97}$$

We will now show that the ensemble

$$\left\{(p_i, (U_A \otimes U_B)\gamma(\psi_i)(U_A^\dagger \otimes U_B^\dagger))\right\}_i \tag{98}$$

is a valid decomposition of $\rho' \coloneqq (U_A \otimes U_B)\rho_{AB}(U_A^\dagger \otimes U_B^\dagger)$ into strictly irreducible generalized private states, achieving the rate in (94). This will show that $K_F(\rho) \geq K_F(\rho')$. To show this, let us fix i arbitrarily and note that, by linearity, $\left\{(p_i, (U_A \otimes U_B)\gamma(\psi_i)(U_A^\dagger \otimes U_B^\dagger))\right\}_i$ is an ensemble decomposition of ρ'. We define $V_i \coloneqq W_{AB}^{(i)} \circ (U_A^\dagger \otimes U_B^\dagger)$ and observe that

$$V_i \rho' V_i^\dagger = \sum_{l,m} \sqrt{\mu_l^{(i)} \mu_m^{(i)}} |e_l^{(i)} f_l^{(i)}\rangle\langle e_m^{(i)} f_m^{(i)}|_{A_K B_K} \otimes U_l^{(i)} \rho_{A_S B_S}^{(i)} (U_m^{(i)})^\dagger. \tag{99}$$

Moreover

$$S_{A_K}(V_i \rho' V_i^\dagger) = K_D(\gamma(\psi_i)) = K_D((U_A \otimes U_B)\gamma(\psi_i)(U_A^\dagger \otimes U_B^\dagger)) = K_D(\rho'). \tag{100}$$

The first equality follows from (97) and the second from the fact that distillable key is invariant under local unitary transformations. Hence for every κ and ensemble decomposition of ρ achieving $K_F(\rho) + \kappa$, we constructed an ensemble decomposition of ρ' achieving the same value. Since $\kappa > 0$ is arbitrary, we conclude that $K_F(\rho) \geq K_F(\rho')$. Finally, since $\rho = (U_A^\dagger \otimes U_B^\dagger)(\rho')(U_A \otimes U_B)$, repeating the above argument with the roles of ρ and ρ' exchanged, we obtain $K_F(\rho') \geq K_F(\rho)$, which implies the desired equality. □

Observation 4. *K_F does not increase under addition of local ancilla, i.e. $K_F(\rho \otimes \rho') \leq K_F(\rho))$, where ρ' is a local state of either Alice or Bob.*

Proof. Let $\{(p_i, \gamma(\psi_i))\}_i$ be an arbitrary ensemble decomposition of ρ into strictly irreducible generalized private states. Then the ensemble

$$\{(p_i, \gamma(\psi_i) \otimes \rho')\}_i \tag{101}$$

is a valid ensemble decomposition of $\rho \otimes \rho'$ (not necessarily optimal). Indeed, local ancilla can be treated as a part of a shield system where each unitary operator that acts on the shield is extended by identity, written explicitly as follows:

$$\widetilde{\gamma}(\psi_i) = \gamma(\psi_i) \otimes \rho' = \sum_{l,m} \sqrt{\lambda_l^{(i)} \lambda_m^{(i)}} |e_l^{(i)} f_l^{(i)}\rangle\langle e_m^{(i)} f_m^{(i)}| \otimes \left(U_l^{(i)} \otimes \mathbb{1}\right)\left(\sigma^{(i)} \otimes \rho'\right)\left((U_m^{(i)})^\dagger \otimes \mathbb{1}\right). \tag{102}$$

From the above formula, it is clear that

$$K_F(\rho) = \sum_i p_i K_F(\gamma(\psi_i)) \tag{103}$$

$$= \sum_i p_i K_F(\widetilde{\gamma}(\psi_i)) \tag{104}$$

$$\geq K_F(\rho \otimes \rho'). \tag{105}$$

We have used the fact that extending the shield of the strictly irreducible generalized private state $\gamma(\psi_i)$ by a local state results in a strictly irreducible generalized private state $\widetilde{\gamma}(\psi_i)$. □

Observation 5. *K_F is non-increasing under the action of a local random unitary channel, i.e.*

$$K_F\left(\sum_x p_x (U_x \otimes \mathbb{1})\gamma_{a\widetilde{A}B}(U_x \otimes \mathbb{1})^\dagger\right) \leq K_F(\gamma_{a\widetilde{A}B}).$$

where the channel $\sum_x U_x(.)U_x^\dagger$ acts on subsystem a.

Proof.

$$K_F\left(\sum_x p_x \left(U_x \otimes \mathbb{1}\right) \gamma_{a\widetilde{A}B} \left(U_x \otimes \mathbb{1}\right)^\dagger\right)$$
$$\leq \sum_x p_x K_F((U_x \otimes \mathbb{1}) \gamma_{a\widetilde{A}B} (U_x \otimes \mathbb{1})^\dagger) \tag{106}$$
$$\leq \sum_x p_x K_F(\gamma_{a\widetilde{A}B}) = K_F(\gamma_{a\widetilde{A}B}). \tag{107}$$

The first inequality holds by Lemma 2, i.e., convexity of K_F, and the second by Observation 3. □

As a consequence of the above observation we notice that K_F is also non-increasing under the action of local von Neumann measurements and local partial traces. Indeed, the action of a local von Neumann measurement can written as

$$\gamma_{a\widetilde{A}B} \mapsto \frac{1}{d_a} \sum_\ell \left(V_\ell \otimes \mathbb{1}\right) \gamma_{a\widetilde{A}B} \left(V_\ell \otimes \mathbb{1}\right)^\dagger,$$

where $V_\ell = \sum_j \exp\{2\pi i \ell j/d\}|j\rangle\langle j|$ and local partial trace can be performed as a composition of three operations for which K_F is non-increasing: local von Neumann measurement, quantum Fourier transform, and local von Neumann measurement.

We note here that, from the above, it follows that K_F is monotonic under arbitrary local quantum operations. Indeed, we showed that K_F is monotonic under basic operations from which any quantum operation can be composed (adding auxiliary system, unitary and tracing out). What remains a challenge is to show that K_F does not increase under classical communication. This fact would imply monotonicity under LOCC in the sense given in the preliminary section, i.e., $K_F(\rho) \geq K_F(\Lambda(\rho))$ for $\Lambda \in$ LOCC. What is less clear is if K_F is collectively monotonic [20, 82], that is, if $K_F(\rho) \geq \sum_i p_i K_F(\rho_i)$ where ρ_i is a post-measurement state (after certain LOCC) and p_i is the corresponding probability of its occurrence. Let us stress here that the approach used in entanglement theory does not apply. In particular, it is not clear to us how to follow the general approach of [83] for establishing K_F to be an entanglement measure because the amount of key in the private state does not seem to be expressible as a direct entropic function of the reduced state of the AB systems (as opposed to subsystems $A_K B_K$, which can be different for each private state). We also note that K_F is not a so-called "mixed convex roof," as introduced in [84]. Indeed, in the latter reference, the mixed convex roof is defined as the infimum over ensembles of *all* mixed states that apply to a given state. Instead, K_F is a function of splitting only into special (in general mixed) states, the generalized private states.

Another important property that we would wish from K_F is asymptotic continuity. However, all known methods from entanglement theory do not immediately apply to show it. To give one example, the method of [81] for proving asymptotic continuity cannot be directly used. This is because a measurement on a purifying system of ρ that splits it into an ensemble of generalized private states does not necessarily generate an ensemble of generalized private states when applied to the purifying system of a state ρ' that is close to ρ in trace distance. Indeed, this is contrary to the fact used in the proof of continuity of E_F [81], according to which any rank-one POVM applied to the purifying system results in an ensemble with pure members, no matter to which state (ρ or ρ') it is applied.

7 Privacy dilution

This section is devoted to the description of how the privacy of a private state $\gamma(\Phi^+)$ can be diluted into an ε-approximation of n copies $\gamma(\psi)^{\otimes n}$ of a generalized private state, with $|\psi\rangle = \sum_{a\in\mathcal{A}} \lambda_a |e_a\rangle|f_a\rangle$. The protocol is such that the error ε in dilution approaches zero with increasing n.

Before providing details of the protocol, we describe two essential subroutines: Permutation Algorithm (PA) and Phase Error Correction (PEC). These procedures take care of the phase errors that occur during the execution of the first six steps of the Dilution Protocol. These two procedures use some auxiliary systems. We need these systems to return at the end of the protocol to their original state. Otherwise, they may leak some information about the key. We therefore also describe the inverse of the PA protocol (IPA), which takes care of this issue.

Since this section is rather technical, below we provide a table of notations used, with the goal of helping the reader in understanding various proofs and constructions.

7.1 Permutation Algorithm

The Permutation Algorithm makes use of two permutations $\pi_{\text{key}}(\mathbf{s}, \hat{\mathbf{s}})$ and $\pi_{\text{shield}}(\mathbf{s}, \hat{\mathbf{s}})$ that allow Alice and Bob to rearrange their subsystems into a desired order. The idea behind these permutations is as follows. By constructing a private state, given that the key takes a value $\mathbf{s}$, the shield should be rotated by the twisting unitary $U_{\mathbf{s}}$. More precisely, the shield system should be in a state $U_{\mathbf{s}} \rho^{\otimes n} U_{\mathbf{s}}^\dagger$, where

$$\mathbf{s} = (\mathbf{s}[1], \ldots, \mathbf{s}[n]) \in \mathcal{A}^n, \tag{108}$$
$$U_{\mathbf{s}} = U_{\mathbf{s}[1]} \otimes U_{\mathbf{s}[2]} \otimes \cdots \otimes U_{\mathbf{s}[n]}. \tag{109}$$

However, when a phase error occurs (as will take place in our dilution protocol described in the next section), then the unitary $U_{\widehat{\mathbf{s}}}$ occurs instead. If $\mathbf{s}$ and $\widehat{\mathbf{s}}$ were of the same type (with the same number of occurrences of symbols in it), then it would be sufficient to permute the systems of the shield, i.e., transform $\widehat{\mathbf{s}}$ into $\mathbf{s}$ by a permutation, thereby correcting the error. However, $\widehat{\mathbf{s}}$ may be of a different type. In what follows,

$\mathcal{A}^n$	a set of all n element sequences of symbols from alphabet $\mathcal{A}$
$\mathbf{s}, \widehat{\mathbf{s}}$	a sequence of symbols
$\mathbf{s}[i]$	i-th element of a sequence $\mathbf{s}$
$\perp_i$	a symbol $\perp$ at i-th position
$\lvert\mathbf{s}\rvert$	length of a sequence $\mathbf{s}$
$\lvert a(\mathbf{s})\rvert$	number of occurrences of symbol a in sequence $\mathbf{s}$
$X[1\dots n]$	a quantum system consisting of n subsystems
$X[i]$	i-th subsystem of a composite quantum system
$X[i:k]$	subsystems of system X of indices from i to k
$\lvert\perp\rangle_i$	a quantum state $\lvert\perp\rangle$ at i-th subsystem of a composite quantum system
$X_{\mathbf{s}_k}$	$U_{\mathbf{s}_k}\rho^{\otimes\lvert\mathbf{s}_k\rvert}U_{\mathbf{s}_k}^\dagger$

Table 1: Notations used in this section.

both sequences under consideration are from the same δ-typical set T_n^δ [65, Section 2.4]; that is, each symbol from the alphabet $\mathcal{A}$ has an empirical frequency that satisfies

$$\left|\lambda_a - \frac{|a(\mathbf{s})|}{n}\right| \leq \delta\lambda_a, \tag{110}$$

where $|a(\mathbf{s})|$ is the number of occurrences of a in string $\mathbf{s}$ and λ_a is the probability that symbol a occurs. Then for all symbols in $\mathcal{A}$ appearing in $\mathbf{s}$ such that their number of occurrences in $\widehat{\mathbf{s}}$ is larger, there is no problem; we can assign some entries of $\widehat{\mathbf{s}}$ to correspond with the same values as in $\mathbf{s}$ in a proper place. However, for all symbols in $\mathbf{s}$ that occur a larger number of times in $\mathbf{s}$ than in $\widehat{\mathbf{s}}$, there is a problem that cannot be resolved by a local permutation. Later on, we will see that $\widehat{\mathbf{s}} = \beta_x(\mathbf{s})$ where $\beta_x : T_n^\delta \to T_n^\delta$ (defined in Lemma 7) is a bijection.

The role of the permutation $\pi_{\text{shield}}(\mathbf{s}, \hat{\mathbf{s}})$ is to correct most of the errors by using the fact that $\mathbf{s}$ and $\widehat{\mathbf{s}}$ are close to being related to each other by a permutation. The permutation $\pi_{\text{shield}}(\mathbf{s}, \hat{\mathbf{s}})$ also swaps aside to systems $T_{A_S}T_{B_S}$ all the shielding systems for which the phase error cannot be corrected by a local permutation. The number of such errors is bounded from above by $L_{\max} \coloneqq \lceil 2\delta n\rceil$. These systems will be treated later by teleportation, local correction on one side, and teleportation back with a small amount of pure form of key, i.e., the singlet state.

In spite of the fact that the permutation $\pi_{\text{key}}(\mathbf{s}, \hat{\mathbf{s}})$ is constructed in the same way as $\pi_{\text{shield}}(\mathbf{s}, \hat{\mathbf{s}})$, its role is different. This operation, from a copy of the system $\widehat{\mathbf{s}}$ and the auxiliary system S_{out} in the state $|\perp\rangle^{\otimes(n+L_{\max})}$, creates a system S_{out} composed of two subsystems in the states $\mathbf{s}_{\text{cor}}$ and $\mathbf{s}_{\text{err}}$, respectively (and leaves $\widehat{\mathbf{s}}$ in the state $|\perp\rangle^{\otimes n}$). The states $\mathbf{s}_{\text{cor}}$ and $\mathbf{s}_{\text{err}}$ indicate how to correct the error on systems $B_S T_{A_S} T_{B_S}$ when they are in Bob's possession after teleportation of T_{A_S} by Alice. The state $\mathbf{s}_{\text{err}}$ indicates which unitary transformations should be inverted as they are incorrect. The state $\mathbf{s}_{\text{cor}}$ indicates that if the symbol $\perp$ occurs at position p_k, then the unitary U_a should be applied if the symbol a is in position p_k in $\mathbf{s}$. When applied to auxiliary systems, the permutation π_{key} creates a state that is further a control system for the Phase Error Correction algorithm. The register holding $\mathbf{s}_{\text{err}}$ indicates how to undo the errors, while the registers holding $\mathbf{s}$ and $\mathbf{s}_{\text{cor}}$ possess information about the correct unitary transformation that needs to be applied on system $T_{A_S}T_{B_S}$. Since the action of the above mentioned permutations is described on a pair $(\mathbf{s}, \widehat{\mathbf{s}})$ of sequences, then they are applied in a control-target manner (with control on the value of $\mathbf{s}$ and $\widehat{\mathbf{s}}$).

At the end of this section, we describe the Permutation Algorithm in more detail. For now, we first claim the existence of the desired permutations, which we argue by proving a number of combinatorial lemmas.

Lemma 3. *Suppose that $\mathbf{x}, \widehat{\mathbf{x}} \in T_n^\delta$. Then there exists an increasing sequence of indices $\{i_k\}_k$ selected from the set $\{1,\dots,n\}$ such that $\mathbf{x}$ can be written as*

$$\mathbf{x} = \mathbf{x}_1\mathbf{x}[i_1]\mathbf{x}_2\mathbf{x}[i_2]\cdots\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})}\mathbf{x}[i_{f(\mathbf{x},\widehat{\mathbf{x}})}]\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})+1}, \tag{111}$$

where $\mathbf{x}_k$ are blocks (not necessarily nonempty) of contiguous elements from the string $\mathbf{x}$,

$$f(\mathbf{x},\widehat{\mathbf{x}}) \coloneqq \sum_{a\in\mathcal{A}} \big||a(\mathbf{x})| - |a(\widehat{\mathbf{x}})|\big| \leq \lceil 2\delta n\rceil, \tag{112}$$

and there exists a permutation π such that

$$\pi(\widehat{\mathbf{x}}) = \mathbf{x}_1\widehat{\mathbf{x}}[j_1]\mathbf{x}_2\widehat{\mathbf{x}}[j_2]\cdots\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})}\widehat{\mathbf{x}}[j_{f(\mathbf{x},\widehat{\mathbf{x}})}]\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})+1}, \tag{113}$$

where $\{j_k\}_k$ is an increasing sequence of indices selected from the set $\{1,\dots,n\}$.

Proof. From strong typicality, for all $a \in \mathcal{A}$, we have that

$$\big||a(\mathbf{x})| - |a(\widehat{\mathbf{x}})|\big| \leq 2\delta\lambda_a n. \tag{114}$$

Therefore $0 \leq f(\mathbf{x},\widehat{\mathbf{x}}) \leq L_{\max}$, where

$$L_{\max} \coloneqq \lceil 2\delta n\rceil. \tag{115}$$

Since $f(\mathbf{x},\widehat{\mathbf{x}})$ counts the difference between the occurrences of each symbol in strings $\mathbf{x}$ and $\widehat{\mathbf{x}}$, then $\mathbf{x}$ and $\widehat{\mathbf{x}}$ have at least $n - f(\mathbf{x},\widehat{\mathbf{x}})$ in common. So we can group $n - f(\mathbf{x},\widehat{\mathbf{x}})$ elements from $\widehat{\mathbf{x}}$ into at most $f(\mathbf{x},\widehat{\mathbf{x}}) + 1$ blocks (not necessarily non-empty) $\widehat{\mathbf{x}}_1, \widehat{\mathbf{x}}_2, \dots, \widehat{\mathbf{x}}_{f(\mathbf{x},\widehat{\mathbf{x}})}, \widehat{\mathbf{x}}_{f(\mathbf{x},\widehat{\mathbf{x}})+1}$ which are equal to blocks

$\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})}, \mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})+1}$ of contiguous elements from $\mathbf{x}$ such that

$$\mathbf{x} = \mathbf{x}_1\mathbf{x}[i_1]\mathbf{x}_2\mathbf{x}[i_2]\ldots\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})}\mathbf{x}[i_{f(\mathbf{x},\widehat{\mathbf{x}})}]\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})+1}, \tag{116}$$

where $i_k = i_{k-1} + |\mathbf{x}_k| + 1$ and $i_1 = |\mathbf{x}_1| + 1$. The remaining $f(\mathbf{x},\widehat{\mathbf{x}})$ elements from the string $\widehat{\mathbf{x}}$ can be denoted as $\widehat{\mathbf{x}}[j_1]\ldots\widehat{\mathbf{x}}[j_{f(\mathbf{x},\widehat{\mathbf{x}})}]$, where j_k are indices of elements in the sequence $\widehat{\mathbf{x}}$. Observe that the elements $\widehat{\mathbf{x}}[j_1]\ldots\widehat{\mathbf{x}}[j_{f(\mathbf{x},\widehat{\mathbf{x}})}]$ can be ordered in such a way that $j_k < j_m$ for $k < m$. Now it is clear that there exists a permutation π that rearranges elements of $\widehat{\mathbf{x}}$ into the desired order. □

Lemma 4. *Suppose that $\mathbf{x}, \widehat{\mathbf{x}} \in T_n^\delta$. Then there exists a permutation π such that*

$$\begin{aligned}\pi(\widehat{\mathbf{x}}\underbrace{\perp\ldots\perp}_{n+L_{\max}}) = \underbrace{\perp\ldots\perp}_{n}\\ \mathbf{x}_1 \perp \mathbf{x}_2 \perp \ldots \mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})} \perp \mathbf{x}_{f(\mathbf{x})+1}\\ \widehat{\mathbf{x}}[j_1]\ldots\widehat{\mathbf{x}}[j_{f(\mathbf{x},\widehat{\mathbf{x}})}]\ \underbrace{\perp\ldots\perp}_{L_{\max}-f(\mathbf{x},\widehat{\mathbf{x}})}.\end{aligned} \tag{117}$$

Proof. From Lemma 3, we know that there exists a permutation π that rearranges the string $\widehat{\mathbf{x}}\underbrace{\perp\ldots\perp}_{n+L_{\max}}$ into

$$\mathbf{x}_1\widehat{\mathbf{x}}[j_1]\mathbf{x}_2\widehat{\mathbf{x}}[j_2]\ldots\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})}\widehat{\mathbf{x}}[j_{f(\mathbf{x},\widehat{\mathbf{x}})}]\mathbf{x}_{f(\mathbf{x},\widehat{\mathbf{x}})+1}\underbrace{\perp\ldots\perp}_{n+L_{\max}}. \tag{118}$$

Now it remains to compose it with $n + f(\mathbf{x},\widehat{\mathbf{x}})$ transpositions to obtain the desired permutation. □

Lemma 5. *Suppose that $\mathbf{s}, \widehat{\mathbf{s}} \in T_n^\delta$. Then there exists a unitary operation corresponding to $\pi_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})$ that maps systems $\widehat{S}$ and S_{out}, which are initially in the state $|\widehat{\mathbf{s}}\rangle_{\widehat{S}}|\perp\rangle_{S_{\text{out}}}^{\otimes(n+L_{\max})}$, to systems in the state $|\mathbf{s}_{\text{all}}\rangle$*

$$\begin{aligned}|\mathbf{s}_{\text{all}}\rangle = |\perp\rangle_{\widehat{S}}^{\otimes n} \otimes |\mathbf{s}_1, \perp_{i_1}, \mathbf{s}_2, \perp_{i_2}, \ldots,\\ \mathbf{s}_{f(\mathbf{s},\widehat{\mathbf{s}})}, \perp_{i_{f(\mathbf{s},\widehat{\mathbf{s}})}}, \mathbf{s}_{f(\mathbf{s},\widehat{\mathbf{s}})+1}, \widehat{\mathbf{s}}[j_1], \widehat{\mathbf{s}}[j_2], \ldots,\\ \widehat{\mathbf{s}}[j_{f(\mathbf{s},\widehat{\mathbf{s}})}], \perp_{(f(\mathbf{s},\widehat{\mathbf{s}})+1)}, \ldots, \perp_{L_{\max}}\rangle_{S_{\text{out}}}\\ \equiv |\underbrace{\perp,\ldots\perp}_{n\ times}\rangle_{\widehat{S}}|\mathbf{s}_{\text{cor}}, \mathbf{s}_{\text{err}}\rangle_{S_{\text{out}}}.\end{aligned} \tag{119}$$

Here for abbreviation, by $\perp_{i_k}$ we mean the state $|\perp\rangle$ at position i_k.

