

Quantum pseudoresources imply cryptography

Alex B. Grilo and Álvaro Yáñez *

Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France

Abstract

While one-way functions (OWFs) serve as the minimal assumption for computational cryptography in the classical setting, in quantum cryptography, we have even weaker cryptographic assumptions such as pseudo-random states, and EFI pairs, among others. Moreover, the minimal assumption for computational quantum cryptography remains an open question. Recently, it has been shown that pseudoentanglement is necessary for the existence of quantum cryptography (Goulão and Elkouss 2024), but no cryptographic construction has been built from it.

In this work, we study the cryptographic usefulness of quantum pseudoresources —a pair of families of quantum states that exhibit a gap in their resource content yet remain computationally indistinguishable. We show that quantum pseudoresources imply a variant of EFI pairs, which we call EPFI pairs, and that these are equivalent to quantum commitments and thus EFI pairs. Our results suggest that, just as randomness is fundamental to classical cryptography, quantum resources may play a similarly crucial role in the quantum setting.

Finally, we focus on the specific case of entanglement, analyzing different definitions of pseudoentanglement and their implications for constructing EPFI pairs. Moreover, we propose a new cryptographic functionality that is intrinsically dependent on entanglement as a resource.

*alvaro.yanguez@lip6.fr

1 Introduction

Many quantum resources are fundamental to achieving quantum advantage in information-processing tasks over conventional classical devices, e.g., entanglement [PV06, HHHH09], coherence [BCP14, SAP17], or "magic" [VHMGE14, HC17]. However, the manipulation of physical systems to operate with these resources is constrained in terms of time and space. Ignoring these computational limitations leads to an impractical characterization of such resources.

Inspired by complexity theory, a recent line of research studies these resources from a computational perspective. This phenomenon, known as *pseudoresources*, characterizes states that do not possess a given resource yet "look like" resourceful states to a computationally bounded observer [HBK24, BMB⁺24]. Among the different resources, the concept of *pseudoentanglement* [ABF⁺23, ABV23, GE24, LREJ25] stands out as a key example, where entanglement is the "hidden" resource of interest. More concretely, it describes the case where two families of states exhibit a large gap in the amount of their entanglement yet remain indistinguishable to a polynomial-time quantum adversary.

In classical cryptography, the resource of randomness plays a crucial role. Moreover, its computational variant, *pseudorandomness*, is at the core of symmetric cryptographic constructions. This naturally raises the question of the role quantum resources play in quantum cryptography. How can pseudoresource states be constructed from other cryptographic primitives? Which cryptographic functionalities can be implemented given the existence of pseudoresources?

In the specific case of pseudoentanglement, various constructions have been proposed, ranging from those based on One-Way Functions (OWFs)¹ for pure states [ABF⁺23, ABV23, LREJ25] to EFI pairs² for mixed states [GE24]. In particular, this latter construction establishes pseudoentanglement as a minimal assumption for the existence of most computationally based quantum cryptographic protocols. However, to the best of our knowledge, no cryptographic primitive has yet been constructed directly from pseudoentangled states.

Beyond entanglement, other quantum resources have also been explored from a computational complexity perspective. For instance, recent work has examined magic states [GLG⁺24] and coherence [HBK24] in the context of complexity theory. Moreover, based on *pseudorandom density matrices* (PRDMs), these resources have also been studied in the case of mixed states [BMB⁺24]. PRDMs, which represent density matrices that are computationally indistinguishable from Haar random ones, and pseudomagic pure states have both been shown to imply EFI pairs [BMB⁺24, GLG⁺24].³

In this work, we take a step further and demonstrate that quantum pseudoresources can be leveraged to construct useful cryptographic primitives. To do so, we introduce an extension of EFI pairs, which we call *EPFI pairs*, and show that they imply quantum commitment in a way similar to how EFI pairs do. More importantly, we present a general method for constructing EPFI pairs from quantum pseudoresources. As a corollary, this establishes that quantum pseudoresources can be used to construct several cryptographic primitives, including commitments, oblivious transfer, and secure multiparty computation.

¹In short, OWFs are functions that are easy to compute but hard to invert.

²An EFI pair consists of two efficiently generated quantum states which are far in trace distance, but which are indistinguishable by computationally bounded adversaries. See Definition 3.1 for a formal definition

³Actually, pseudomagic implies EPFI pairs, that we define in this work.

1.1 Our contribution

We describe now our contributions in more details.

1.1.1 Definition of EPFI pairs and constructing commitment schemes.

The cryptographic primitive of EFI pairs (Efficiently generated, statistically far and indistinguishable states) was first defined in [BCQ23], and it consists of a pair of states ρ and σ that are far in trace distance but cannot be efficiently distinguished by polynomial-time algorithms. In [BCQ23], they showed that EFI pairs are equivalent to quantum commitments, more specifically, to the statistically binding variant of canonical quantum commitments introduced in [Yan22]. Consequently, EFI pairs serve as a fundamental assumption for the existence of commitments, oblivious transfer, multiparty computation, and computational zero-knowledge proofs for non-trivial languages.