Proof. The desired operation is a quantum realization (i.e., a permutation of quantum systems) of a permutation from Lemma 4. Since every permutation is a composition of transpositions, it is clear that such a quantum operation can be constructed as a composition of SWAP operations. □

Lemma 6. *Suppose that $\mathbf{s}, \widehat{\mathbf{s}} \in T_n^\delta$, the permutation $\pi_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})$ corresponds to a unitary operation from Lemma 5, and system A_S is in the state*

$$U_{\widehat{\mathbf{s}}}\rho^{\otimes n}U_{\widehat{\mathbf{s}}}^\dagger.$$

Then there exists a unitary operation $\pi_{\text{shield}}(\mathbf{s},\widehat{\mathbf{s}})$ that maps systems $A_S[1\ldots n], \widetilde{A}_S[1\ldots n]$ and $T_{A_S}[1\ldots L_{\max}]$ where $\widetilde{A}_S[1\ldots n]$ is initially in state $|\perp\rangle^{\otimes n}$ and $T_{A_S}[1\ldots L_{\max}]$ is initially in state $|\perp\rangle^{\otimes L_{\max}}$ into systems in the states

$$A_S \to |\perp\rangle^{\otimes n}, \tag{120}$$

$$\widetilde{A}_S[1\ldots n] \to \tag{121}$$

$$\begin{aligned}U_{\mathbf{s}_1}\rho^{\otimes|\mathbf{s}_1|}U_{\mathbf{s}_1}^\dagger \otimes |\perp\rangle\langle\perp|_{i_1} \otimes U_{\mathbf{s}_2}\rho^{\otimes|\mathbf{s}_2|}U_{\mathbf{s}_2}^\dagger \otimes |\perp\rangle\langle\perp|_{i_2} \otimes\\ \ldots \otimes |\perp\rangle\langle\perp|_{i_{f(\mathbf{s},\widehat{\mathbf{s}})}} \otimes U_{\mathbf{s}_{f(\mathbf{s},\widehat{\mathbf{s}})+1}}\rho^{\otimes|\mathbf{s}_{f(\mathbf{s},\widehat{\mathbf{s}})+1}|}U_{\mathbf{s}_{f(\mathbf{s},\widehat{\mathbf{s}})+1}}^\dagger,\end{aligned} \tag{122}$$

$$T_{A_S} \to A_S[j_1]\ldots A_S[j_{f(\mathbf{s},\widehat{\mathbf{s}})}]\ \underbrace{\perp\ldots\perp}_{L_{\max}-f(\mathbf{s},\widehat{\mathbf{s}})}, \tag{123}$$

where indices i_k, j_k and blocks $\mathbf{s}_k$ are the same as in a given quantum operation $\pi_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})$.

Proof. This operation is almost the same as the given $\pi_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})$, but it acts on different subsystems. □

We now aim to define the action of PA for Alice, which uses the permutations defined above. See Algorithm 1 below. Bob's version is almost the same, but with the interchange of symbols $A \leftrightarrow B$. The procedure first creates auxiliary systems $\widehat{S}$, $\widehat{S}_1$, T_{A_S}, and $\widetilde{A}_S[1\ldots n]$ and then performs permutations τ_{key}^{PA} and $\tau_{\text{shield}}^{PA}$, which are based on $\pi_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})$ and $\pi_{\text{shield}}(\mathbf{s},\widehat{\mathbf{s}})$ as defined in Lemmas 5 and 6, respectively.

Algorithm 1 Permutation Algorithm

1: **procedure** PA($A_K[1\ldots n], A_S[1\ldots n]$)
2: From $|\mathbf{s}\rangle_{A_K}$, locally create the state $|\mathbf{s}\rangle_{A_K}|\beta_x(\mathbf{s})\rangle_{\widehat{S}}|\beta_x(\mathbf{s})\rangle_{\widehat{S}_1} \equiv |\mathbf{s}\rangle_A|\widehat{\mathbf{s}}\rangle_{\widehat{S}}|\widehat{\mathbf{s}}\rangle_{\widehat{S}_1}$.
3: create a register T_{A_S} of size $L_{\max}$ in the state $|\perp\rangle^{\otimes L_{\max}}$.
4: create a register $\widetilde{A}_S[1\ldots n]$ in the state $|\perp\rangle^{\otimes n}$.
5: create a register S_{out} in the state $|\perp\rangle^{\otimes(n+L_{\max})}$
6: Alice performs the following unitary on $A_K\widehat{S}\widehat{S}_1S_{\text{out}}$: $\tau_{\text{key}}^{PA} := \sum_{\mathbf{s},\widehat{\mathbf{s}}\in T_n^\delta}|\mathbf{s},\widehat{\mathbf{s}}\rangle\langle\mathbf{s},\widehat{\mathbf{s}}|_{A_K\widehat{S}} \otimes \pi_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})_{\widehat{S}_1S_{\text{out}}}$
7: Alice performs the following unitary on $A_K\widehat{S}A_S\widetilde{A}_ST_{A_S}$: $\tau_{\text{shield}}^{PA} := \sum_{\mathbf{s},\widehat{\mathbf{s}}\in T_n^\delta}|\mathbf{s},\widehat{\mathbf{s}}\rangle\langle\mathbf{s},\widehat{\mathbf{s}}|_{A_K\widehat{S}} \otimes \pi_{\text{shield}}(\mathbf{s},\widehat{\mathbf{s}})_{A_S\widetilde{A}_ST_{A_S}} + \sum_{(\mathbf{s},\widehat{\mathbf{s}})\notin T_n^\delta\times T_n^\delta}|\mathbf{s},\widehat{\mathbf{s}}\rangle\langle\mathbf{s},\widehat{\mathbf{s}}|_{A_K\widehat{S}} \otimes \mathbb{1}_{A_S\widetilde{A}_ST_{A_S}}$

To summarize this subsection, we provide an example for the reader who is more interested in the idea of the protocol rather than in a strict mathematical proof. Let $n = 9$, $\delta = \frac{7}{9}$, $\mathcal{A} = \{a, b, c, d\}$ and $\lambda_x = \frac{1}{4}$

for each $x \in \mathcal{A}$. For this example, we choose the following two strings from $\mathcal{A}^n$

$$\mathbf{s} = (b, c, c, b, d, b, a, a, c), \tag{124}$$
$$\widehat{\mathbf{s}} = (c, b, b, c, c, d, a, d, c). \tag{125}$$

It is easy to check that these two strings belong to the δ-typical set T_n^δ. Given n and δ as chosen above, we find that $L_{\max} = 14$. The states of the systems $\widehat{S}_1$, S_{out}, A_S, $\widetilde{A}_S$, and T_{A_S} before and after the application of τ_{key}^{PA} and $\tau_{\text{shield}}^{PA}$ are depicted in Figures 2 and 3, respectively.

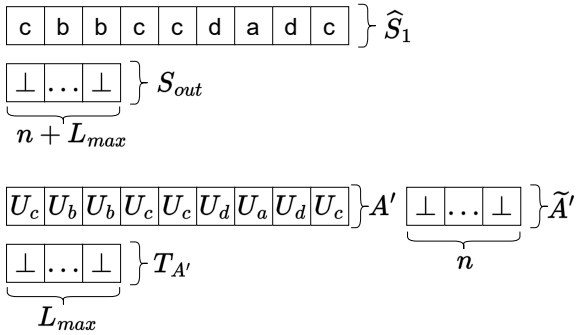


Figure 2: Systems $\widehat{S}_1, S_{\text{out}}, A_S, \widetilde{A}_S, T_{A_S}$ before the application of τ_{key}^{PA} and $\tau_{\text{shield}}^{PA}$.

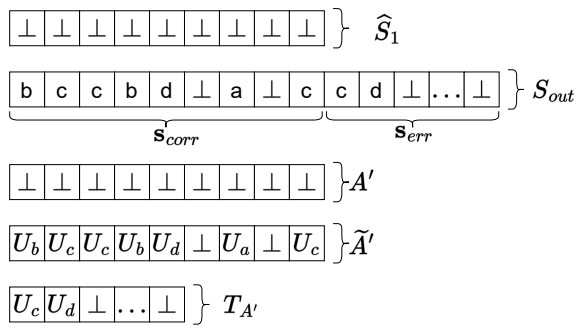


Figure 3: Systems $\widehat{S}_1, S_{\text{out}}, A_S, \widetilde{A}_S, T_{A_S}$ after the application of τ_{key}^{PA} and $\tau_{\text{shield}}^{PA}$.

7.2 Phase error correction algorithm

We now explain how the output of the PA (applied both by Alice and by Bob), taken as the input of the Phase Error Correction (PEC) algorithm, is used to correct coherently the errors that remain after the PA procedure. Most of the errors have been corrected by PA. However, the errors that came out due to a type mismatch of $\mathbf{s}$ and $\widehat{\mathbf{s}} \equiv \beta_x(\mathbf{s})$, collected in the system $T_{A_S}T_{B_S}$ need to be handled separately. By notation, $|x\rangle_j$ is equal to the j-th subsystem of the state $|x\rangle$. Further, S_{out}^B denotes system S_{out} obtained by applying τ_{key}^{PA} by Bob during the execution of PA given in Algorithm 1. The aforementioned errors can be corrected in two steps:

1. untwisting incorrect unitaries,
2. applying correct unitaries.

The first step is easy to perform because it suffices for Bob to apply the following unitary operation

$$\tau_1^{\text{PEC}} := \bigotimes_{i=1}^{L_{\max}} \Big[\sum_{a \neq \perp} |a\rangle\langle a|_{\mathbf{s}_{\text{err}}[i]} \otimes U_{a,T_{A_S}[i]T_{B_S}[i]}^{\dagger} + |\perp\rangle\langle\perp|_{\mathbf{s}_{\text{err}}[i]} \otimes \mathbb{1}_{a,T_{A_S}[i]T_{B_S}[i]} \Big]. \tag{126}$$

Performing the second step requires auxiliary system C initially in state $|1\rangle_C$ that will be used as a counter. To make use of this counter, we define the following unitary operation

$$U_{XC}^{\text{shift}} := \sum_{a \in \mathcal{A}} |a\rangle\langle a|_X \otimes \mathbb{1}_C + |\perp\rangle\langle\perp|_X \otimes U_C^{\oplus 1}, \tag{127}$$

where $U^{\oplus 1}$ is a unitary operation that transforms $|t\rangle$ into $|(t \oplus 1) \mod L_{\max}\rangle$. To perform the second step, Bob has to do the following procedure. For each $i \in \{1, \ldots, n\}$, Bob applies

$$\tau_2^{\text{PEC}}(i) := \sum_{b \in \mathcal{A}} \sum_{c=1}^{L_{\max}} \sum_{a \in \mathcal{A} \cup \{\perp\}} |a\rangle\langle a|_{\mathbf{s}[i]} \otimes |b\rangle\langle b|_{\mathbf{s}_{\text{cor}}[i]} \otimes |c\rangle\langle c|_C \otimes \mathbb{1}_{T_{A_S}T_{B_S}} + |a\rangle\langle a|_{\mathbf{s}[i]} \otimes |\perp\rangle\langle\perp|_{\mathbf{s}_{\text{cor}}[i]} \otimes |c\rangle\langle c|_C \otimes U_{T_{A_S}T_{B_S}}^{a,c}, \tag{128}$$

where

$$U_{T_{A_S}T_{B_S}}^{a,c} := U_{a,T_{A_S}[c]T_{B_S}[c]} \otimes \mathbb{1}_{T_{A_S}[\neq c]T_{B_S}[\neq c]} \tag{129}$$

and U_a is a unitary operation from the definition of private states and corresponding to the symbol a (see (51)). Next he applies $U_{\mathbf{s}_{\text{cor}}[i]C}^{\text{shift}}$, as defined in (127). We conclude this section by presenting the PEC algorithm in a compact format:

Algorithm 2 Phase Error Correction Algorithm

1: **procedure** PEC($B_K S_{\text{out}}^B T_{A_S} T_{B_S}$)
2: Alice teleports the system T_{A_S} to Bob.
3: Bob creates system C in state $|1\rangle$.
4: Bob performs
5: $\tau_1^{\text{PEC}} := \otimes_{i=1}^{L_{\max}} \big[\sum_{a \neq \perp} |a\rangle\langle a|_{\mathbf{s}_{\text{err}}[i]} \otimes U_{a,T_{A_i'}T_{B_i'}}^{\dagger} + |\perp\rangle\langle\perp|_{\mathbf{s}_{\text{err}}[i]} \otimes \mathbb{1}_{a,T_{A_i'}T_{B_i'}} \big]$
6: **for** i = 1 to n **do**
7: $\tau_2^{\text{PEC}}(i)$,
8: $U_{\mathbf{s}_{\text{cor}}[i]C}^{\text{shift}}$
9: **endfor**
10: Bob teleports the system T_{A_S} back to Alice.
11: Bob resets his counter system C to state $|1\rangle$ by applying $\left(U_{\mathbf{s}_{\text{cor}}[i]C}^{\text{shift}}\right)^{\dagger}$ n times.

To continue the example given in the previous section, we present the action of τ_1^{PEC} in Figure 4, $\tau_2^{\text{PEC}}(6)$ in Figure 5, and $U_{\mathbf{s}_{\text{cor}}C}^{\text{shift}}$ in Figure 6.

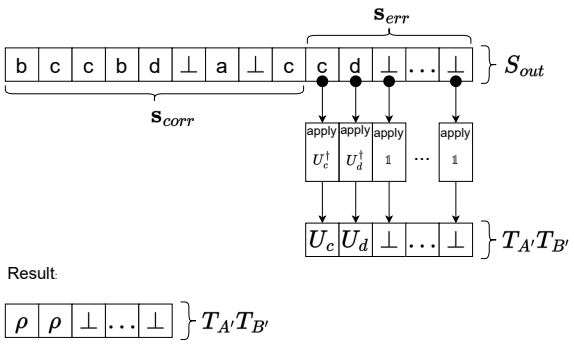


Figure 4: τ_1^{PEC} operation. Control systems are marked with a black dot. If there is a symbol $a \in \mathcal{A}$ on $\mathbf{s}_{\mathrm{err}}[k]$, then it applies $U_a^\dagger$ on the system $T_{A_S}T_{B_S}[k]$. On the other hand, if there is a symbol $\perp$ on $\mathbf{s}_{\mathrm{err}}[k]$, then it applies $\mathbb{1}$. After the action of τ_1^{PEC}, states stored in the system $T_{A_S}T_{B_S}$ become untwisted.

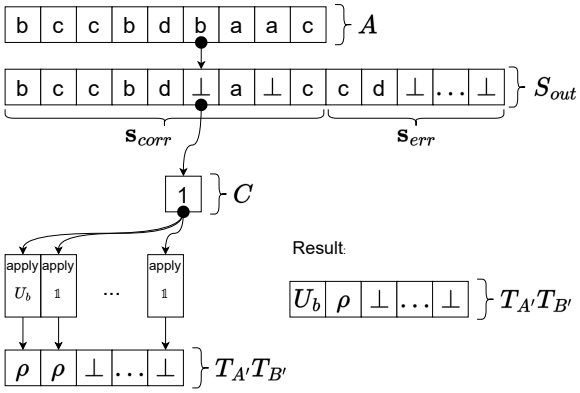


Figure 5: The action of $\tau_2^{\mathrm{PEC}}(6)$ operation. Notice that this is only one step from the loop which iterates from $i = 1$ to $i = 9$ and for each i, the operation $\tau_2^{\mathrm{PEC}}(i)$ is performed. $\tau_2^{\mathrm{PEC}}(6)$ operation has a control on $A_K[6]$, $\mathbf{s}_{\mathrm{cor}}[6]$, C and target on $T_{A_S}T_{B_S}$. If it 'sees' $\perp$ on $\mathbf{s}_{\mathrm{cor}}[6]$, then it applies U_b on $T_{A_S}T_{B_S}[1]$ where b, 1 are states of system $\mathbf{s}_{\mathrm{cor}}[6]$ and C respectively. Otherwise, it applies $\mathbb{1}$. As a result of this operation, the state $T_{A_S}T_{B_S}[1]$ is twisted with a correct unitary operation. Notice also that after this operation state of the system C will be shifted, because $\mathbf{s}_{\mathrm{cor}}[6]$ is in a $\perp$ state (see Figure 6 or Step 8 of Algorithm 2).

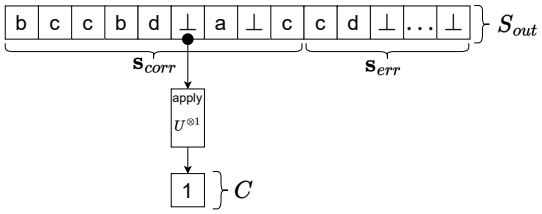


Figure 6: The action of $U^{\mathrm{shift}}_{\mathbf{s}_{\mathrm{cor}}[6]C}$ operation. It has control on $\mathbf{s}_{\mathrm{cor}}[6]$ system and target on C system. If there is a $\perp$ symbol on $\mathbf{s}_{\mathrm{cor}}[6]$, then the state of C is incremented by 1.

7.3 Inverting PA Protocol

In the preceding two sections, we have seen that the composition of PA and PEC is, in fact, a composition of twistings, i.e., controlled-unitary operations. The first one has a control on $|\mathbf{s}\rangle_{A_K}$ and creates $|\widehat{\mathbf{s}}\rangle$. The next one τ^{PA}_{key} has a control on $|\mathbf{s}\rangle_{A_K}|\widehat{\mathbf{s}}\rangle_{\widehat{S}}$ and permutes $|\widehat{\mathbf{s}}\rangle_{\widehat{S}_1}|\mathbf{s}_{\mathrm{out}}\rangle$. Further $\tau^{PA}_{\mathrm{shield}}$ is applied with a control on $|\mathbf{s}\rangle_{A_K}|\widehat{\mathbf{s}}\rangle_{\widehat{S}}$ and with a target on $A_S[1\dots n]\widetilde{A}_S[1\dots n]T_{A_S}[1\dots L_{\max}]$. Next, PEC also performs twistings, specified by τ_1^{PEC} and τ_2^{PEC} given in lines 5 and 8 of the definition of PEC. Note that the twisting operations mentioned above involve auxiliary systems initiated in a tensor power of $|0\rangle$ or $|\perp\rangle$. These auxiliary systems were changed via further operations.

In this section, we show that all the auxiliary systems can be uncomputed to their original state and therefore traced out with no leakage of information about the key of systems A_KB_K of the generalized private state to Eve. It is the final building block of the privacy dilution protocol. Note here that if we trace out the auxiliary systems to Eve without resetting them to the initial state, she will learn about the key part of the state to be produced. The output of this procedure would no longer be the $\widetilde{\gamma}(\rho_{\delta,n})$ state, which is undesirable.

In what follows, we describe the Inverting Permutation Algorithm, which outputs the desired state only on the systems $A_KA_SB_KB_S$. However, at first, we will describe a procedure of rearranging subsystems of systems $A_S, \widetilde{A}_S, T_{A_S}, B_S, \widetilde{B}_S, T_{B_S}$ to obtain the correct state on A_S, B_S and $|\perp\rangle^{\otimes(n+L_{\max})}$ on the remaining auxiliary systems. To do this, we have to define another unitary operation, namely

$$\tau_1^{\mathrm{IPA}}(i) := \sum_{c=1}^{L_{\max}} \sum_{a\in\mathcal{A}} |a\rangle\langle a|_{\mathbf{s}_{\mathrm{cor}}[i]} \otimes |c\rangle\langle c|_C \otimes \mathbb{1}_{T_{A_S}\widetilde{A}_S} +$$

$$|\perp\rangle\langle\perp|_{\mathbf{s}_{\mathrm{cor}}[i]} \otimes |c\rangle\langle c|_C \otimes W^{c,i}_{T_{A_S}\widetilde{A}_S}, \quad (130)$$

where

$$W^{c,i}_{T_{A_S}\widetilde{A}_S} := \mathrm{SWAP}[\widetilde{A}_S[i], T_{A_S}[c]] \otimes \mathbb{1}_{\widetilde{A}_S[\neq i]T_{A_S}[\neq c]}. \quad (131)$$

To perform this operation, Alice creates an auxiliary system C that will serve as a counter (Bob has already created it during the PEC algorithm). Now, for each $i \in \{1,\dots,n\}$, both of them have to perform the same steps on appropriate systems, as follows:

1. apply $\tau_1^{\mathrm{IPA}}(i)$,
2. apply $U^{\mathrm{shift}}_{\mathbf{s}_{\mathrm{cor}}[i]C}$.

After these steps, both of them have to swap systems $\widetilde{A}_S$ and A_S to obtain a corrected shield in system A_S and the state $|\perp\rangle^{\otimes(n+L_{\max})}$ in systems $\widetilde{A}_S$ and T_{A_S}. It only remains to reset the counter by performing $\left(U^{\mathrm{shift}}_{\mathbf{s}_{\mathrm{cor}}[i]C}\right)^\dagger$ n times.

The description of IPA is as follows.

Algorithm 3 Inverting PA

1: **procedure** IPA($A_K A_S \widehat{S}_1 S_{\text{out}} T_{A_S}, \beta_x$)
2: Alice creates system C in state $|1\rangle$
3: Alice does:
4: **for** i $= 1$ to n **do**
5: $\tau_1^{\text{IPA}}(i)$,
6: $U^{\text{shift}}_{\mathbf{s}_{\text{cor}}[i]C}$
7: **endfor**
8: Alice swaps systems A_S and $\widetilde{A}_S$
9: Alice performs the following unitary on $B_K \widehat{S} \widehat{S}_1 S_{\text{out}}$: $\tau^{PA\dagger}_{\text{key}} \equiv \sum_{\mathbf{s},\widehat{\mathbf{s}} \in T_n^\delta} |\mathbf{s},\widehat{\mathbf{s}}\rangle\langle \mathbf{s},\widehat{\mathbf{s}}|_{B_K \widehat{S}} \otimes \pi^{-1}_{\text{key}}(\mathbf{s},\widehat{\mathbf{s}})_{\widehat{S}_1 S_{\text{out}}}$
10: Alice undoes the creation of $|\widehat{s}\rangle_{\widehat{S}} |\widehat{s}\rangle_{\widehat{S}_1}$ done in Step 1 of PA by applying $U^\dagger_{\beta_x}$ twice
11: Alice applies CNOTs to reset the state $|\mathbf{s}\rangle$ to $|0\rangle^{\otimes n}$ in systems $\widehat{S}, \widehat{S}_1$
12: Alice traces out the auxiliary systems $\widehat{S}\widehat{S}_1 S_{\text{out}} \widetilde{A}_S T_{A_S}$.

Lastly, we depict the action of $\tau_1^{\text{IPA}}(8)$ in Figure 7.

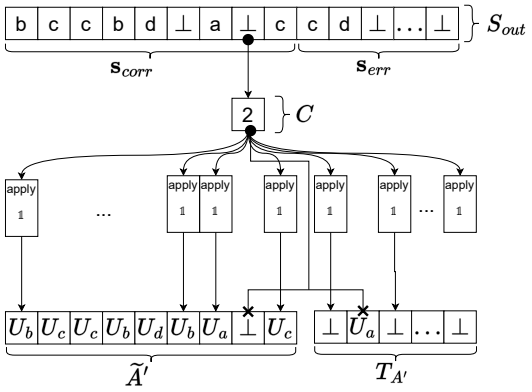


Figure 7: $\tau_1^{\text{IPA}}(8)$ operation. Notice that this is only one step from the loop, which iterates from $i = 1$ to $i = 9$. The state of the counter system C is 2 since it has been shifted when $i = 6$ (see Figure 6 and Step 6 of Algorithm 3). This operation swaps $\widetilde{A}_S[8]$ (since $i = 8$) and $T_{A_S}[2]$ (since state of the counter system C is 2) and applies $\mathbb{1}$ to systems $\widetilde{A}_S[\neq 8]$ and $T_{A_S}[\neq 2]$. The swap operation occurs, because system $\mathbf{s}_{\text{cor}}[i]$ is in a state $\perp$. If this system was in a state other than $\perp$, then the operation $\tau_1^{\text{IPA}}(8)$ would apply the identity $\mathbb{1}$ to all systems.

7.4 Privacy dilution protocol

We now introduce the privacy dilution protocol, which transforms a private state into a generalized private state. It uses the fact that the secure one-time pad protocol is a classical correspondent of quantum teleportation.

Theorem 3. *For any generalized private state $\gamma(\psi)$ with $|\psi\rangle = \sum_{a\in\mathcal{A}} \lambda_a |e_a\rangle|f_a\rangle$ and sufficiently large number $n \in \mathbb{N}$, the state $\gamma(\psi)^{\otimes n}$ can be created by LOCC from a strictly irreducible private state $\gamma_{d_n}(\Phi^+) \otimes |\Phi^+\rangle\langle\Phi^+|_{d'_n}$ with error less than 2ε in trace distance, key rate $\log_2 d_n = \lceil n(S(A_K)_\psi + \eta)\rceil$, and $\log_2 d'_n = \lceil 4\delta n\rceil$, where $\eta, \varepsilon, \delta \to 0$ as $n \to \infty$.*

Before proving Theorem 3 in Section 7.5, we describe the Privacy Dilution protocol, which assures the validity of the claim made here. To this end, we first define a private state $\gamma_{d_n}(\Phi^+)$, followed by the steps of the Dilution Protocol.

Let $|\psi\rangle = \sum_{a\in\mathcal{A}} \sqrt{\lambda_a}|e_a\rangle|f_a\rangle$. Further denote

$$\psi^{\otimes n} = \sum_{\mathbf{s}} \sqrt{\lambda_{\mathbf{s}}} |e_{\mathbf{s}} f_{\mathbf{s}}\rangle, \tag{132}$$

$$\gamma(\psi)^{\otimes n} = \sum_{\mathbf{s},\mathbf{s}'=0}^{|\mathcal{A}|^n-1} \sqrt{\lambda_{\mathbf{s}}\lambda_{\mathbf{s}'}} |e_{\mathbf{s}} f_{\mathbf{s}}\rangle\langle e_{\mathbf{s}'} f_{\mathbf{s}'}| \otimes U_{\mathbf{s}} \widetilde{\rho}_{A_S B_S} U^\dagger_{\mathbf{s}'}, \tag{133}$$

where more precisely,

$$\widetilde{\rho}_{A_S B_S} = \rho^{\otimes n}_{A_S B_S}, \tag{134}$$

$$\mathbf{s} = (\mathbf{s}[1], \ldots, \mathbf{s}[n]) \in \mathcal{A}^n, \tag{135}$$

$$U_{\mathbf{s}} = U_{\mathbf{s}[1]} \otimes U_{\mathbf{s}[2]} \otimes \cdots \otimes U_{\mathbf{s}[n]}, \tag{136}$$

$$\lambda_{\mathbf{s}} = \lambda_{\mathbf{s}[1]} \times \lambda_{\mathbf{s}[2]} \times \cdots \times \lambda_{\mathbf{s}[n]}. \tag{137}$$

It will be convenient to work with an approximate version of this state. It is sufficient because $\gamma(\psi)^{\otimes n}$ is isomorphic to $\widetilde{\gamma}(\psi^{\otimes n})$, where in the latter state the shielding system is $\widetilde{\rho}_{A_S B_S}$ and the twisting is constructed by $\{U_{\mathbf{s}}\}_{\mathbf{s}}$. We further note that we will be able to construct only an approximate version of $\widetilde{\gamma}_{A_S B_S}$, namely, one that twists only the typical subspace, i.e. $\text{span}(\{|e_{\mathbf{s}} f_{\mathbf{s}}\rangle\}_{\mathbf{s}\in T_n^\delta})$, of the space $\text{span}(\{|e_{\mathbf{s}} f_{\mathbf{s}}\rangle\}_{\mathbf{s}\in\mathcal{A}^n})$. To this end, note that, for each $\varepsilon > 0$ and $\delta > 0$, there exists sufficiently large n such that

$$\left\| \psi^{\otimes n} - \frac{1}{N} \sum_{\mathbf{s},\mathbf{s}'\in T_n^\delta} |\psi_{\mathbf{s}}\rangle\langle\psi_{\mathbf{s}'}| \right\|_1 \leq \varepsilon, \tag{138}$$

where $|\psi_{\mathbf{s}}\rangle \coloneqq \sqrt{\lambda_{\mathbf{s}}}|e_{\mathbf{s}}\rangle|f_{\mathbf{s}}\rangle$, T_n^δ is the set of δ-typical sequences of n symbols from the alphabet $\mathcal{A}$, and $N = \sum_{s\in T_n^\delta} \lambda_{\mathbf{s}}$, so that $N \geq 1 - \varepsilon$, due to the law of large numbers (see Section 4). These are sequences with a number of each symbol close to its expected value by δ in modulus. Let

$$\rho_{\delta,n} \coloneqq \frac{1}{N} \sum_{\mathbf{s},\mathbf{s}'\in T_n^\delta} |\psi_{\mathbf{s}}\rangle\langle\psi_{\mathbf{s}'}|. \tag{139}$$

According to the above, by the data-processing inequality for the trace distance and the triangle inequality, for every $\varepsilon, \delta > 0$ and sufficiently large n,

$$\left\|\widetilde{\gamma}(\psi^{\otimes n}) - \widetilde{\gamma}(\rho_{\delta,n})\right\|_1 \leq 3\varepsilon, \tag{140}$$

where $\widetilde{\gamma}(\rho_{\delta,n})$ is defined as

$$\widetilde{\gamma}(\rho_{\delta,n}) \coloneqq$$
$$(1-\varepsilon)\sum_{\mathbf{s},\mathbf{s}'\in T_n^\delta}\frac{\sqrt{\lambda_{\mathbf{s}}\lambda_{\mathbf{s}'}}}{N}|e_{\mathbf{s}}f_{\mathbf{s}}\rangle\langle e_{\mathbf{s}'}f_{\mathbf{s}'}|\otimes U_{\mathbf{s}}\widetilde{\rho}_{A_SB_S}U_{\mathbf{s}'}^\dagger + \varepsilon|\varnothing\varnothing\varnothing\varnothing\rangle\langle\varnothing\varnothing\varnothing\varnothing|_{A_KB_KA_SB_S}, \quad (141)$$

with $\varnothing \notin \{\mathcal{A}\cup\{\perp\}\}$.

We now construct a private state from which we will be able to produce the state $\widetilde{\gamma}(\rho_{\delta,n})$, which is sufficient for us due to the above closeness relation. We design it using an optimal compression encoding [66]. This encoding, call it C, maps one-to-one $|\mathcal{A}|$-ry strings $\mathbf{s}$ of symbols from $\mathcal{A}$ with entropy

$$H(\{\lambda_{\mathbf{s}}\}_{\mathbf{s}}) = H\left(\left\{\prod_{i=1}^n \lambda_{(\mathbf{s})[i]}\right\}_{\mathbf{s}}\right) = S(A_K)_\psi \quad (142)$$

into codewords $c(\mathbf{s})$ of length at most $L(n,\eta) \equiv \lceil n(S(A_K)_\psi+\eta)\rceil$ for some $\eta>0$, which converges to 0 as $n\to\infty$ (here, $H(\cdot)$ denotes the Shannon entropy of a distribution). These codewords are orthogonal when treated as pure states in a computational basis. A simple example of such an encoding is mapping δ_1-strongly typical sequences to all sequences (in lexicographic order) of length $\lceil nS(A_K)_\psi(1+\delta_1)\rceil$ and all not δ_1-strongly typical sequences (see definition in (29) and its properties) to an error symbol $\varnothing$ (which happens with negligible probability $\leq\varepsilon$ for sufficiently large n). In that case we identify η with $\delta_1 S(A_K)_\psi$. However, any other compression scheme with rate $L(n,\eta)$, which does not map a strongly typical sequence to an error state, works in this case.

We will consider now only the δ-typical sequences $\mathbf{s}$, as these are the only ones appearing in $\rho_{\delta,n}$ that get twisted in $\widetilde{\gamma}(\rho_{\delta,n})$. Let the encoding C assign $\mathbf{s}\mapsto c(\mathbf{s})$, where $c(\mathbf{s})$ is a codeword that corresponds to $\mathbf{s}$ via the chosen encoding of string $\mathbf{s}$, which is of size $L(n,\eta)$ at most. Further, we order each codeword $c(\mathbf{s})$ lexicographically, denoted by $r(c(\mathbf{s}))$, so that they correspond further one-to-one to $|\mathcal{A}|$-ary strings of length $L(n,\eta)$ through the mapping R. Because in the case of the strongly typical sequences, the Shannon compression scheme is lossless, C is a bijection. Therefore there exists a bijection $\mathbf{s}(r)\coloneqq C^{-1}\circ R^{-1}(r)$ that maps r back to $\mathbf{s}$.

We are ready to construct $\gamma_{d_n}(\Phi^+)$ from which we will create $\widetilde{\gamma}(\rho_{\delta,n})$, along with the assistance of a sublinear amount of entanglement. The construction is as follows

$$\gamma_{d_n}(\Phi^+) = \sum_{r,r'}\frac{1}{d_n}|rr\rangle\langle r'r'|\otimes U_{\mathbf{s}(r)}\rho_{A_SB_S}^{\otimes n}U_{\mathbf{s}(r')}^\dagger \quad (143)$$

where

$$U_{\mathbf{s}(r)} = U_{\mathbf{s}(r)[1]}\otimes\cdots\otimes U_{\mathbf{s}(r)[n]}, \quad (144)$$
$$\mathbf{s}(r) \equiv (\mathbf{s}(r)[1],\ldots,\mathbf{s}(r)[n]), \quad (145)$$
$$\rho_{A_SB_S}^{\otimes n} \equiv \widetilde{\rho}_{A_SB_S}, \quad (146)$$

as given in the definition of the state $\widetilde{\gamma}(\rho_{\delta,n})$.

Due to the above choice of a private state, the proposed protocol only modifies the key part of the involved state, while the shield is prepared in advance in an almost correct form, that is up to the permutation of the local subsystems.

Consider $|\phi\rangle = \sum_{a\in\mathcal{A}}\sqrt{\lambda_a}|e_a\rangle$. We first note that by an isometry between entangled and coherent superposition states, for the $\varepsilon,\delta>0$ and n chosen as above, the following inequality holds [59]

$$\left\|\phi^{\otimes n} - \frac{1}{N}\sum_{\mathbf{s},\mathbf{s}'\in T_n^\delta}|\phi_{\mathbf{s}}\rangle\langle\phi_{\mathbf{s}'}|\right\|_1 \leq \varepsilon, \quad (147)$$

where $\phi_{\mathbf{s}} = \sqrt{\lambda_{\mathbf{s}}}|e_{\mathbf{s}}\rangle$. Next, we will use the typical state $\sigma_{\delta,n}\coloneqq\frac{1}{N}\sum_{\mathbf{s},\mathbf{s}'\in T_n^\delta}|\phi_{\mathbf{s}}\rangle\langle\phi_{\mathbf{s}'}|$.

The Dilution Protocol consists of the steps we define in what follows. In each step $2,\ldots,7$, when a defined action encounters a system in the $\varnothing$ symbol, it is assumed to be defined as an identity operation. However, the situation when the system is in the $\varnothing$ state happens with negligible probability $\leq O(\varepsilon)$. We note that steps 1-6 resemble the coherence dilution protocol from [59]. We give below the steps of the protocol.

1. Alice creates $\phi^{\otimes n}\coloneqq\sum_{\mathbf{s}=0}^{|\mathcal{A}|^n-1}\sqrt{\lambda_{\mathbf{s}}}|e_{\mathbf{s}}\rangle_{A''}$, and transforms it into $\widetilde{\sigma}_{\delta,n}\coloneqq(1-\varepsilon)\sigma_{\delta,n}+\varepsilon|\varnothing\rangle\langle\varnothing|$ by replacing an atypical $\mathbf{s}$ with an error state $|\varnothing\rangle\langle\varnothing|$, which however occurs with probability less than $O(\varepsilon)$.

2. Alice applies a unitary transformation that maps $|e_{\mathbf{s}}\rangle_{A''}$ into $|\mathbf{s}\rangle_{A''}$. Then she performs coherently a classical encoding C based compression algorithm [66] which transforms $\widetilde{\sigma}_{\delta,n}$ into

$$\sigma'_{\delta,n} = (1-\varepsilon)\frac{1}{N}\sum_{c,c'=0}^{d_n-1}\sqrt{\lambda_{\mathbf{s}(c)}\lambda_{\mathbf{s}(c')}}|c\rangle\langle c'|+\varepsilon|\varnothing\rangle\langle\varnothing|, \quad (148)$$

   where c is a codeword of the encoding C, the classical encoding maps $\mathbf{s}\mapsto c$, and $\mathbf{s}(c)=C^{-1}(c)$. On symbol $\varnothing$, the encoding is defined as the identity operation.

3. Alice performs a two-outcome POVM on the system A'' that determines if the system is in the state $|\varnothing\rangle$ or not. If the system A'' is in the state $\varnothing$, Alice publicly communicates this to Bob, and they both replace the system $A'B'$ with the $|\varnothing\varnothing\varnothing\varnothing\rangle_{A_KB_KA_SB_S}$ state, trace out system A'', and stop the Privacy Dilution in a failure state, which happens with probability $\leq O(\varepsilon)$.

   Otherwise, Alice performs the controlled-XOR operation with A'' as the control and the subsystem A_K of $\gamma_{d_n}(\Phi^+)_{A_KA_SB_KB_S}$ as the target. This operation transforms the state $|c\rangle_{A_K}$ into $|c\oplus r\rangle$, with $\oplus$ being a digit-wise addition modulo $|\mathcal{A}|$ operation.

4. Alice measures the system A_K and communicates the result of this measurement $x \equiv c \oplus r$ publicly to Bob.

5. Bob performs the unitary transformation $|x \ominus c\rangle \to |c\rangle$ on system B_K.

6. Alice and Bob coherently apply the inverse of the compression algorithm C, which transforms $|c\rangle$ back into $|\mathbf{s}\rangle$ and $|c'\rangle$ into $|\mathbf{s}'\rangle$, respectively.

7. Alice and Bob perform the algorithms to correct phase errors, i.e., apply IPA$\circ$ PEC$\circ$ PA. Alice traces out system A_K, and Bob traces out the corresponding system holding the state of the message $|x\rangle\langle x|$.

8. Alice changes coherently a basis state $|\mathbf{s}\rangle_{A''}$ into $|e_{\mathbf{s}}\rangle_{A''}$, by applying

$$W_{A''} = \sum_{\mathbf{s}\in T_n^\delta} |e_{\mathbf{s}}\rangle\langle \mathbf{s}| + \sum_{\mathbf{s}\notin T_n^\delta} |\mathbf{s}\rangle\langle \mathbf{s}| + |\varnothing\rangle\langle\varnothing|, \quad (149)$$

while Bob changes $|\mathbf{s}'\rangle_{B_K}$ to $|f_{\mathbf{s}'}\rangle_{B_K}$ analogously.

In the next section, we prove that the resulting state (taking into account an error event) of the Dilution Protocol is equal to $\widetilde{\gamma}_{\delta,n}$ given in (141).

7.5 Correctness of the Privacy Dilution Protocol

We now give a proof of Theorem 3.

Proof of Theorem 3. We comment on the steps of the Privacy Dilution Protocol to show its correctness, thereby proving Theorem 3.

For the sake of readability, we omit in the notation the fact discussed in point 2 that the sequence $\mathbf{s}$ may be atypical, resulting in state $|\varnothing\varnothing\varnothing\varnothing\rangle_{A_K B_K A_S B_S}$. We will assume further that each sequence $\mathbf{s}$ is typical, i.e., belongs to the set T_n^δ.

After the second step, that is, compressing the ancillary state by mapping $\mathbf{s} \mapsto c$ on system A'', the total state of $A''A_K B_K A_S B_S$ systems is

$$\sum_{c,c',r,r'} \frac{1}{d_n} \frac{\sqrt{\lambda_{\mathbf{s}(c)}\lambda_{\mathbf{s}(c')}}}{N} |c\rangle\langle c'| \otimes |rr\rangle\langle r'r'| \otimes U_{\mathbf{s}(r)} \widetilde{\rho}_{A_S B_S} U^\dagger_{\mathbf{s}(r')}, \quad (150)$$

where $d_n = |\mathcal{A}|^{\lceil L(n,\eta)\rceil}$. After the third step, which applies the controlled-XOR operation, the total state of the system is as follows

$$\sum_{c,c',r,r'} \frac{1}{d_n} \frac{\sqrt{\lambda_{\mathbf{s}(c)}\lambda_{\mathbf{s}(c')}}}{N} |c\rangle\langle c'|_{A''} \otimes |r\oplus c, r\rangle\langle r'\oplus c', r'|_{AB} \otimes U_{\mathbf{s}(r)} \widetilde{\rho}_{A_S B_S} U^\dagger_{\mathbf{s}(r')}. \quad (151)$$

After measurement of system A_K in step 4, the state collapses with probability $\frac{1}{d_n}$ to state $|x\rangle\langle x|$ with $x = r\oplus c = r'\oplus c'$ on system A. Since this implies $r = x\ominus c$ and $r' = x\ominus c'$, (where $\ominus$ is the inverse of the modulo-XOR operation $\oplus$, i.e., it adds an opposite element in a group of addition modulo $|\mathcal{A}|$), then after tracing out A_K, the total state on systems $A''B_K A_S B_S$ is

$$\sum_{c,c'} \frac{\sqrt{\lambda_{\mathbf{s}(c)}\lambda_{\mathbf{s}(c')}}}{N} |c\rangle\langle c'|_{A''} \otimes |x\ominus c\rangle\langle x\ominus c'|_{B_K} \otimes U_{\mathbf{s}(x\ominus c)} \widetilde{\rho}_{A_S B_S} U^\dagger_{\mathbf{s}(x\ominus c')}. \quad (152)$$

Further in step 5, Bob, knowing x, transforms $|x\ominus c\rangle\langle x\ominus c'| \equiv |r\rangle\langle r'| \to |c\rangle\langle c'|$ which can be done unitarily by applying $W \equiv \sum_c |c\rangle\langle x\ominus c|$ since $\{|x\ominus c\rangle\}_c$ forms a basis, as does $\{|c\rangle\}_c$. Hence, the total state is as follows

$$\sum_{c,c'} \frac{\sqrt{\lambda_{\mathbf{s}(c)}\lambda_{\mathbf{s}(c')}}}{N} |c\rangle\langle c'|_{A''} \otimes |c\rangle\langle c'|_{B_K} \otimes U_{\mathbf{s}(x\ominus c)} \widetilde{\rho}_{A_S B_S} U^\dagger_{\mathbf{s}(x\ominus c')}. \quad (153)$$

In step 6, both Alice and Bob apply the decompression algorithm, which maps $|c\rangle$ back to $|\mathbf{s}(c)\rangle$ on Alice's side, and $|c'\rangle \mapsto |\mathbf{s}(c')\rangle$ on Bob's side, so the resulting state is

$$\sum_{\mathbf{s},\mathbf{s}'\in T_n^\delta} \frac{\sqrt{\lambda_{\mathbf{s}}\lambda_{\mathbf{s}'}}}{N} |\mathbf{s}\rangle\langle \mathbf{s}'|_{A''} \otimes |\mathbf{s}\rangle\langle \mathbf{s}'|_{B_K} \otimes U_{\beta_x(\mathbf{s})} \widetilde{\rho}_{A_S B_S} U^\dagger_{\beta_x(\mathbf{s}')}, \quad (154)$$

where we identify $\mathbf{s}(c)$ with $\mathbf{s}$ and $\mathbf{s}(c')$ with $\mathbf{s}'$, which is possible due to the bijection between $\mathbf{s}(c)$ and c (and between $\mathbf{s}(c')$ and c'). We also note that the index c, as we show below, is no longer needed in the description of the state. We introduce a function of $\mathbf{s}$ and $\mathbf{s}'$ denoted as β_x instead. To describe this function, we introduce and apply Lemma 7.

The map β_x indicates the pattern of the "phase errors." Indeed, the indices of the key part $\mathbf{s}$ and $\beta_x(\mathbf{s})$ of identifying $U_{\beta_x(\mathbf{s})}$ do not match in general as they should in the state $\widetilde{\gamma}_{\delta,n}$. We would like to perform the mapping β_x^{-1}; however, we need to do it using a negligible amount of private key. In what follows, we will do it by an LOCC operation accompanied by $O(n\delta)$ copies of the singlet state. The latter assistance of entanglement will not alter the overall private key cost of the transformation since we can eventually take the limit $\delta \to 0$.

We now describe the phase-error correction algorithm invoked in Step 7 of the protocol. As a warm-up, let us observe that when $\mathbf{s}$ and $\widehat{\mathbf{s}}$ are of the same type, then for each $\mathbf{s}$ the mapping β_x^{-1} is a permutation $\pi(\mathbf{s})$. Hence in the ideal (yet unreachable) case of $\delta = 0$, it would be enough to define an error-correcting

map $\mathcal{P}_{\text{ideal}}$ as

$$\mathcal{P}_{\text{ideal}} \coloneqq \sum_{\mathbf{s}\in T_n^\delta} |\mathbf{s}\rangle\langle\mathbf{s}|_{A''} \otimes \pi(\mathbf{s})_{A_S}, \tag{155}$$

and the same map for systems $B_K B_S$. However, we need to modify the above map so that it takes care of the fact that the mapping β_x can map $\mathbf{s}$ into a sequence $\widehat{\mathbf{s}}$ that is not of the same type. Fortunately, it is an automorphism, so we control how much the $\mathbf{s}$ and $\beta_x(\mathbf{s})$ sequences differ: for each symbol $a \in \{0,\ldots,|\mathcal{A}|-1\}$ the number of occurrences of a in $\mathbf{s}$ (written as $|a(\mathbf{s})|$) differs from $|a(\widehat{\mathbf{s}})|$ at most by $\lceil 2\delta n\rceil$ (see Lemma 3). We have defined the action of partial inversion of β_x, called Permutation Algorithm (PA), by Algorithm 1 given in Section 7.1.

Let us further denote by $U_{\mathbf{s}_{\text{cor}}}$ a tensor product $\bigotimes_{i=1}^n U_{\mathbf{s}_{\text{cor}}[i]}$ of unitaries corresponding to the sequence $\mathbf{s}_{\text{cor}}$ in a way that, if in position i, there is the symbol a in $\mathbf{s}_{\text{cor}}$, then $U_{\mathbf{s}_{\text{cor}}[i]} = U_a$, and when the symbol $\perp$ is at this position, then $U_{\mathbf{s}_{\text{cor}}[i]} = \mathbb{1}$.

The mapping of the PA can be captured by a transformation of a purification of the state from (154), i.e.,

$$\sum_{\mathbf{s}\in T_n^\delta} \sqrt{\frac{\lambda_{\mathbf{s}}}{N}} |\mathbf{ss}\rangle (U_{\beta_x(\mathbf{s})} \otimes \mathbb{1}_E) |\chi^{\otimes n}\rangle_{A_S B_S E} \tag{156}$$

(where $|\chi\rangle_{A_S B_S E}$ is a purification of the state $\widetilde{\rho}_{A_S B_S}$ to system E) into a state

$$\begin{aligned}
&\sum_{\mathbf{s}\in T_n^\delta} \sqrt{\frac{\lambda_{\mathbf{s}}}{N}} |\mathbf{ss}\rangle_{A_K B_K} (U_{\mathbf{s}_{\text{cor}}} \otimes U_{\widehat{\mathbf{s}}[q_1]} \otimes \cdots \otimes U_{\widehat{\mathbf{s}}[q_{f(\mathbf{s})}]} \otimes \\
&\mathbb{1}_{f(\mathbf{s})+1} \otimes \cdots \otimes \mathbb{1}_{L_{\max}} \otimes \mathrm{I}_E) |\widetilde{\chi}\rangle \\
&\Big[\widetilde{A}_{S\mathbf{s}_{\text{cor}}}, T_{A_S}[1:f(\mathbf{s})], T^{\perp}_{A_S}[f(\mathbf{s})+1:L_{\max}] \\
&\widetilde{B}_{S\mathbf{s}_{\text{cor}}}, T_{B_S}[1:f(\mathbf{s})], T^{\perp}_{B_S}[f(\mathbf{s})+1:L_{\max}] E\Big] .
\end{aligned} \tag{157}$$

In the above for ease of reading we identify $\widetilde{|\chi\rangle}_Y$ with $\widetilde{|\chi\rangle}[Y]$. We also added a $\perp$ symbol in superscript in $T^{\perp}_{A_S}[f(\mathbf{s})+1:L_{\max}]$ to keep in mind that particular systems are in the $|\perp\rangle$ state. By $\widetilde{|\chi\rangle}$ we mean the purification of the shield systems such that whenever $\mathbf{s}_{\text{cor}}[i] = \perp$, the state $|\chi_i\rangle$ (i.e., the i-th subsystem of $|\chi\rangle$) is meant to be the purification of the state $|\perp\perp\rangle_{A_S B_S}$ to the system E. If this is not the case, the i-th subsystem of $|\chi\rangle$ equals the purification of the state $\rho_{A_S B_S}$. We have also omitted the systems $A_S B_S[1\ldots n]$ as they are in the state $|\perp\rangle^{\otimes n}$. Moreover, $U_{\widehat{\mathbf{s}}[j_k]}$ are unitaries whose indices do not match the index of the key at position i_k in $|\mathbf{s}\rangle_{A_K}$ (reflecting the phase error). The $L_{\max} - f(\mathbf{s})$ systems $T_{A_S}[f(\mathbf{s})+1]\cdots T_{A_S}[L_{\max}]$ are in the state $|\perp\rangle$.

Next, the PEC procedure described in Algorithm 2 is executed. It begins by teleporting to Bob the $L_{\max}$ states of the systems

$$A_S[j_1]\cdots A_S[j_{f(\mathbf{s})}]\,|\perp\rangle_{j_{f(\mathbf{s})}+1}\cdots|\perp\rangle_{L_{\max}}, \tag{158}$$

which are now stored in system T_{A_S}. There are $f(\mathbf{s})$ "phase errors". Namely for $k = 1,\ldots,f(\mathbf{s})$ the p_k are the positions for which $\mathbf{s}_{\text{cor}}$ has $|\perp\rangle$, indicating that $\mathbf{s}[i_k] \neq \widehat{\mathbf{s}}[j_k]$ at this position. In other words, at position i_k the key system has symbol $\mathbf{s}[i_k]$, while $U_{\widehat{\mathbf{s}}[j_k]}$ is performed on $T_{A_S B_S}[k]$ instead of $U_{\mathbf{s}[i_k]}$. For this reason Bob performs controlled-unitary operations τ_1^{PEC} and τ_2^{PEC} to correct these errors on systems

$$T_{A_S}[1]\cdots T_{A_S}[f(\mathbf{s})] T_{B_S}[1]\cdots T_{B_S}[f(\mathbf{s})],$$

leaving systems

$$T_{A_S}[f(\mathbf{s})+1]\cdots T_{A_S}[L_{\max}], T_{B_S}[f(\mathbf{s})+1]\cdots T_{B_S}[L_{\max}]$$

untouched. Indeed, this is what PEC does. The unitary τ_1^{PEC} undoes the action of $U_{\widehat{s}[j_k]}$ on system j_k for each $k = 1,\ldots,f(\mathbf{s})$, leaving these systems in state $\rho_{A_S B_S}$ each. Further τ_2^{PEC} rotates the latter states by appropriate unitaries U_a demanded by symbols $\mathbf{s}[i_k] = a$ for each k. Bob further teleports back the systems that he got from Alice. After the phase errors are corrected, the state of (157) gets transformed into the following form

$$\begin{aligned}
&\sum_{\mathbf{s}\in T_n^\delta} \sqrt{\frac{\lambda_{\mathbf{s}}}{N}} |\mathbf{ss}\rangle_{A_K B_K} (U_{\mathbf{s}_{\text{cor}}} \otimes U_{\mathbf{s}[p_1]} \otimes \cdots \otimes U_{\mathbf{s}[p_{f(\mathbf{s})}]} \otimes \\
&\mathbb{1}_{f(\mathbf{s})+1} \otimes \cdots \otimes \mathbb{1}_{L_{\max}} \otimes \mathbb{1}_E) |\widetilde{\chi}\rangle \\
&\Big[\widetilde{A}_{S\mathbf{s}_{\text{cor}}}, T_{A_S}[1:f(\mathbf{s})], T^{\perp}_{A_S}[f(\mathbf{s})+1:L_{\max}] \\
&\widetilde{B}_{S\mathbf{s}_{\text{cor}}}, T_{B_S}[1:f(\mathbf{s})], T^{\perp}_{B_S}[f(\mathbf{s})+1:L_{\max}] E\Big]
\end{aligned} \tag{159}$$

where the only difference (apart from the different state of the auxiliary systems that we discuss shortly) is that instead of incorrect $U_{\widehat{\mathbf{s}}[i]}$ there comes $U_{\mathbf{s}[i]}$ which are correct "phases." Performing PA involves borrowing the auxiliary systems $\widetilde{A}_S, T_{A_S} S_{\text{out}}$, as well as the ones needed to produce $\widehat{S}$ and its copy $\widehat{S}_1$. Then, there comes the Inverting PA (IPA) procedure, the task of which is to (i) put back the corrected shielding systems as well as the accompanying correct ones from $\widetilde{A}_S T_{A_S} T_{B_S}$ to $A_S B_S[1\ldots n]$ systems, (ii) uncompute the auxiliary systems $\widehat{S}$ and $\widehat{S}_1$ to their original state $|0\rangle$ of the initial dimension. The first task of IPA is rather complicated since it has to rearrange coherently the entries corrected by the PEC algorithm and conserve the order of the remaining ones. This procedure is performed in a control-target manner, where control is on systems $\mathbf{s}_{\text{cor}}$ and C. The former system identifies when the SWAP operation should be applied, while the latter identifies which part of T_{A_S} should be swapped. Section 7.3 provides an extensive description of this procedure. On the other hand, the second task of IPA is simple since it is completed by applying the inverse of the twisting τ_{key}^{PA}, i.e., $\tau_{\text{key}}^{PA\dagger}$. Further, the $U_{\beta_x}^\dagger$ applied twice uncomputes $\widehat{S}$ to a state of the systems A, which is then

uncopied by CNOT operations. Finally, the systems $\widehat{S}_1^A \widehat{S}_1^B S_{\text{out}}^A S_{\text{out}}^B \widetilde{A}_S T_{A_S} \widetilde{B}_S T_{B_S}$ are then traced out in their original state. The resulting state is

$$\sum_{\mathbf{s}\in T_n^\delta} \sqrt{\frac{\lambda_{\mathbf{s}}}{N}} |\mathbf{ss}\rangle_{A_K B_K} U_{\mathbf{s}} \otimes \mathbb{1}_E |\chi\rangle_{A_S B_S E}. \tag{160}$$

The auxiliary systems were traced out in their original state. Hence, this tracing out of auxiliary systems does not disclose any further knowledge to Eve about the above state.

We have then demonstrated explicitly, by constructing the operations of the Dilution Protocol, that they are a composition of twisting unitary operations, teleportation of a state whose dimension is independent of the value of the key, and giving back the auxiliary systems in their original state. Since the teleported system is also teleported back, we can consider their composition as an identity operation on the state. Since the states of auxiliary systems are returned to their original state, and the protocol transforms $A_K B_K A_S B_S[1 \dots n]$ back to the desired state, there is no security leakage when we trace out the auxiliary systems.

We note here that mapping of Step 8 of the Dilution Protocol given in Sec. 7.4, i.e., $|\mathbf{s}\rangle_{A_K} \to |e_{\mathbf{s}}\rangle_{A_K}$ on Alice's key part and $|\mathbf{s}\rangle_{B_K} \to |f_{\mathbf{s}}\rangle_{B_K}$ on Bob's one, can also be done by local unitary transformations.

Finally, we observe that the system A_K, which is communicated by Alice to Bob publicly, is initially correlated with the shielding system: $|x\rangle\langle x| \otimes U_{\beta_x(\mathbf{s})} \widetilde{\rho}_{A_S B_S} U_{\beta_x(\mathbf{s})}^\dagger$. However, after the protocol is done in Step 8, the function β_x is inverted: for every $\mathbf{s}$ on shield there is $U_{\mathbf{s}}(\widetilde{\rho}_{A_S B_S}) U_{\mathbf{s}}^\dagger$. Hence, the shielding systems become independent from $|x\rangle\langle x|_{A_K}$, and the total output state is in the desired form. Note here that the parties trace out the systems holding information about $|x\rangle\langle x|$ only at the end of the protocol since the PA procedure uses this register to perform U_{β_x}. To summarize, the resulting state of the protocol is in the desired form of the approximate twisted typical subspace of the state $|\psi\rangle^{\otimes n}$. Due to (140), we have obtained a state that approximates another, which is locally equivalent to $\gamma(\psi)^{\otimes n}$. This concludes the proof of the correctness of the Privacy Dilution protocol described above and in Theorem 3. □

Lemma 7. *The map $\beta_x : T_n^\delta \to T_n^\delta$ defined on a sequence $\mathbf{s}(c)$ as $\beta_x(\mathbf{s}(c)) = \widehat{\mathbf{s}} \equiv \mathbf{s}(x \ominus c)$ is a bijection given by the following formula*

$$\beta_x := C^{-1} \circ R^{-1} \circ \ominus_{|\mathcal{A}|} \circ X_- \circ C, \tag{161}$$

where the X_- map subtracts x digit-wise modulo $|\mathcal{A}|$ and $\ominus_{|\mathcal{A}|}$ takes a digit-wise opposite number modulo $|\mathcal{A}|$, i.e., such that together they add to 0 modulo $|\mathcal{A}|$.

Proof. First, by the definition of the notation $\mathbf{s}(r)$, for $\widehat{r} := x \ominus c$ the bijection $C^{-1} \circ R^{-1}$ maps $\widehat{r}$ to $\mathbf{s}(x \ominus c)$ (via some c' not necessarily equal to c, see diagram below). On the other hand, we can bijectively reconstruct the string $\mathbf{s}(c)$ from $\widehat{r}$. We do so by first obtaining from $\widehat{r}$ the string $\widetilde{r} = c \ominus x$, i.e., the opposite number to $x \ominus c$, which is done by the map $\ominus_{|\mathcal{A}|}$. We compose it by adding x mod $|\mathcal{A}|$, i.e., with the map X_+ that results in $c(\mathbf{s})$. We finally compose the latter maps with C^{-1} to obtain $\mathbf{s}(c)$. Now, by inverting the last sequence of bijections, i.e., getting $\ominus_{|\mathcal{A}|} \circ X_- \circ C$ (note that $\ominus_{|\mathcal{A}|}$ is self-inverse), we obtain bijective mapping from $\mathbf{s}$ to $\widehat{r}$. Composing the latter bijection with $C^{-1} \circ R^{-1}$ we obtain the β_x given in (161). The action of the β_x bijection can be captured through the following diagram

$$\begin{array}{ccccc} \mathbf{s}(x \ominus c) & \underset{C^{-1}}{\overset{C}{\rightleftarrows}} & c' & \underset{R^{-1}}{\overset{R}{\rightleftarrows}} & \hat{r} = x \ominus c \\ {\scriptstyle \beta_x}\uparrow\downarrow{\scriptstyle \beta_x^{-1}} & & & & \updownarrow{\scriptstyle \ominus_{|\mathcal{A}|}} \\ \mathbf{s}(c) & \underset{C^{-1}}{\overset{C}{\rightleftarrows}} & c & \underset{X_+}{\overset{X_-}{\rightleftarrows}} & c \ominus x \end{array}$$

This concludes the proof. □

Remark 3. *We have designed a privacy dilution protocol that transforms an ideal private state into a generalized private state by LOCC. Our protocol uses at least $o(1)$ rate of privacy in the form of pure entanglement. It remains open to determine if pure entanglement is actually needed for this task. It is worth noticing that whenever the twisting unitaries, U_a, are incoherent operations (composition of incoherent gates), then the DP can be completed by incoherent operations [85].*

8 Regularized key of formation upper bounds key cost

We now show that the regularized key of formation is an upper bound on the key cost. For ease of writing, we will make use of the following definition.

Definition 6. *A private state $\gamma(\Phi^+)$ is θ-related to a generalized private state $\gamma(\phi)$ if there exists $n \in \mathbb{Z}^+$ such that from $\gamma(\Phi^+)$ one can create $\gamma(\phi)^{\otimes n}$ by LOCC, up to an error θ in trace distance. For ease of writing, we sometimes omit θ whenever irrelevant or known from the context.*

Let us note here that for each generalized private state $\gamma(\psi)$ and $\theta > 0$ there exists a private state θ-related to $\gamma(\psi)$, as assured by Theorem 3. We are ready to state the main result of this section.

Theorem 4. *For every bipartite state ρ_{AB},*

$$K_F^\infty(\rho_{AB}) \geq K_C(\rho_{AB}). \tag{162}$$

Proof. Let $\{(p_i, \gamma(\psi_i))\}_{i=1}^k$ be an optimal ensemble for K_F. For this part of the proof, we assume that K_F is attained on a finite ensemble with k elements.

By Lemma 1, we have that $k \leq (|\mathcal{A}| \times |\mathcal{B}|)^2 + 1$. The case when it is not attained will be considered later as a small modification of what follows. To prove the inequality, we first note, following [35], that by typicality arguments, for all $\varepsilon, \delta_0 > 0$ and sufficiently large n, we have that

$$\rho^{\otimes n} \approx_\varepsilon \rho_n \equiv \sum_{\mathbf{s}\in T_n^{\delta_0}} p_{\mathbf{s}} \gamma(\psi_{\mathbf{s}[1]}) \otimes \gamma(\psi_{\mathbf{s}[2]}) \otimes \cdots \otimes \gamma(\psi_{\mathbf{s}[n]}). \tag{163}$$

The latter state is locally unitarily equivalent to

$$\widetilde{\rho}_n \equiv \sum_{\mathbf{s}\in T_n^{\delta_0}} p_{\mathbf{s}} \gamma(\psi_{\mathbf{s}}), \tag{164}$$

where the string $\mathbf{s}$ belongs to a strongly typical set $T_n^{\delta_0}$ with a property that it contains each state $\gamma(\psi_i)$, at least $\lfloor p_i n - \delta_0 p_i n \rfloor$ and at most $\lceil p_i n + \delta_0 p_i n \rceil$ times. We note that δ_0 can be arbitrarily small for sufficiently large n.

Let us now fix $\mathbf{s} \in T_n^{\delta_0}$. Then $\gamma(\psi_{\mathbf{s}})$ is such that each state $\gamma(\psi_i)$ in $\gamma(\psi_{\mathbf{s}})$ occurs $l_i(n) \in \mathbb{N}$ times, which satisfies

$$\lfloor p_i n - \delta_0 p_i n \rfloor \leq l_i(n) \leq \lceil n p_i + \delta_0 p_i n \rceil. \tag{165}$$

We aim to create an approximate version of $\gamma(\psi_{\mathbf{s}})$.

We will do it using a sub-protocol that has access to a private state $\gamma_{d_n(i)}(\Phi^+)$ ε_i-related to $\gamma(\psi_i)$; this sub-protocol will create an ε_i-approximation of the latter state. For the sake of this proof, it suffices to set $\varepsilon_i = \varepsilon$. We also set $\delta_i > 0$ arbitrarily for $i \in \{1, \dots k\}$. As noted, the existence of $\gamma_{d_n(i)}(\Phi^+)$ is assured by Theorem 3. More precisely, given sufficiently large n we will obtain sufficiently large $d_n(i)$ satisfying

$$\log d_n(i) = \lceil l_i(n) \times (S(A_K)_{\psi_i} + \eta_i + 2\delta_i) \rceil, \tag{166}$$

(where $\eta_i = \delta_i S(A_K)_{\psi_i}$) such that the Dilution Protocol described in Section 7 creates from $\gamma_{d_n(i)}(\Phi^+)$ a state that ε_i-approximates in trace norm $\gamma(\psi_i)^{\otimes l_i(n)}$. Let us denote this protocol as $\mathcal{P}_i$.

We note here that due to the definition of K_F, each $\gamma(\psi_i)$ is strictly irreducible. Hence by (143), $\gamma_{d_n(i)}(\Phi^+)$ is also a strictly irreducible private state. Thus, using $\mathcal{P}_i$ as a subroutine, we will create ρ_{AB} from a strictly irreducible private state, as demanded by the definition of K_C.

Performing protocol $\mathcal{P}_i$ for each $i \in [k]$, by the triangle inequality, we obtain $\gamma_{\approx}(\psi_{\mathbf{s}})$ that is a $\theta := \sum_i \varepsilon_i$-approximation of the state

$$\bigotimes_{i=1}^{k} \gamma(\psi_i)^{\otimes l_i(n)}. \tag{167}$$

Let us note here that the actual amount of key needed to create $\gamma_{\approx}(\psi_{\mathbf{s}})$ varies depending on the value of $\mathbf{s}$, due to fluctuations of the number of occurrences of states $\gamma(\psi_i)$, i.e., $l_i(n)$ in sequence $\mathbf{s}$. However, by definition of K_C, we need a *single* private state from which we can create our target state given in (164). We will therefore choose a private state with an amount of key exceeding K_F by a vanishing factor (proportional to $\delta_0 \times K_F \leq \delta_0 d_{AB}$ by a vanishing constant) which will be ready for the worst-case (the largest) amount of key needed to create $\gamma_{\approx}(\psi_{\mathbf{s}})$. Namely, we will define a private state which is $O(\epsilon)$-related to $\gamma(\psi_{\mathbf{s}})$ for *every* δ_0-strongly typical $\mathbf{s}$.

To achieve this task, we choose $\gamma_{d_n^*}(\Phi^+)$ to be a private state θ-related to a generalized private state of the form

$$\gamma^+ := \bigotimes_{i=1}^{k} \gamma(\psi_i)^{\otimes l_i(n)^+}. \tag{168}$$

The dimension d_n^* of the key part of $\gamma_{d_n^*}(\Phi^+)$ satisfies

$$\log_2 d_n^* := \sum_{i=1}^{k} \lceil l_i(n)^+ \times (S(A_K)_{\psi_i} + \eta_i + 2\delta_i) \rceil, \tag{169}$$

where

$$l_i(n)^+ := \lceil n p_i + \delta_0 p_i n \rceil. \tag{170}$$

We focus on this case, as the above state uses the largest private key. Intuitively, it can allow for the creation of $\gamma_{\approx}(\psi_{\mathbf{s}})$ for any other δ_0-typical $\mathbf{s} \neq \mathbf{s}_0$ by performing partial trace operations if less key is needed to produce $\gamma(\psi_{\mathbf{s}})$.

To finalize the procedure of creating an approximate version of $\gamma(\psi_{\mathbf{s}})$, we need to permute locally (in the same way for Alice and Bob) subsystems of $\widetilde{\gamma}_{\approx}(\psi_{\mathbf{s}})$ by some permutation $\pi_{\mathbf{s}}$, defined as

$$\mathbf{s}_0 \equiv (\underbrace{1 \dots 1}_{l_1(n) \text{ times}}, \underbrace{2 \dots 2}_{l_2(n) \text{ times}}, \dots, \underbrace{k \dots k}_{l_k(n) \text{ times}}) \to \mathbf{s}. \tag{171}$$

We are ready to formalize the protocol $\mathcal{P}$, which takes as input $\gamma_{d_n^*}(\Phi^+)$ and outputs an approximation of $\widetilde{\rho}_n = \sum_{\mathbf{s}\in T_n^{\delta_0}} p_s \gamma(\psi_{\mathbf{s}})$. It consists of the following steps:

1. Draw $\mathbf{s}$ at random with probability $p_{\mathbf{s}}$ in order to produce an approximation of $\gamma(\psi_{\mathbf{s}})$ from the related private state $\gamma_{d_n^*}(\Phi^+)$.
2. For each $i \in [k]$, apply $\mathcal{P}_i$ to produce a θ-approximation $\gamma_{\approx}^+(\psi_{\mathbf{s}})$ of the state γ^+.
3. If $\mathbf{s} \neq \mathbf{s}_0$, trace out some of the subsystems of $\gamma_{\approx}^+(\psi_{\mathbf{s}})$ to obtain the θ-approximation $\gamma_{\approx}(\psi_{\mathbf{s}})$ of
$$\bigotimes_{i=1}^{k} \gamma(\psi_i)^{\otimes l_i(n)}. \tag{172}$$
4. If $\mathbf{s} \neq \mathbf{s_0}$, apply the permutation $\pi_{\mathbf{s}}$ to the local subsystems of $\gamma_{\approx}(\psi_{\mathbf{s}})$ to create a θ-approximation of $\gamma(\psi_{\mathbf{s}})$.

5. Erase the symbol $\mathbf{s}$, producing a mixed state over typical labels $\mathbf{s}$.

By construction, the above protocol $\mathcal{P}$ creates a θ-approximation of the state $\widetilde{\rho}_n$, which is locally unitarily equivalent to ρ_n given in (163). Let $V \equiv V_A \otimes V_B$ denote the unitary transforming $\widetilde{\rho}_n$ into ρ_n. Now, by the triangle inequality, the construction of $\mathcal{P}$, and (163), we obtain

$$\begin{aligned}
&\left\|V\mathcal{P}(\gamma_{d_n^*}(\Phi^+))V^\dagger - \rho^{\otimes n}\right\|_1 \\
&\leq \left\|V\mathcal{P}(\gamma_{d_n^*}(\Phi^+))V^\dagger - \rho_n\right\|_1 + \left\|\rho^{\otimes n} - \rho_n\right\|_1 \quad (173)\\
&\leq \theta + \varepsilon, \quad (174)
\end{aligned}$$

for sufficiently large n. We note here that without loss of generality $\varepsilon + \theta \leq (k+1)\varepsilon \leq \varepsilon(d_{AB}^2+1)$ (see Lemma 1).

Since V is local, $\mathcal{P}' \equiv V \circ \mathcal{P}$ is an LOCC protocol that creates an approximation of $\rho_{AB}^{\otimes n}$, using $\log d_n^*$ bits of private key. Hence, its rate is an upper bound on K_C. We now compute the latter rate. As we will see, it asymptotically reaches the value of $K_F(\rho_{AB})$.

In total, the rate of the protocol $\mathcal{P}'$ is

$$\begin{aligned}
&\frac{\log_2 d_n^*}{n} \\
&= \frac{1}{n}\sum_{i=1}^k \left\lceil l_i^+(n)[S(A_K)_{\psi_i} + \eta_i + 2\delta_i]\right\rceil \quad (175)\\
&\leq \frac{1}{n}\sum_{i=1}^k l_i^+(n)[S(A_K)_{\psi_i} + \eta_i + 2\delta_i] + \frac{k}{n} \quad (176)\\
&\leq \sum_{i=1}^k \frac{l_i^+(n)}{n}[S(A_K)_{\psi_i} + \eta_i + 2\delta_i] + \frac{d_{AB}^2+1}{n} \quad (177)\\
&\leq \sum_{i=1}^k p_i(1+\delta_0)[S(A_K)_{\psi_i} + \eta_i + 2\delta_i] \\
&\quad + \frac{k[S(A_K)_{\psi_i} + \eta_i + 2\delta_i]}{n} + \frac{d_{AB}^2+1}{n} \quad (178)\\
&\leq \sum_{i=1}^k p_i(1+\delta_0)[S(A_K)_{\psi_i} + \eta_i + 2\delta_i] \\
&\quad + \frac{(d_{AB}^2+1)(\log(d_{AB})+3)}{n} + \frac{d_{AB}^2+1}{n} \quad (179)\\
&\to_{n\to\infty} \sum_{i=1}^k p_i(1+\delta_0)[S(A_K)_{\psi_i} + 2\delta_i + \eta_i] \quad (180)\\
&= (1+\delta_0)\sum_{i=1}^k p_i S(A_K)_{\psi_i} + (1+\delta_0)\sum_{i=1}^k p_i(\eta_i + 2\delta_i) \quad (181)\\
&= \sum_{i=1}^k p_i S(A_K)_{\psi_i} + \delta_0 \sum_{i=1}^k p_i S(A_K)_{\psi_i} \\
&\quad + (1+\delta_0)\sum_{i=1}^k p_i(\eta_i + 2\delta_i) \quad (182)\\
&= K_F(\rho_{AB}) + \delta_0 \sum_{i=1}^k p_i S(A_K)_{\psi_i} \\
&\quad + (1+\delta_0)\sum_{i=1}^k p_i(\eta_i + 2\delta_i). \quad (183)
\end{aligned}$$

In the above, the first inequality is by an upper bound by 1 to each $\lceil . \rceil$ term. Next, we bound k from above by d_{AB}^2+1 by Lemma 1. Further, we upper bound the $\lceil . \rceil$ in the definition of each $l_i^+(n)$ and upper bound the term $S(A_K)_{\psi_i} + \eta_i + 2\delta_i$ by $\log d_{AB} + 3$ by noting that local entropy cannot exceed the logarithm of the local dimension, and without loss of generality, η_i, δ_i can be considered as ≤ 1. We finally take the limit of large n and reorder terms.

We have proven then, that for all $\varepsilon > 0$, there exists a sufficiently large $N \in \mathbb{N}$ such that for each $n > N$, a private state $\gamma_{d_n^*}(\Phi^+)$ and a LOCC protocol $\mathcal{P}'$ producing, by acting on the latter state, an output state that is at least $(d_{AB}^2+1)\varepsilon$-close in trace norm to $\rho^{\otimes n}$. Moreover, since $K_C^\varepsilon(\rho_{AB}^{\otimes n})$ is by definition the infimum over such protocols, then $(1/n)K_C^\varepsilon(\rho_{AB}^{\otimes n}) \leq \frac{\log_2 d_n^*}{n}$. Combining it with the latter chain of inequalities, we obtain

$$\begin{aligned}
&\limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho_{AB}^{\otimes n}) \\
&\leq \limsup_{n\to\infty} \frac{\log_2 d_n^*}{n} \quad (184)\\
&\leq K_F(\rho_{AB}) + \delta_0 \sum_{i=1}^k p_i S(A_K)_{\psi_i} \\
&\quad + (1+\delta_0)\sum_{i=1}^k p_i(\eta_i + 2\delta_i). \quad (185)
\end{aligned}$$

This holds for arbitrarily small $\delta_i > 0$ (so as η_i, since $\eta_i = \delta_i S(A_K)_{\psi_i}$) $(i = 0, \ldots k)$. Hence

$$\limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho_{AB}^{\otimes n}) \leq K_F(\rho_{AB}). \quad (186)$$

But this holds true for each $\varepsilon > 0$, and so $K_C(\rho_{AB}) \leq K_F(\rho_{AB})$.

The latter inequality is proved under the assumption that K_F is attained by an ensemble of k generalized private states with k. If it is not the case, then K_F is by the definition of the infimum is a limit of quantities $\sum_{i=1}^{k(m)} p_i^{(m)} S_{A_K}(\gamma(\psi_i)^{(m)})$ with $k(m) \leq d_{AB}^2 + 1$ (see Lemma 1) and $m \to \infty$. We can then fix $\kappa > 0$ arbitrarily small for which there exists t_0 such that $K_F(\rho_{AB}) + \kappa = \sum_{i=1}^{k(t_0)} p_i^{(t_0)} S_{A_K}(\gamma(\psi_i)^{(t_0)})$, and prove by the above argument that $K_F + \kappa \geq K_C$. Since this holds for every $\kappa > 0$, we have $K_F \geq K_C$ in general (without assumption about the attainability of the infimum in the definition of K_F).

By analogy with [35], the same argument as above proves $K_F(\rho_{AB}^{\otimes t})/t \geq K_C(\rho_{AB}^{\otimes t})/t$ for every finite, fixed positive integer $t \in \mathbb{Z}^+$. Since K_C is additive, i.e. $K_C(\rho_{AB}^{\otimes t}) = tK_C(\rho_{AB})$ (see Lemma 8), then

$$\lim_{t\to\infty} \frac{1}{t} K_F(\rho_{AB}^{\otimes t}) \geq \lim_{t\to\infty} \frac{1}{t} K_C(\rho_{AB}^{\otimes t}) \quad (187)$$

$$= \lim_{t\to\infty} \frac{1}{t} t K_C(\rho_{AB}) \tag{188}$$
$$= K_C(\rho_{AB}). \tag{189}$$

So we have proved that $K_F^\infty(\rho_{AB}) \geq K_C(\rho_{AB})$. We have used above the fact, that K_C is additive on tensor product of a bipartite state. We prove this below, partially in the spirit of the proof for distillable entanglement given in [82]. □

Lemma 8. *K_C is additive; i.e., for every positive integer $r \in \mathbb{Z}^+$,*

$$K_C(\rho^{\otimes r}) = r K_C(\rho). \tag{190}$$

Proof.

$$K_C(\rho^{\otimes r}) = \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes nr}) \tag{191}$$
$$= r \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{rn} K_C^\varepsilon(\rho^{\otimes nr}) \tag{192}$$
$$= r K_C(\rho). \tag{193}$$

The second equality holds by the next lemma. □

Lemma 9. *For each $r \in \mathbb{Z}^+$, the following equality holds*

$$\sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}) = \sup_{\varepsilon\in(0,1)} \limsup_{n\to\infty} \frac{1}{rn} K_C^\varepsilon(\rho^{\otimes nr}). \tag{194}$$

Proof. Let $\varepsilon > 0$. Since $\{rn\}_n$ is a subsequence of a sequence $\{n\}_n$, then

$$\limsup_{n\to\infty} \frac{1}{rn} K_C^\varepsilon(\rho^{\otimes nr}) \leq \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}). \tag{195}$$

We will show by contradiction that the converse inequality holds. Assume that there exists $M > 0$ such that

$$\eta_{\text{sup}}^r := \limsup_{n\to\infty} \frac{1}{rn} K_C^\varepsilon(\rho^{\otimes nr}) \tag{196}$$
$$< M < \limsup_{n\to\infty} \frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}). \tag{197}$$

Let $0 < \varepsilon_1 < (M - \eta_{\text{sup}}^r)/2$. From the definition of the limit superior, there exists N such that, for all $m \in \mathbb{Z}^+$ and $n := r \cdot m > N$,

$$\frac{1}{n} K_C^\varepsilon(\rho^{\otimes n}) \leq \eta_{\text{sup}}^r + \varepsilon_1 < M. \tag{198}$$

Let us denote as $\{\overline{n}_k\}_k$, with $\overline{n}_k > N$, a sequence of all indices such that

$$M < \frac{1}{\overline{n}_k} K_C^\varepsilon(\rho^{\otimes \overline{n}_k}). \tag{199}$$

Observe that for each $\overline{n}_k$ there exists $s_k \leq r$ such that $\overline{n}_k + s_k = r \cdot l =: \underline{n}_k > N$. This defines a subsequence $\{\underline{n}_k\}_k$ for which

$$\left| \frac{1}{\underline{n}_k} K_C^\varepsilon(\rho^{\otimes \underline{n}_k}) - \eta_{\text{sup}}^r \right| \leq \varepsilon_1. \tag{200}$$

We can choose then a subsequence $\{\underline{n}_{k_l}\}_l$ such that

$$\eta := \lim_{l\to\infty} \frac{1}{\underline{n}_{k_l}} K_C^\varepsilon(\rho^{\otimes \underline{n}_{k_l}}) \leq \eta_{\text{sup}}^r + \varepsilon_1 < M, \tag{201}$$

and also choose the corresponding subsequence $\{\overline{n}_{k_l}\}_l$. For simplicity, from now on we will denote $\{\underline{n}_{k_l}\}_l$ as $\{i_k\}$ and $\{\overline{n}_{k_l}\}_l$ as $\{n_k\}_k$.

Now we summarize the current construction and reduce redundancy in the notation. We chose two precisely prepared subsequences $\{n_k\}_k$, $\{i_k\}_k$ such that

$$\forall_k\, i_k = n_k + s_k, \quad s_k \leq r, \tag{202}$$
$$\forall_k\, \frac{1}{i_k} K_C^\varepsilon(\rho^{\otimes i_k}) < \eta_{\text{sup}}^r + \varepsilon_1 < M < \frac{1}{n_k} K_C^\varepsilon(\rho^{\otimes n_k}), \tag{203}$$
$$\lim_{k\to\infty} \frac{1}{i_k} K_C^\varepsilon(\rho^{\otimes i_k}) \text{ (denoted as } \eta) \leq \eta_{\text{sup}}^r + \varepsilon_1. \tag{204}$$

Now we can write $\rho^{\otimes i_k} = \rho^{\otimes n_k} \otimes \rho^{\otimes s_k}$. Since K_C^ε is an infimum over $\Lambda \in \text{LOCC}$ and $\gamma_d \in \text{SIR}$, then for each $\delta_{i_k} > 0$ there exist $\Lambda_{i_k} \in \text{LOCC}$, $\gamma_{d_{i_k}}$ such that $\Lambda_{i_k}(\gamma_{d_{i_k}}) \approx_\varepsilon \rho^{\otimes i_k}$ and

$$\frac{1}{i_k} K_C^\varepsilon(\rho^{\otimes i_k}) + \delta_{i_k} \geq \frac{\log d_{i_k}}{i_k}. \tag{205}$$

But Λ_{i_k}, composed with a partial trace that will trace out s_k redundant systems, is an LOCC protocol Λ_{n_k} such that $\Lambda_{n_k}(\gamma_{d_{i_k}}) \approx_\varepsilon \rho^{\otimes n_k}$. Since it is a particular protocol, then we have

$$\frac{\log d_{i_k}}{n_k} \geq \frac{1}{n_k} K_C^\varepsilon(\rho^{\otimes n_k}). \tag{206}$$

Combining above inequalities we obtain

$$K_C^\varepsilon(\rho^{\otimes i_k}) + i_k \delta_{i_k} \geq \log d_{i_k} \geq K_C^\varepsilon(\rho^{\otimes n_k}). \tag{207}$$

But this holds true for all $\delta_{i_k} > 0$, so we conclude that

$$K_C^\varepsilon(\rho^{\otimes i_k}) \geq K_C^\varepsilon(\rho^{\otimes n_k})$$
$$\frac{1}{n_k} K_C^\varepsilon(\rho^{\otimes i_k}) \geq \frac{1}{n_k} K_C^\varepsilon(\rho^{\otimes n_k}), \tag{208}$$

which is true for all k. Combining (204), (208) and (202) we obtain

$$\frac{1}{i_k - s_k} K_C^\varepsilon(\rho^{\otimes i_k}) \geq \frac{1}{n_k} K_C^\varepsilon(\rho^{\otimes n_k}) > \frac{1}{i_k} K_C^\varepsilon(\rho^{\otimes i_k}). \tag{209}$$

It only remains to observe that

$$\left(\frac{1}{i_k - s_k} K_C^{\varepsilon}(\rho^{\otimes i_k}) - \frac{1}{i_k} K_C^{\varepsilon}(\rho^{\otimes i_k})\right) = \frac{s_k}{i_k - s_k}\left(\frac{1}{i_k} K_C^{\varepsilon}(\rho^{\otimes i_k})\right) \to 0 \cdot \eta = 0 \quad (210)$$

as $k \to \infty$. So by the sandwich rule

$$\lim_{k\to\infty} \frac{1}{n_k} K_C^{\varepsilon}(\rho^{\otimes n_k}) \leq \eta_{\text{sup}}^r + \varepsilon_1 < M \quad (211)$$

$$< \frac{1}{n_k} K_C^{\varepsilon}(\rho^{\otimes n_k}) \quad \forall_k, \quad (212)$$

which is a contradiction. So

$$\limsup_{n\to\infty} \frac{1}{rn} K_C^{\varepsilon}(\rho^{\otimes nr}) \geq \limsup_{n\to\infty} \frac{1}{n} K_C^{\varepsilon}(\rho^{\otimes n}) \quad (213)$$

for each $\varepsilon > 0$. □

Remark 4. *As noted in Remark 2, the existence of entangled but zero distillable key states would result in a redefinition of the key cost. Similarly, K_F would change to a smaller quantity K'_F. Still, however, the following meaningful bound $K'_C \leq K_C \leq K_F^{\infty}$, resulting from our findings, would hold.*

9 Key cost of generalized private states

In this section, we prove several lemmas, which allow us to conclude that the key of formation, key cost, and distillable key are all equal for (irreducible) generalized private states. We begin with a series of lemmas, which allow us to prove the main result of this section, that is, Theorem 5.

Lemma 10. *For $\gamma(\psi)$ a generalized private state, the following equality holds*

$$S_{A_K}[\gamma(\psi)] = S_{A_K}(\psi). \quad (214)$$

Proof. Consider that

$$S_{A_K}[\gamma(\psi)] = S(\text{Tr}_{B_K A_S B_S}[\gamma(\psi)]) \quad (215)$$

$$= S(\text{Tr}_{B_K A_S B_S}[\widetilde{U}^{\dagger}\gamma(\psi)\widetilde{U}]) \quad (216)$$

$$= S(\text{Tr}_{B_K A_S B_S}[\psi \otimes \rho_{A_S B_S}]) \quad (217)$$

$$= S(\text{Tr}_{B_K}[\psi]) \quad (218)$$

$$= S_{A_K}(\psi). \quad (219)$$

In the above, the first equality is by definition. The second comes from the fact that the twisting U is a unitary that can be substituted with one acting only on systems $B_K A_S B_S$: $\widetilde{U} = \sum_i |i\rangle\langle i|_{B_K} \otimes U_i^{A_S B_S}$ in the case of generalized private states (for this idea, see [86]), and because the trace does not depend on the basis in which it is performed (here, the trace over systems $B_K A_S B_S$ does not depend on the basis $\widetilde{U}^{\dagger}$ which is defined on systems $B_K A_S B_S$ only). The last equality follows from the definition of the generalized private state. □

It was claimed, yet not argued explicitly in [33], that generalized private states are irreducible when the conditional states $U_i \rho_{A_S B_S} U_i^{\dagger}$ are separable for each $i \in [d_k]$. We provide an explicit argument below.

Lemma 11. *A strictly irreducible generalized private state $\gamma(\psi)$ satisfies*

$$K_D(\gamma(\psi)) = S_{A_K}(\psi) = E_R(\gamma(\psi)) = E_R^{\infty}(\gamma(\psi)). \quad (220)$$

Proof. Consider an arbitrary generalized private state $\gamma(\psi) = U(\psi_{A_K B_K} \otimes \rho_{A_S B_S})U^{\dagger}$, with $U = \sum_i |ii\rangle\langle ii|_{A_K B_K} \otimes U_i^{A_S B_S}$. We first show that $K_D(\gamma(\psi)) \geq S_{A_K}(\psi)$ and then that $E_R(\gamma(\psi)) \leq S_{A_K}(\psi)$. Since $E_R \geq E_R^{\infty} \geq K_D$ [16, 17], the claim follows by proving these two inequalities.

To show that $K_D(\gamma(\psi)) \geq S_{A_K}(\psi)$, we note that, after the measurement of system A_K of $\gamma(\psi)$ in the computational basis, the system $A_K B_K$ is in state $\rho_{A_K B_K} := \sum_i \mu_i |ii\rangle\langle ii|_{A_K B_K}$ such that $H(\{\mu_i\}) = S_{A_K}(\psi) = I(A_K; B_K)_{\rho_{A_K B_K}}$. Therefore, the Devetak–Winter protocol [25] applied to systems $A_K B_K$ produces $I(A_K; B_K) - I(A_K; E) = I(A_K; B_K)$ of key, as $I(A_K; E) = 0$ by the construction of the $\gamma(\psi_i)$. This proves $K_D(\gamma(\psi)) \geq S_{A_K}(\psi)$.

To show that $E_R(\gamma(\psi)) \leq S_{A_K}(\psi)$, let us choose a state $\sigma_{A_K B_K A_S B_S} := \sum_i \mu_i |ii\rangle\langle ii|_{A_K B_K} \otimes U_i \rho_{A_S B_S} U_i^{\dagger}$, which is, by the assumption of strict irreducibility of $\gamma(\psi)$, separable. We then observe that

$$D(\gamma(\psi)\|\sigma) = D(\psi_{A_K B_K} \otimes \rho_{A_S B_S} \| \sigma_{A_K B_K} \otimes \rho_{A_S B_S}) \quad (221)$$

$$= D(\psi_{A_K B_K} \| \sigma_{A_K B_K}) \quad (222)$$

$$= S_{A_K}(\psi), \quad (223)$$

where the first equality follows from the fact that the relative entropy is invariant under joint application of a unitary transformation $U^{\dagger}(\cdot)U$ to both its arguments. The second comes from the identity

$$D(\rho \otimes \sigma \| \rho' \otimes \sigma) = D(\rho \| \rho'), \quad (224)$$

and the last stems from a direct computation. By the above argument, we have by the definition of E_R that $E_R \leq S_{A_K}(\psi)$ as the choice of $\sigma_{A_K B_K A_S B_S}$ may be suboptimal when taking the infimum of the relative entropy "distance" from separable states. □

Due to Lemma 11, we can rephrase Definition 5 as follows.

Definition 7. *The key of formation of a state ρ is defined as*

$$K_F(\rho) := \inf_{\{\sum_k p_k \gamma(\psi_k) = \rho\}} \sum_k p_k K_D(\gamma(\psi_k)), \quad (225)$$

where the infimum is taken over strictly irreducible generalized private states.

We are now ready to show that the key of formation of a strictly irreducible private state $\gamma(\psi)$ is equal to $S_{A_K}(\psi)$.

Lemma 12. *For every strictly irreducible generalized private state $\gamma(\psi)$,*

$$K_F(\gamma(\psi)) = S_{A_K}(\psi). \tag{226}$$

Proof. First, by the definition of K_F, $\gamma(\psi)$ itself is a valid (singleton) decomposition into irreducible generalized private states. Hence $K_F(\gamma(\psi)) \leq S_{A_K}(\psi)$. On the other hand, for $\kappa > 0$, let the ensemble $\{p_i, \gamma(\psi_i)\}$ of γ be κ-optimal, giving $\sum_i p_i S(A_K)_{\psi_i} = K_F + \kappa$. Then

$$\begin{aligned} K_F(\gamma) + \kappa &= \sum_i p_i K_D(\gamma(\psi_i)) && (227)\\ &\geq K_D\left(\sum_i p_i \gamma(\psi_i)\right) && (228)\\ &= K_D(\gamma) && (229)\\ &= S_{A_K}(\psi), && (230) \end{aligned}$$

where the inequality is due to the fact that K_D is convex on mixtures $\sum_i p_i\sigma_i$ of states satisfying $K_D(\sigma_i) = E_R(\sigma_i)$ due to convexity of E_R and the fact that it is an upper bound on K_D (see Proposition 4.14 in [34]). Since the above inequality is true for all $\kappa > 0$ by the definition of K_F, we obtain the thesis. □

We will compute the entanglement of formation and entanglement cost for generalized private states. In analogy to pure states, we will have $K_D(\gamma) = K_C(\gamma) = K_F(\gamma)$, as stated below. However, the key is not equal to the entropy of a whole subsystem of a bipartite state γ but the entropy of a part of the subsystem (system A_K only).

We will need one more lemma to show the aforementioned equivalence.

Lemma 13. *For every bipartite state ρ_{AB}, the following inequalities hold*

$$K_F(\rho_{AB}) \geq K_F^\infty(\rho_{AB}) \geq K_D(\rho_{AB}). \tag{231}$$

Proof. There are multiple ways to show this. One stems from the fact that $K_F \geq K_F^\infty$ by subadditivity of K_F (Corollary 2), and the fact that $K_F^\infty \geq K_C \geq K_D$ (Theorem 4). □

We are ready to state the main result of this section.

Theorem 5. *For a strictly irreducible generalized private state $\gamma(\psi) \equiv \gamma_{A_K A_S B_K B_S}$ with key part $A_K B_K$, the following equalities hold*

$$\begin{aligned} K_C(\gamma) = K_D(\gamma) = E_R^\infty(\gamma) = E_R(\gamma) = K_F(\gamma)\\ = K_F^\infty(\gamma) = S_{A_K}(\gamma) = S_{A_K}(\psi). \end{aligned} \tag{232}$$

Proof. The last equality $S_{A_K}(\gamma(\psi)) = S_{A_K}(\psi)$ follows from Lemma 10. Furthermore, by Lemma 11, we have

$$K_D(\gamma(\psi)) = E_R^\infty(\gamma(\psi)) = E_R(\gamma(\psi)) = S_{A_K}(\psi). \tag{233}$$

We have further that $K_F(\gamma(\psi)) = S_A(\psi)$ by Lemma 12. It is thus sufficient to prove that $K_C(\gamma) = K_F(\gamma)$. To see this, we note first that by the above considerations, $K_F(\gamma) = K_D(\gamma)$. Further we note that K_F satisfies $K_F \geq K_F^\infty(\gamma) \geq K_D(\gamma)$ by Lemma 13. This fact implies that

$$K_F(\gamma) \geq K_F^\infty(\gamma) \geq K_D(\gamma) = K_F(\gamma), \tag{234}$$

and hence $K_F(\gamma) = K_F^\infty(\gamma)$. We then use Theorem 4, which states that $K_F^\infty \geq K_C$ and reuse the argument stated in the proof of Lemma 13, which states that $K_F^\infty \geq K_C \geq K_D$. Combining all the above arguments we obtain

$$K_F(\gamma) \geq K_F^\infty(\gamma) \geq K_C(\gamma) \geq K_D(\gamma) = K_F(\gamma), \tag{235}$$

which finishes the proof. □

Remark 5. *In entanglement theory, every proper entanglement monotone lies between the distillable entanglement and the entanglement cost [57]. However, not every proper entanglement monotone lies between the distillable key and the key cost. An example of this contrasting behavior involves the squashed entanglement which for the so-called flower states [46] (that are strictly irreducible private bits) amounts to $E_{\mathrm{sq}}(\gamma_{A_K B_K A_S B_S}) = 1 + \frac{\log|A_S|}{2} > 1 = K_C(\gamma_{A_K B_K A_S B_S})$ for $|A_S| \geq 2$ [87]. This is also a counterexample which shows that E_{sq} does not satisfy the equality from Theorem 5.*

10 Yield-cost relation for privacy

In this section we derive the yield-cost relation for privacy, following the results for entanglement in [53]. We note here that in [54] the yield-cost relation for a number of resource theories has been developed. However, inspecting the assumptions of Theorem 8 of [54] shows that the resource theory of private key (under the assumption that SEP is the free set of it) does satisfy one of them. Indeed, although it holds true that $D_{\min} = D_{\max}$ (see (47) and (45) for the definitions) for private states, the equality $D_{\min,\mathrm{aff(SEP)}} = D_{\max}$ does not hold, where

$$\begin{aligned} D_{\min,\mathrm{aff(SEP)}}(\rho) &:= \inf_{\sigma\in\mathrm{aff(SEP)}} D_{\min}(\rho\|\sigma) && (236)\\ &= \inf_{\sigma\in\mathrm{aff(SEP)}} D_h^{\varepsilon=0}(\rho\|\sigma) && (237) \end{aligned}$$

and aff(SEP) is the affine hull of the set SEP. Indeed, like in the case of entanglement theory, $D_{\min,\mathrm{aff(SEP)}} = 0$ in this case, since the set SEP spans the whole space of self-adjoint operators acting on a

finite-dimensional Hilbert space (see [88]). Whether one can use Theorem 8 of [54] is still open due to possible relation $D_{\min,\mathrm{SEP}}(\gamma_{d_k,d_s}) = D_{r,\mathrm{SEP}}(\gamma_{d_k,d_s})$ for all $\gamma_{d_k,d_s} \in \mathrm{SIR}$, where

$$D_{r,\mathrm{SEP}}(\rho) \coloneqq \inf\left\{ \log_2(1+r) : \frac{\rho + r\sigma}{1+r} \in \mathrm{SEP}, \sigma \in \mathrm{SEP} \right\} \quad (238)$$

is a measure of the robustness of entanglement [89] of the state ρ. However, our findings provide a tighter bound on K_D^{ε} by a function of $K_C^{\varepsilon'}$ for $\varepsilon = \varepsilon' < \frac{1}{2}$ than the relation given via the Theorem 8 of [54], if it holds.

Before we state the yield-cost relation for the one-shot case, let us define the one-shot distillable key.

Definition 8. *Fix $\varepsilon \in [0,1]$. The one-shot distillable key $K_D^{\varepsilon}(\rho)$ of a state ρ_{AB} is defined as*

$$K_D^{\varepsilon}(\rho) \coloneqq \sup_{\substack{\mathcal{L}\in\mathrm{LOCC},\\ \gamma_{d_k,d_s}\in\mathrm{SIR}}} \left\{ \begin{array}{c} \log_2 d_k : \\ \frac{1}{2}\|\mathcal{L}(\rho) - \gamma_{d_k,d_s}\|_1 \leq \varepsilon \end{array} \right\}, \quad (239)$$

where the supremum is taken over every LOCC channel $\mathcal{L}$ and every strictly irreducible private state γ_{d_k,d_s} with an arbitrarily large, finite shield dimension $d_s \geq 1$.

Theorem 6. *For every bipartite state ρ, the following inequality holds*

$$K_D^{\varepsilon_2}(\rho) \leq K_C^{\varepsilon_1}(\rho) + \log_2\left(\frac{1}{1-(\varepsilon_1+\varepsilon_2)}\right). \quad (240)$$

for $\varepsilon_1 + \varepsilon_2 < 1$ and $\varepsilon_1, \varepsilon_2 \in [0,1]$.

Proof. We first prove that for every γ_{d_k,d_s} that is irreducible, the following inequality holds

$$\begin{aligned} E_R^{\varepsilon}(\gamma_{d_k,d_s}) &= \inf_{\sigma\in\mathrm{SEP}} D_h^{\varepsilon}(\gamma_{d_k,d_s}\|\sigma) \\ &\leq \log_2 d_k - \log_2(1-\varepsilon). \end{aligned} \quad (241)$$

Let us fix then $\gamma_{d_k,d_s} = U(\Phi^+ \otimes \rho_{A_S B_S})U^\dagger \in \mathrm{SIR}$, where $U = \sum_i |ii\rangle\langle ii| \otimes U_i$ and $U_i \rho_{A_S B_S} U_i^\dagger \in \mathrm{SEP}$ for all $i \in \{0,\ldots,d_k-1\}$.

Now, to see the above inequality, let us first note that it suffices to prove the following lower bound

$$\sup_{\sigma\in\mathrm{SEP}} \inf_{\Omega\in T} \mathrm{Tr}\,(\Omega\sigma) \geq \frac{1-\varepsilon}{d_k}, \quad (242)$$

where

$$T \coloneqq \{0 \leq \Omega \leq \mathbb{1}_{d_k^2\times d_s^2}, \mathrm{Tr}(\Omega\gamma_{d_k,d_s}) \geq 1-\varepsilon\}. \quad (243)$$

Indeed, by multiplying both sides of (241) by -1, we get

$$\sup_{\sigma\in\mathrm{SEP}} \log_2\left(\inf_{\Omega\in T} \mathrm{Tr}(\Omega\sigma)\right) \geq -\log_2 d_k + \log_2(1-\varepsilon). \quad (244)$$

Now, taking the power of two on both sides, we get

$$\sup_{\sigma\in\mathrm{SEP}} \inf_{\Omega\in T} \mathrm{Tr}(\Omega\sigma) \geq \frac{1-\varepsilon}{d_k}. \quad (245)$$

The above inequality follows from Theorem 7 below and the fact that the relative ε-hypothesis divergence is an upper bound on the one-shot key, by using the idea of the proof of Theorem 1 in [53].

Consider two LOCC channels, $\mathcal{L}_{A_1^K B_1^K A_1^S B_1^S \to AB}$ and $\mathcal{L}_{AB\to A_2^K B_2^K A_2^S B_2^S}$ such that $\mathcal{L}_{A_1^K B_1^K A_1^S B_1^S \to AB}$ maps $\gamma_{d_k^1,d_s^1}$ up to ε_1 in normalized trace distance into ρ_{AB} and $\mathcal{L}_{AB\to A_2^K B_2^K A_2^S B_2^S}$ maps ρ_{AB} into $\gamma_{d_k^2,d_s^2}$ up to ε_2 in normalized trace distance. By composing these maps, we get a new one satisfying

$$\frac{1}{2}\left\|\mathcal{L}_{AB\to A_2^K B_2^K A_2^S B_2^S} \circ \mathcal{L}_{A_1^K B_1^K A_1^S B_1^S \to AB}(\gamma_{d_k',d_s'}) - \gamma_{d_k'',d_s''}\right\|_1 \leq \varepsilon_1 + \varepsilon_2. \quad (246)$$

It implies that

$$\log_2 d_k'' \leq \log_2 d_k' + \log_2\left(\frac{1}{\varepsilon'}\right), \quad (247)$$

with $\varepsilon' \coloneqq \varepsilon_1 + \varepsilon_2$ because

$$\begin{aligned} \log_2 d_k'' &\leq K_D^{\varepsilon'}(A_1^K A_1^S : A_1^K B_1^S)_{\gamma_{d_k',d_s'}} && (248)\\ &\leq E_R^{\varepsilon'}(\gamma_{d_k',d_s'}) && (249)\\ &\leq \log_2 d_k' + \log_2\left(\frac{1}{1-\varepsilon'}\right), && (250) \end{aligned}$$

where the first inequality is due to the fact that the distillation of $\gamma_{d_k'',d_s''}$ from $\gamma_{d_k',d_s'}$ via ρ_{AB} may be a sub-optimal process of distillation $\gamma_{d_k'',d_s''}$ from $\gamma_{d_k',d_s'}$ in general. The next inequality follows from [31, Theorem 8]. The last one follows from Theorem 7. Taking supremum over processes that produce $\gamma_{d_k'',d_s''}$ and infimum over processes that create ρ_{AB} from $\gamma_{d_k',d_s'}$, we obtain the statement of the theorem. □

Theorem 7. *For every strictly irreducible private state $\gamma_{d_k,d_s} = U(\Phi^+ \otimes \rho_{A_S B_S})U^\dagger$, the following inequality holds*

$$\sup_{\sigma\in\mathrm{SEP}} \inf_{\Omega\in T} \mathrm{Tr}\,(\Omega\sigma) \geq \frac{(1-\varepsilon)}{d_k}, \quad (251)$$

where $T = \{0 \leq \Omega \leq \mathbb{1}_{d_k^2\times d_s^2}, \mathrm{Tr}(\Omega\gamma_{d_k,d_s}) \geq 1-\varepsilon\}$.

Proof. Consider $\sigma = U(\sigma_k \otimes \rho_{A_S B_S})U^\dagger \in \mathrm{SEP}$ as an ansatz, where $\sigma_k = (1/d_k)^{-1}\sum_i |ii\rangle\langle ii|$. Recall that $U = \sum_{i=0}^{d_k-1} |ii\rangle\langle ii| \otimes U_i$ and that, by the assumption of strict irreducibility, $U_i \rho_{A_S B_S} U_i^\dagger$ is separable for each i. Observe then that

$$\mathrm{Tr}(\Omega U(\Phi_{d_k}^+ \otimes \rho_{A_S B_S})U^\dagger) \geq 1-\varepsilon \quad (252)$$

is equivalent by cyclicity of trace to

$$\mathrm{Tr}(U^\dagger \Omega U(\Phi_{d_k}^+ \otimes \rho_{A_S B_S})) \geq 1-\varepsilon. \quad (253)$$

Denoting now $\widetilde{\Omega} \equiv U^\dagger \Omega U$, note then that

$$\mathrm{Tr}(\Omega\sigma) = \mathrm{Tr}(\Omega U(\sigma_k \otimes \rho_{A_S B_S})U^\dagger) \tag{254}$$
$$= \mathrm{Tr}(\widetilde{\Omega}(\sigma_k \otimes \rho_{A_S B_S})). \tag{255}$$

These equalities follow by the choice of σ and cyclicity of trace. We have then that the left-hand side (LHS) of the formula (242) is lower bounded (by the particular choice of σ) as follows

$$\inf_{\widetilde{\Omega}\in T_1} \mathrm{Tr}(\widetilde{\Omega}(\sigma_k \otimes \rho_{A_S B_S})), \tag{256}$$

where

$$T_1 := \{0 \leq \widetilde{\Omega} \leq \mathbb{1}_{d_k^2 \times d_s^2}, \mathrm{Tr}(\widetilde{\Omega}(\Phi^+_{d_k} \otimes \rho_{A_S B_S})) \geq 1-\varepsilon\}. \tag{257}$$

The above quantity is an instance of semi-definite optimization. Indeed, we can cast it as follows

$$\begin{aligned} &\inf_{\widetilde{\Omega}} \mathrm{Tr}(\widetilde{\Omega}(\sigma_k \otimes \rho_{A_S B_S})) \\ &0 \leq \widetilde{\Omega} \leq \mathbb{1}_{d_k^2 \times d_s^2}, \\ &\mathrm{Tr}(\widetilde{\Omega}(\Phi^+_{d_k} \otimes \rho_{A_S B_S})) \geq (1-\varepsilon) \end{aligned} \tag{258}$$

which by weak duality admits a lower bound of the form

$$\begin{aligned} &\sup_{y,Y} y(1-\varepsilon) - \mathrm{Tr}(Y) \\ &Y \geq (y\Phi^+_{d_k} - \sigma_k) \otimes \rho_{A_S B_S}, \\ &y, Y \geq 0. \end{aligned} \tag{259}$$

Indeed, to see this, consider that

$$\inf_{\widetilde{\Omega}\geq 0} \left\{ \begin{array}{c} \mathrm{Tr}[\widetilde{\Omega}\,(\sigma_k \otimes \rho_{A_S B_S})] : \\ \widetilde{\Omega} \leq \mathbb{1}, \\ \mathrm{Tr}\left[\widetilde{\Omega}\left(\Phi^+_{d_k} \otimes \rho_{A_S B_S}\right)\right] \geq 1-\varepsilon \end{array} \right\}$$

$$= \inf_{\widetilde{\Omega}\geq 0} \left\{ \begin{array}{c} \mathrm{Tr}[\widetilde{\Omega}\,(\sigma_k \otimes \rho_{A_S B_S})] + \\ \sup_{Y\geq 0} \mathrm{Tr}\left[Y\left(\widetilde{\Omega} - \mathbb{1}\right)\right] + \\ \sup_{y\geq 0} y \left(\begin{array}{c} 1-\varepsilon \\ -\mathrm{Tr}\left[\widetilde{\Omega}\left(\Phi^+_{d_k} \otimes \rho_{A_S B_S}\right)\right] \end{array} \right) \end{array} \right\} \tag{260}$$

$$= \inf_{\widetilde{\Omega}\geq 0} \sup_{\substack{Y\geq 0, \\ y\geq 0}} \left\{ \begin{array}{c} \mathrm{Tr}[\widetilde{\Omega}\,(\sigma_k \otimes \rho_{A_S B_S})] + \\ \mathrm{Tr}\left[Y\left(\widetilde{\Omega} - \mathbb{1}\right)\right] + \\ y\left(1-\varepsilon - \mathrm{Tr}\left[\widetilde{\Omega}\left(\Phi^+_{d_k} \otimes \rho_{A_S B_S}\right)\right]\right) \end{array} \right\} \tag{261}$$

$$\geq \sup_{\substack{Y\geq 0, \\ y\geq 0}} \inf_{\widetilde{\Omega}\geq 0} \left\{ \begin{array}{c} \mathrm{Tr}[\widetilde{\Omega}\,(\sigma_k \otimes \rho_{A_S B_S})] + \\ \mathrm{Tr}\left[Y\left(\widetilde{\Omega} - \mathbb{1}\right)\right] + \\ y\left(1-\varepsilon - \mathrm{Tr}\left[\widetilde{\Omega}\left(\Phi^+_{d_k} \otimes \rho_{A_S B_S}\right)\right]\right) \end{array} \right\} \tag{262}$$

$$= \sup_{\substack{Y\geq 0, \\ y\geq 0}} \inf_{\widetilde{\Omega}\geq 0} \left\{ \begin{array}{c} y\,(1-\varepsilon) - \mathrm{Tr}[Y] + \\ \mathrm{Tr}\left[\widetilde{\Omega}\left(Y - \left(y\Phi^+_{d_k} - \sigma_k\right) \otimes \rho_{A_S B_S}\right)\right] \end{array} \right\} \tag{263}$$

$$= \sup_{\substack{Y\geq 0, \\ y\geq 0}} \left\{ \begin{array}{c} y\,(1-\varepsilon) - \mathrm{Tr}[Y] + \\ \inf_{\widetilde{\Omega}\geq 0} \mathrm{Tr}\left[\widetilde{\Omega}\left(\begin{array}{c} Y - (y\Phi^+_{d_k} - \sigma_k) \\ \otimes \rho_{A_S B_S} \end{array} \right)\right] \end{array} \right\} \tag{264}$$

$$= \sup_{Y\geq 0, y\geq 0} \left\{ \begin{array}{c} y\,(1-\varepsilon) - \mathrm{Tr}[Y] : \\ Y \geq \left(y\Phi^+_{d_k} - \sigma_k\right) \otimes \rho_{A_S B_S} \end{array} \right\}. \tag{265}$$

The first equality follows by the introduction of Lagrange multipliers and because

$$\sup_{Y\geq 0} \mathrm{Tr}\left[Y\left(\widetilde{\Omega} - \mathbb{1}\right)\right] = +\infty \tag{266}$$

if and only if $\widetilde{\Omega} \not\leq \mathbb{1}$ and

$$\sup_{y\geq 0} y\left(1-\varepsilon - \mathrm{Tr}\left[\widetilde{\Omega}\left(\Phi^+_{d_k} \otimes \rho_{A_S B_S}\right)\right]\right) = +\infty \tag{267}$$

if and only if $\mathrm{Tr}\left[\widetilde{\Omega}\left(\Phi^+_{d_k} \otimes \rho_{A_S B_S}\right)\right] \not\geq 1-\varepsilon$. The second equality follows by moving suprema to the outside. The inequality follows from the max-min inequality. The third equality follows from some basic algebra. The penultimate equality follows from moving the infimum inside. The final equality follows because

$$\inf_{\widetilde{\Omega}\geq 0} \mathrm{Tr}\left[\widetilde{\Omega}\left(Y - \left(y\Phi^+_{d_k} - \sigma_k\right) \otimes \rho_{A_S B_S}\right)\right] = -\infty \tag{268}$$

if and only if $Y \not\geq \left(y\Phi^+_{d_k} - \sigma_k\right) \otimes \rho_{A_S B_S}$.

We now observe that any choice of y and Y in (259) gives another lower bound on the above quantity, as it is a supremum over these variables. We will choose $Y = 0$ and $y = \frac{1}{d_k}$. We need to argue that this choice satisfies the constraints. To show this, it suffices to prove that

$$\left(\frac{1}{d_k}\Phi^+_{d_k} - \sigma_k\right) \otimes \rho_{A_S B_S} \leq Y = 0. \tag{269}$$

Since $\rho_{A_S B_S} \geq 0$, as $\rho_{A_S B_S}$ is a state, the above holds if and only if

$$\frac{1}{d_k}\Phi^+_{d_k} - \sigma_k \leq 0. \tag{270}$$

To prove this, we observe that the state σ_k is equivalent to a maximally entangled state measured locally by a von Neumann measurement in the computational basis. Such a measurement can be simulated by applying random unitary transformations that perform *dephasing*. We take d_k unitary transformations of the form [90]:

$$V_l := \sum_{j=0}^{d-1} e^{2\pi i l j/d_k} |j\rangle\langle j|. \tag{271}$$

Given this choice, it follows that

$$\sigma_k = \frac{1}{d_k} \sum_{l=0}^{d_k-1} (V_l \otimes \mathbb{1})\Phi^+_{d_k}(V_l \otimes \mathbb{1})^\dagger. \tag{272}$$

We also note that the states $|\psi_l\rangle\langle\psi_l| \equiv (V_l \otimes \mathbb{1})\Phi^+_{d_k}(V_l^\dagger \otimes \mathbb{1})$ are mutually orthogonal [52], and form a subset of the basis of maximally entangled states in $d_k \otimes d_k$. Thus expanding matrix $\frac{1}{d_k}\Phi^+_{d_k} - \sigma_k$ in this basis we see that

$$\frac{1}{d_k}\Phi^+_{d_k} - \frac{1}{d_k}\Phi^+_{d_k} - \frac{1}{d_k}\sum_{l>0}^{d_k-1}(V_l \otimes \mathbb{1})\Phi^+_{d_k}(V_l^\dagger \otimes \mathbb{1}), \quad (273)$$

which is negative, as we aimed to argue, since the first two terms cancel out, and the reminder has negative eigenvalues in the considered basis. By the choice of y and (259) we conclude that the infimum in (256) is bounded from below by $\dfrac{1-\varepsilon}{d_k}$ as claimed. □

As a corollary of Theorem 6, it follows that all strictly irreducible private states are to a large extent "units" of privacy, i.e., their cost is $\approx \log_2 d_k$. We state this fact in the corollary below.

Corollary 1. *Let γ_{d_k,d_s} be a strictly irreducible private state. Then*

$$\log_2 d_k - \log_2\left(\frac{1}{1-\varepsilon}\right) \leq K_C^\varepsilon(\gamma_{d_k,d_s}) \leq \log_2 d_k. \quad (274)$$

Proof. The inequality on the RHS stems from the definition of K_C^ε, while the inequality on the LHS is due to Theorem 6, by picking $\varepsilon_1 = \varepsilon$ and $\varepsilon_2 = 0$, and the fact that $K_D^0(\gamma_{d_k,d_s}) = \log_2 d_k$. □

11 Key cost of a quantum device

We now define a quantity for a quantum device, which is analogous to the key cost of a state. We follow the idea of introducing measures of quantum nonlocality based on entanglement measures, as provided in [41] (see also [91]). Non-locality measures obtained in this way are called reduced entanglement measures. For a given device, the reduced entanglement measure E is obtained by taking the minimal value of E over all quantum states that lead to the device when one can vary over measurement settings. It is natural to consider reduced key cost and reduced key of formation obtained in this way.

A device, i.e., a conditional probability distribution of two outputs (a, b) given two inputs (x, y), denoted as $P(ab|xy)$ is quantum if and only if there exists a state ρ_{AB} such that

$$\mathrm{Tr}(\rho_{AB}(\mathrm{M}_x^a \otimes \mathrm{M}_y^b)) = P(ab|xy). \quad (275)$$

We denote such a device as $(\mathcal{M}, \rho_{AB})$, where $\mathcal{M} = \mathrm{M}_x^a \otimes \mathrm{M}_y^b$. Below, we define the cost of a device for the bipartite case, with the multipartite case following along similar lines.

Definition 9. *Let $\varepsilon > 0$. The key cost of a quantum device $P(ab|xy)$ is equal to the reduced single-shot key cost*

$$K_C^\varepsilon(P(ab|xy)) \equiv K_C^{\varepsilon\downarrow}(P(ab|xy)) \coloneqq \inf_{\substack{\rho_{AB},\\ \mathrm{M}_x^a \otimes \mathrm{M}_y^b}} \{K_C^\varepsilon(\rho_{AB}) : \mathrm{Tr}(\rho_{AB}\mathrm{M}_x^a \otimes \mathrm{M}_y^b) = P(ab|xy)\}. \quad (276)$$

Besides the technical origin of the above definition of a single-shot key cost of a device, it has a clear operational interpretation. Namely, it can be viewed as the minimal cost (in terms of device-dependent secure key) incurred by a mistrustful vendor upon creation of the device. Let us note here that the dishonest provider of a device $P(a, b|x, y)$ during production process is only limited by the future statistics of inputs and outputs of the device, which motivates taking the infimum over states and measurements compatible with $P(a, b|x, y)$.

We now establish a nontrivial bound for all devices that admit a realization on states with a positive partial transpose (PPT states). The PPT states satisfy $\mathbb{1}_A \otimes T_B(\rho_{AB}) \equiv \rho_{AB}^{\Gamma_B} \geq 0$, where T_B is the transposition map applied to system B. The set of all PPT states is denoted as PPT. We say that $P(ab|xy) \in$ PPT iff $P(ab|xy) = \mathrm{Tr}(\rho_{AB}\mathrm{M}_x^a \otimes \mathrm{M}_y^b)$ for some measurements $\mathrm{M}_x^a \otimes \mathrm{M}_y^b$ and a state ρ_{AB} with positive partial transpose. We call the state ρ_{AB} a PPT realization of $P(ab|xy)$.

Proposition 1. *For all $\varepsilon > 0$ and for every $P(ab|xy) \in$ PPT with PPT realization ρ_{AB}, the following inequality holds*

$$K_C^\varepsilon(P(ab|xy)) \leq \min\{K_C^\varepsilon(\rho_{AB}), K_C^\varepsilon(\rho_{AB}^{\Gamma_B})\}. \quad (277)$$

Proof. Following [41] it suffices to notice that, by the identity $\mathrm{Tr}(XY) = \mathrm{Tr}\left(X^\Gamma Y^\Gamma\right)$ and the fact that $\rho_{AB}^{\Gamma_B} \geq 0$, we have that, for every realization $(\sigma_{AB}, \mathcal{N})$ with $\mathcal{N} = \mathrm{N}_x^a \otimes \mathrm{N}_y^b$ of a device $P(ab|xy)$, the equality $(\sigma, \mathcal{N}) = (\sigma^{\Gamma_B}, \mathcal{N}^{\Gamma_B})$ holds. □

We can also define the device-independent key cost of a state.

Definition 10. *The device-independent key cost of a bipartite state ρ_{AB} is defined as*

$$K_C^\varepsilon(\rho_{AB}) \coloneqq \sup_{\mathcal{M}} K_C^\varepsilon(\rho_{AB}, \mathcal{M}). \quad (278)$$

In particular, for the states ρ on $\mathbb{C}^{2d_s} \otimes \mathbb{C}^{2d_s}$ given in [45] for which it is proven in [41], that device-independent key is (strictly) upper bounded by $K_{\mathrm{D}}(\rho^\Gamma)$, there is

$$K_C^\varepsilon(\rho_{AB}) \leq K_C^\varepsilon(\rho_{AB}^\Gamma) \leq \frac{1}{\sqrt{d_s}+1}. \quad (279)$$

These states have vanishing device-independent key cost with increasing dimension d_s. Interestingly, however, they have a device-dependent key rate equal to one. It corresponds to the fact that these states tend to be indistinguishable from their separable key-attacked version (i.e., K_C is zero) where distinguishability is performed using LOCC operations [92, 34]. One can also define an asymptotic version of the key cost of a device, which, apart from an analogy of (279), can be related to the device-independent key via Eqs. (2) and (5) of [41]

$$\begin{aligned} K_{\mathrm{DI}}(\rho) &\leq K_D^{\downarrow}(\rho) \\ &\leq K_C^{\downarrow}(\rho) \equiv \sup_{\mathcal{M}} \inf_{(\sigma,\mathcal{N})=(\rho,\mathcal{M})} K_C(\sigma). \end{aligned} \tag{280}$$

Analogous results can be obtained for the reduced key of formation, which is defined as

$$\begin{aligned} &K_F(P(ab|xy)) \coloneqq \\ &\inf_{(\mathcal{N},\sigma_{AB})} \{K_F(\sigma_{AB}) : (\mathcal{N},\sigma_{AB}) = P(ab|xy)\}. \end{aligned} \tag{281}$$

Furthermore, definitions analogous to Defs. 9 and 10 lead to the key cost for a given set of parameters tested in a DIQKD protocol. These are obtained by replacing the infimum over states ρ_{AB} and measurements $\mathcal{M}$ compatible with the device $P(a,b|x,y)$ by the infimum over those compatible with the parameters of the game score (e.g. CHSH) and quantum bit error rate value (for analogous approach in context of device-independent key, see [93]).

Remark 6. *We note here that the measure defined in (281) need not coincide with the key of formation of a device, which would be an analog of K_F for quantum states. The latter analog would involve the infimum over splittings into devices that contain an ideal device-independent key (denoted as IDIK). While devices lying on the boundary of a quantum set (i.e. having quantum realization) belong to IDIK, it is unclear if they exhaust IDIK.*

12 Proof of subadditivity of K_F

It is easy to observe that the key of formation is subadditive. We state it in a more general form for any convex roof measure. Let S denote a subset of all finite-dimensional quantum states with the following properties:

1. S is closed under tensor product,
2. every quantum state ρ can be written as a convex combination of elements from S.

Note that, as an example, the set of all pure states satisfies the conditions above. A convex-roof measure E_S, with respect to the set S of ρ, is then

$$E_S(\rho) = \inf_{\{(p_i,\rho_i)\}_i} \sum_i p_i f(\rho_i) \tag{282}$$

for some real non-negative valued function f, where the infimum is taken over every ensemble decomposition $\sum_i p_i\rho_i = \rho$ and $\rho_i \in S$ for all i.

Observation 6. *For a convex-roof measure E_S taken with respect to set S that is closed under tensor products, E_S is subadditive; i.e., $E_S(\rho\otimes\rho') \leq E_S(\rho) + E_S(\rho')$.*

Proof. Let $\{(p_i,\sigma_i)\}_i$ and $\{(q_j,\tau_j)\}_j$ be two ensemble decompositions that attain $E_S(\rho)$ and $E_S(\rho')$ respectively. Then, from the facts that S is closed under tensor products and $\sigma_i,\tau_j \in S$, we have that $\{(p_iq_j,\sigma_i\otimes\tau_j)\}_{i,j}$ is a valid ensemble decomposition of $\rho\otimes\rho'$. However, it can be suboptimal, concluding the proof. □

We have then the following corollary.

Corollary 2. *K_F is subadditive.*

Proof. It follows from Observation 6 and the fact that the set of generalized private states is closed under tensor products. The fact that strictly irreducible private states are closed under tensor products was observed in the proof of [52, Theorem 29 (Supplementary Material)].

We give the proof for generalized private states for the sake of completeness. To see the above, consider a tensor-product $\gamma^{(1)}_{A_1^KA_1^SB_1^KB_1^S} \equiv \gamma^{(1)}$ with $\gamma^{(2)}_{A_2^KA_2^SB_2^KB_2^S} \equiv \gamma^{(2)}$ where

$$\gamma^{(1)} \coloneqq U_1|\psi_1\rangle\langle\psi_1|_{A_1^KB_1^K}\otimes\rho_{A_1^SB_1^S}U_1^\dagger, \tag{283}$$

$$\gamma^{(2)} \coloneqq U_2|\psi_2\rangle\langle\psi_2|_{A_2^KB_2^K}\otimes\rho_{A_2^SB_2^S}U_2^\dagger, \tag{284}$$

$$U_1 \coloneqq \sum_i |ii\rangle\langle ii|\otimes U_i^{(1)}, \tag{285}$$

$$U_2 \coloneqq \sum_i |ii\rangle\langle ii|\otimes U_i^{(2)}. \tag{286}$$

Consider local unitary transformations $V_{A_1^S,A_2^K}\otimes V_{B_1^S,B_2^K}$ that swap the shield systems $A_1^SB_1^S$ of the private state $\gamma^{(1)}_{A_1^KA_1^SB_1^KB_1^S}$ with (properly embedded to equal dimensions) the key part of $A_2^KB_2^K$ of $\gamma^{(2)}_{A_2^KA_2^SB_2^KB_2^S}$. It follows that the state

$$\begin{aligned} &\left(V_{A_1^S,A_2^K}\otimes V_{B_1^S,B_2^K}\right)\left(\gamma^{(1)}\otimes\gamma^{(2)}\right)\times \\ &\qquad\left(V^\dagger_{A_1^S,A_2^K}\otimes V^\dagger_{B_1^S,B_2^K}\right) \end{aligned} \tag{287}$$

is a generalized private state of the form

$$W\Big(|\psi_1\rangle\langle\psi_1|_{A_1^KB_1^K}\otimes|\psi_2\rangle\langle\psi_2|_{A_2^KB_2^K} \otimes\rho_{A_1^SB_1^S}\otimes\rho_{A_2^SB_2^S}\Big)W^\dagger$$

$$\equiv W|\psi_1\rangle\langle\psi_1|_{A_1^K B_1^K}\otimes|\psi_2\rangle\langle\psi_2|_{A_2^K B_2^K}\otimes\rho_{A_1^S A_2^S B_1^S B_2^S}W^\dagger, \tag{288}$$

where

$$W \coloneqq \sum_{i,j}|ii\rangle\langle ii|_{A_1^K B_1^K}\otimes|jj\rangle\langle jj|_{A_2^K B_2^K}\otimes U_i^{(1)}\otimes U_j^{(2)}, \tag{289}$$

which completes the proof. □

13 Outlook and Discussion

We have introduced two quantities central to the resource theory of privacy: private key cost and private key of formation. We have done so assuming the faithfulness of the distillable key (i.e., nonexistence of entangled states with zero distillable key). One of our fundamental contributions is that the regularized key of formation of a bipartite state upper bounds the key cost ($K_F^\infty \geq K_C$). Equality holds (i.e., $K_F^\infty = K_C$) if K_F is an asymptotically continuous entanglement monotone. While we have shown the monotonicity of K_F with respect to some basic operations (see Section 6), the monotonicity (on average) under von Neumann measurements and asymptotic continuity beyond trivial cases, remain important open problems. The importance of these problems also stems from the fact that they would imply non-trivial results for the key cost of quantum channels.

Let us note here that K_C, similar to most operational entanglement measure, is difficult to compute. However, the bounds $E_R^\infty \leq K_C \leq K_F^\infty \leq K_F$ provide a way to estimate it. It is then an interesting open problem to determine for which states other than strictly irreducible generalized private states, can K_F be found analytically or computed numerically, beyond the trivial upper bound $K_F \leq E_F$ or the lower bound $E_R^\infty \leq K_F$ established here.

It is striking that, while showing a function to be entanglement monotone is standard by now [20], all known methods from entanglement theory do not immediately apply to show that K_F is an asymptotically continuous LOCC monotone. For a detailed discussion see Section 6.1.

We consider it salient to generalize our findings to the settings of conference key agreement [94, 31]. It is also of prime importance to compute K_C for some states other than generalized private states.

We stress that, from a purely mathematical perspective, rather than from an operational viewpoint, the presented results remain valid even if entangled but zero distillable key states were to exist (see Remarks 2 and 4).

Note added. Upon finishing this article, we became aware that the most general definition of the key cost, denoted as K_C^s and called strict key cost (corresponding to the K_C' mentioned in Remark 2), was proposed by Stefan Bäuml [95] in his master's thesis, along with some initial observations. Ref. [95] includes also the main result of [51], which characterized irreducible private states.

Acknowledgements

KH acknowledges the Fulbright Program and Cornell ECE for hospitality during the Fulbright scholarship at the School of Electrical and Computer Engineering of Cornell University. KH acknowledges 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). SD acknowledges support from the Science and Engineering Research Board (now ANRF), Department of Science and Technology, Government of India, under Grant No. SRG/2023/000217 and the Ministry of Electronics and Information Technology (MeitY), Government of India, under Grant No. 4(3)/2024-ITEA. SD also thanks IIIT Hyderabad for the Faculty Seed Grant. KH acknowledges National Science Centre, Poland, grant Opus 25, UMO-2023/49/B/ST2/02468. MMW acknowledges support from the National Science Foundation under Grant No. 2315398.

References

[1] Eric Chitambar and Gilad Gour. "Quantum resource theories". Reviews of Modern Physics **91**, 025001 (2019).

[2] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. "Purification of noisy entanglement and faithful teleportation via noisy channels". Physical Review Letters **76**, 722–725 (1996).

[3] Ueli M. Maurer. "Secret key agreement by public discussion from common information". IEEE Transactions on Information Theory **39**, 733–742 (1993).

[4] Renato Renner and Stefan Wolf. "New bounds in secret-key agreement: The gap between formation and secrecy extraction". In Lecture Notes in Computer Science. Pages 562–577. Springer Berlin Heidelberg (2003).

[5] Nicolas Gisin and Stefan Wolf. "Linking classical and quantum key agreement: Is there "bound information"?". In Proceedings of Crypto 2000,

Lecture Notes in Computer Science. Volume 1880, pages 482–500. (2000).

[6] Antonio Acín, Juan Ignacio Cirac, and Lluis Masanes. "Multipartite bound information exists and can be activated". Physical Review Letters **92**, 107903 (2004).

[7] Andreas Winter. "Secret, public and quantum correlation cost of triples of random variables". In Proceedings of the 2005 International Symposium on Information Theory. Pages 2270–2274. (2005).

[8] Karol Horodecki, Michał Horodecki, Pawel Horodecki, and Jonathan Oppenheim. "Information theories with adversaries, intrinsic information, and entanglement". Foundations of Physics **35**, 2027–2040 (2005).

[9] Eric Chitambar, Min-Hsiu Hsieh, and Andreas Winter. "The private and public correlation cost of three random variables with collaboration". IEEE Transactions on Information Theory **62**, 2034–2043 (2016).

[10] Eric Chitambar, Ben Fortescue, and Min-Hsiu Hsieh. "Classical analog to entanglement reversibility". Physical Review Letters **115**, 090501 (2015).

[11] Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner. "Unifying classical and quantum key distillation". In Theory of Cryptography. Pages 456–478. Springer Berlin Heidelberg (2007).

[12] Maris Ozols, Graeme Smith, and John A. Smolin. "Bound entangled states with a private key and their classical counterpart". Physical Review Letters **112**, 110502 (2014).

[13] Eric Chitambar, Ben Fortescue, and Min-Hsiu Hsieh. "The conditional common information in classical and quantum secret key distillation". IEEE Transactions on Information Theory **64**, 7381–7394 (2018).

[14] Daniel Collins and Sandu Popescu. "Classical analog of entanglement". Physical Review A **65**, 032321 (2002).

[15] Stephanie Wehner, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead". Science **362**, eaam9288 (2018).

[16] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "Secure key from bound entanglement". Physical Review Letters **94**, 160502 (2005).

[17] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "General paradigm for distilling classical key from quantum states". IEEE Transactions on Information Theory **55**, 1898–1929 (2009).

[18] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information". Cambridge University Press. Cambridge, UK (2000).

[19] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?". Physical Review Letters **80**, 5239–5242 (1998).

[20] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki. "Quantum entanglement". Reviews of Modern Physics **81**, 865–942 (2009).

[21] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. "Mixed-state entanglement and quantum error correction". Physical Review A **54**, 3824–3851 (1996). arXiv:quant-ph/9604024.

[22] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. Page 175. India (1984).

[23] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". Physical Review Letters **67**, 661–663 (1991).

[24] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. "Quantum cryptography". Reviews of Modern Physics **74**, 145–195 (2002).

[25] Igor Devetak and Andreas Winter. "Distillation of secret key and entanglement from quantum states". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207–235 (2005).

[26] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. "Device-independent security of quantum cryptography against collective attacks". Physical Review Letters **98**, 230501 (2007).

[27] Marcin Pawłowski and Nicolas Brunner. "Semi-device-independent security of one-way quantum key distribution". Physical Review A **84**, 010302 (2011).

[28] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution". Physical Review Letters **108**, 130503 (2012).

[29] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. "Practical device-independent quantum cryptography via entropy accumulation". Nature Communications **9**, 459 (2018).

[30] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. "Secure quantum key distribution with realistic devices". Reviews of Modern Physics **92**, 025002 (2020).

[31] Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki. "Universal limitations on quantum key distribution

over a network". Physical Review X **11**, 041016 (2021).

[32] Matthias Christandl. "The structure of bipartite quantum states - insights from group theory and cryptography". PhD thesis. University of Cambridge. (2006).

[33] Karol Horodecki, Michał Studziński, Ryszard P. Kostecki, Omer Sakarya, and Dong Yang. "Upper bounds on the leakage of private data and an operational approach to Markovianity". Physical Review A **104**, 052422 (2021).

[34] Karol Horodecki. "General paradigm for distilling classical key from quantum states — On quantum entanglement and security". PhD thesis. University of Warsaw. (2008). url: https://www.mimuw.edu.pl/media/uploads/doctorates/thesis-karol-horodecki.pdf.

[35] Patrick M. Hayden, Michal Horodecki, and Barbara M. Terhal. "The asymptotic entanglement cost of preparing a quantum state". Journal of Physics A: Mathematical and General **34**, 6891–6898 (2001).

[36] Hayata Yamasaki, Kohdai Kuroiwa, Patrick Hayden, and Ludovico Lami. "Entanglement cost for infinite-dimensional physical systems". Communications in Mathematical Physics **406**, 277 (2025).

[37] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Debbie Leung, and Jonathan Oppenheim. "Unconditional privacy over channels which cannot convey quantum information". Physical Review Letters **100**, 110502 (2008).

[38] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Debbie Leung, and Jonathan Oppenheim. "Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity". IEEE Transactions on Information Theory **54**, 2604–2620 (2008).

[39] Graeme Smith and Jon Yard. "Quantum communication with zero-capacity channels". Science **321**, 1812–1815 (2008). arXiv:0807.4935.

[40] Ignatius W. Primaatmaja, Koon Tong Goh, Ernest Y.-Z. Tan, John T.-F. Khoo, Shouvik Ghorai, and Charles C.-W. Lim. "Security of device-independent quantum key distribution protocols: a review". Quantum **7**, 932 (2023).

[41] Matthias Christandl, Roberto Ferrara, and Karol Horodecki. "Upper bounds on device-independent quantum key distribution". Physical Review Letters **126**, 160501 (2021).

[42] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". Reviews of Modern Physics **86**, 419–478 (2014).

[43] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. "Entanglement as a precondition for secure quantum key distribution". Physical Review Letters **92**, 217903 (2004).

[44] "Open quantum problems—IQOQI Vienna". https://oqp.iqoqi.oeaw.ac.at/open-quantum-problems.

[45] Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki. "Low-dimensional bound entanglement with one-way distillable cryptographic key". IEEE Transactions on Information Theory **54**, 2621–2625 (2008).

[46] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. "Locking entanglement with a single qubit". Physical Review Letters **94**, 200501 (2005).

[47] Vlatko Vedral, Martin B. Plenio, M. A. Rippin, and Peter L. Knight. "Quantifying entanglement". Physical Review Letters **78**, 2275–2279 (1997).

[48] Matthias Christandl, Norbert Schuch, and Andreas Winter. "Entanglement of the antisymmetric state". Communications in Mathematical Physics **311**, 397–422 (2012). arXiv:0910.4151.

[49] Stefan Bäuml, Matthias Christandl, Karol Horodecki, and Andreas Winter. "Limitations on quantum key repeaters". Nature Communications **6**, 6908 (2015). arXiv:1402.5927.

[50] Mark M. Wilde. "Squashed entanglement and approximate private states". Quantum Information Processing **15**, 4563–4580 (2016). arXiv:1606.08028.

[51] Karol Horodecki, Piotr Ćwikliński, Adam Rutkowski, and Michał Studziński. "On distilling secure key from reducible private states and (non)existence of entangled key-undistillable states". New Journal of Physics **20**, 083021 (2016). arXiv:1612.08938.

[52] Matthias Christandl and Roberto Ferrara. "Private states, quantum data hiding, and the swapping of perfect secrecy". Physical Review Letters **119**, 220506 (2017).

[53] Mark M. Wilde. "Second law of entanglement dynamics for the non-asymptotic regime". In Proceedings of the 2021 IEEE Information Theory Workshop (ITW). Pages 1–6. (2021).

[54] Ryuji Takagi, Bartosz Regula, and Mark M. Wilde. "One-shot yield-cost relations in general quantum resource theories". PRX Quantum **3**, 010348 (2022).

[55] Dong Yang, Michał Horodecki, Ryszard Horodecki, and Barbara Synak-Radtke. "Irreversibility for all bound entangled states". Physical Review Letters **95**, 190501 (2005).

[56] Matthias Christandl and Andreas Winter. ""Squashed entanglement": An additive entanglement measure". Journal of Mathematical Physics **45**, 829–840 (2004).

[57] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Limits for entanglement measures". Physical Review Letters **84**, 2014–2017 (2000).

[58] Hoi-Kwong Lo and Sandu Popescu. "Classical communication cost of entanglement manipulation: Is entanglement an interconvertible resource?". Physical Review Letters **83**, 1459–1462 (1999).

[59] Andreas Winter and Dong Yang. "Operational resource theory of coherence". Physical Review Letters **116**, 120404 (2016).

[60] Ingemar Bengtsson and Karol Życzkowski. "Geometry of quantum states. an introduction to quantum entanglement". Cambridge University Press. (2006).

[61] John Watrous. "Theory of quantum information". Cambridge University Press. (2018).

[62] Armin Uhlmann. "The "transition probability" in the state space of a *-algebra". Reports on Mathematical Physics **9**, 273–279 (1976).

[63] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. "Everything you always wanted to know about LOCC (but were afraid to ask)". Communications in Mathematical Physics **328**, 303–326 (2014).

[64] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. "Quantum nonlocality without entanglement". Physical Review A **59**, 1070–1091 (1999).

[65] Abbas El Gamal and Young-Han Kim. "Network information theory". Cambridge University Press. (2011).

[66] Thomas M. Cover and Joy A. Thomas. "Elements of information theory". Wiley Series in Telecommunications and Signal Processing. Wiley-Interscience. (2006). 2nd edition.

[67] Claude E. Shannon. "A mathematical theory of communication". Bell System Technical Journal **27**, 379–423 (1948).

[68] Nicolas J. Cerf and Christoph Adami. "Negative entropy and information in quantum mechanics". Physical Review Letters **79**, 5194–5197 (1997).

[69] Elliott H. Lieb and Mary Beth Ruskai. "Proof of the strong subadditivity of quantum-mechanical entropy". Journal of Mathematical Physics **14**, 1938–1941 (1973).

[70] Yury Polyanskiy and Sergio Verdú. "Arimoto channel coding converse and Rényi divergence". In Proceedings of the 48th Annual Allerton Conference on Communication, Control, and Computation. Pages 1327–1333. (2010).

[71] Mark M. Wilde, Andreas Winter, and Dong Yang. "Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy". Communications in Mathematical Physics **331**, 593–622 (2014).

[72] Hisaharu Umegaki. "Conditional expectations in an operator algebra, IV (entropy and information)". Kodai Mathematical Seminar Reports **14**, 59–85 (1962).

[73] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. "On quantum Rényi entropies: a new definition and some properties". Journal of Mathematical Physics **54**, 122203 (2013).

[74] Rupert L. Frank and Elliott H. Lieb. "Monotonicity of a relative Rényi entropy". Journal of Mathematical Physics **54**, 122201 (2013).

[75] Mark M. Wilde. "Optimized quantum f-divergences and data processing". Journal of Physics A **51**, 374002 (2018). arXiv:1710.10252.

[76] Nilanjana Datta. "Min- and max-relative entropies and a new entanglement monotone". IEEE Transactions on Information Theory **55**, 2816–2826 (2009).

[77] Nilanjana Datta. "Max-relative entropy of entanglement, alias log robustness". International Journal of Quantum Information **7**, 475–491 (2009).

[78] Francesco Buscemi and Nilanjana Datta. "The quantum capacity of channels with arbitrarily correlated noise". IEEE Transactions on Information Theory **56**, 1447–1460 (2010).

[79] Ligong Wang and Renato Renner. "One-shot classical-quantum capacity and hypothesis testing". Physical Review Letters **108**, 200501 (2012).

[80] Xin Wang and Mark M. Wilde. "Resource theory of asymmetric distinguishability". Physical Review Research **1**, 033170 (2019).

[81] Andreas Winter. "Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints". Communications in Mathematical Physics **347**, 291–313 (2016).

[82] Jens Eisert and Mark M Wilde. "A smallest computable entanglement monotone". In 2022 IEEE International Symposium on Information Theory (ISIT). Pages 2439–2444. IEEE (2022).

[83] Guifré Vidal. "Entanglement monotones". Journal of Modern Optics **47**, 355–376 (2000).

[84] Dong Yang, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Wei Song. "Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof". IEEE Transactions on Information Theory **55**, 3375–3387 (2009).

[85] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. "Colloquium: Quantum coherence as a resource". Reviews of Modern Physics **89**, 041003 (2017). arXiv:1609.02439.

[86] Karol Horodecki, Debbie Leung, Hoi-Kwong Lo, and Jonathan Oppenheim. "Quantum key distribution based on arbitrarily weak distillable entangled states". Physical Review Letters **96**, 070501 (2006).
[87] Matthias Christandl and Andreas Winter. "Uncertainty, monogamy, and locking of quantum correlations". IEEE Transactions on Information Theory **51**, 3159–3165 (2005).
[88] Bartosz Regula, Kaifeng Bu, Ryuji Takagi, and Zi-Wen Liu. "Benchmarking one-shot distillation in general quantum resource theories". Physical Review A **101**, 062315 (2020).
[89] Guifré Vidal and Rolf Tarrach. "Robustness of entanglement". Physical Review A **59**, 141–155 (1999).
[90] Berry Groisman, Sandu Popescu, and Andreas Winter. "Quantum, classical, and total amount of correlations in a quantum state". Physical Review A **72**, 032317 (2005).
[91] Karol Horodecki, Marek Winczewski, and Siddhartha Das. "Fundamental limitations on the device-independent quantum conference key agreement". Physical Review A **105**, 022604 (2022).
[92] Karol Horodecki and Gláucia Murta. "Bounds on quantum nonlocality via partial transposition". Physical Review A **92**, 010301(R) (2015).
[93] Eneet Kaur, Karol Horodecki, and Siddhartha Das. "Upper bounds on device-independent quantum key distribution rates in static and dynamic scenarios". Physical Review Applied**18** (2022).
[94] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. "Quantum conference key agreement: A review". Advanced Quantum Technologies **3**, 2000025 (2020).
[95] Stefan Bäuml. "On bound key and the use of bound entanglement". Master's thesis. Ludwig Maximilians Universität München. (2010).