In order to achieve our results, we need to slightly modify such a definition as follows. We consider two keyed families of states $\{\rho_k\}_k$ and $\{\sigma_{k'}\}_{k'}$, and we require that for every k and k' , ρ_k is far from $\sigma_{k'}$ in trace distance, but are still indistinguishable by efficient algorithms. We call such pair of ensembles as EPFI pairs for Efficiently generated, pairwise statistically far and computationally indistinguishable families. We notice that an EFI pair can be seen as an EPFI pair in which each ensemble contains one element. However, EPFI pairs do not trivially imply EFI pairs: we can have families of states that are pairwise far but whose mixture is close.

In Section 3, we demonstrate that the existence of EPFI pairs of ensembles implies the existence of quantum commitments. Informally, a commitment scheme is a two-party cryptographic primitive in which a committer commits to a bit that remains hidden from the receiver until the committer chooses to reveal it. The scheme must satisfy two properties: *binding*, meaning the committer cannot change the committed value, and *hiding*, meaning the receiver cannot learn the value before the reveal phase.

We focus on the canonical quantum commitments introduced in [Yan22], where it is shown that proving either binding or hiding in the *semi-honest* setting—where both parties follow the protocol during the commitment phase—is sufficient. This model simplifies analysis by restricting adversarial behavior to the reveal phase and was proven in [Yan22] to be equivalent to stronger notions of binding, such as sum-binding [Unr16]. For completeness, we briefly explain this construction.

As with EFI pairs, EPFI pairs naturally lead to the construction of canonical quantum commitments.

- **Commit stage:** The committer commits to a bit b by generating a bipartite state $|\psi^b\rangle_{CR}$ and sending the register C to the receiver.
- **Reveal stage:** The committer discloses register R along with the bit b , allowing the receiver to verify the commitment by projecting onto $|\psi^b\rangle_{CR}$. If the verification fails, the receiver aborts.

In our construction, we introduce a classical key to accommodate the use of state ensembles. This modification does not alter the protocol since the key is also revealed in the opening stage. Our approach closely follows the honest statistical binding and computational hiding canonical quantum commitments construction from EFI pairs of [BCQ23]. Here, the committed register C contains a state sampled from one of the EPFI pairs. In the reveal stage, the committer provides

the receiver with the purification of the sampled state, the secret key associated with the state, and the committed bit.

Honest binding follows from the statistical distance between any state sampled from one family of the EPFI pair and all states from the opposing ensemble together with Uhlmann’s theorem [Uhl76]. Similarly, computational hiding follows from the computational indistinguishability of EPFI pairs. Thus, just as EFI pairs yield a statistically binding canonical quantum commitment when restricted to two algorithms, EPFI pairs provide the same commitment structure when generalized to two families of algorithms for two possible committed values. This new functionality, EPFI pairs, it is going to play a central role in the construction of cryptography from different quantum pseudoresources, as sketched in Figure 1.

1.1.2 EPFI from quantum pseudoresources.

We explore the role of pseudoresourced states in quantum cryptography and demonstrate how they can lead to the construction of EPFI pairs and thus, cryptography, as represented in Figure 1. In quantum information theory, a resource refers to any intrinsic property of a quantum system—such as entanglement, magic, or coherence—that provides an advantage for information processing tasks. Each resource is characterized by a corresponding set of free (resourceless) states and the free operations that cannot generate the resource. Various measures quantify these resources by evaluating, informally, how “far” a state is from the set of free states. One particularly relevant measure, and the one we adopt in this work, is the *relative entropy of resource*.

Informal definition 1 (η -gapped pseudoresource). *A pair of efficiently generated families of quantum states is said to have an η -gapped pseudoresource if there is at least an η -gap in the relative entropy of the resource of the states sampled from each one of the families, but these families are computationally indistinguishable.*

Therefore, under computational restrictions, the inherent resource properties of quantum states can be effectively concealed. This phenomenon has been extensively studied in the contexts of entanglement [ABF⁺23, ABV23, GE24, LREJ25], magic [GLG⁺24], and coherence [HBK24]. More generally, works such as [HBK24, BMB⁺24] have characterized pseudoresources for any resource monotone. In our approach, we focus on the relative entropy of resource—though the definition can be extended to any asymptotically continuous monotone function—to formalize the notion of a pseudoresource.

We construct EPFI pairs by assuming the existence of a pair of families of states with an η -gapped pseudoresource. The construction follows naturally: each family in the pseudoresourced pair directly corresponds to a family in the EPFI pair. The efficient generation and computational indistinguishability properties of EPFI pairs are immediate from the definition of an η -gapped pseudoresource. However, establishing statistical distance requires further analysis. Our approach relies on an inequality from [Win16] that relates the relative entropy of resources to trace distance. Informally, statistical fairness follows from the asymptotic continuity of the resource measure: when two states exhibit a significant gap in their resource value (in this case, relative entropy of resource), they must also exhibit a large gap in trace distance.

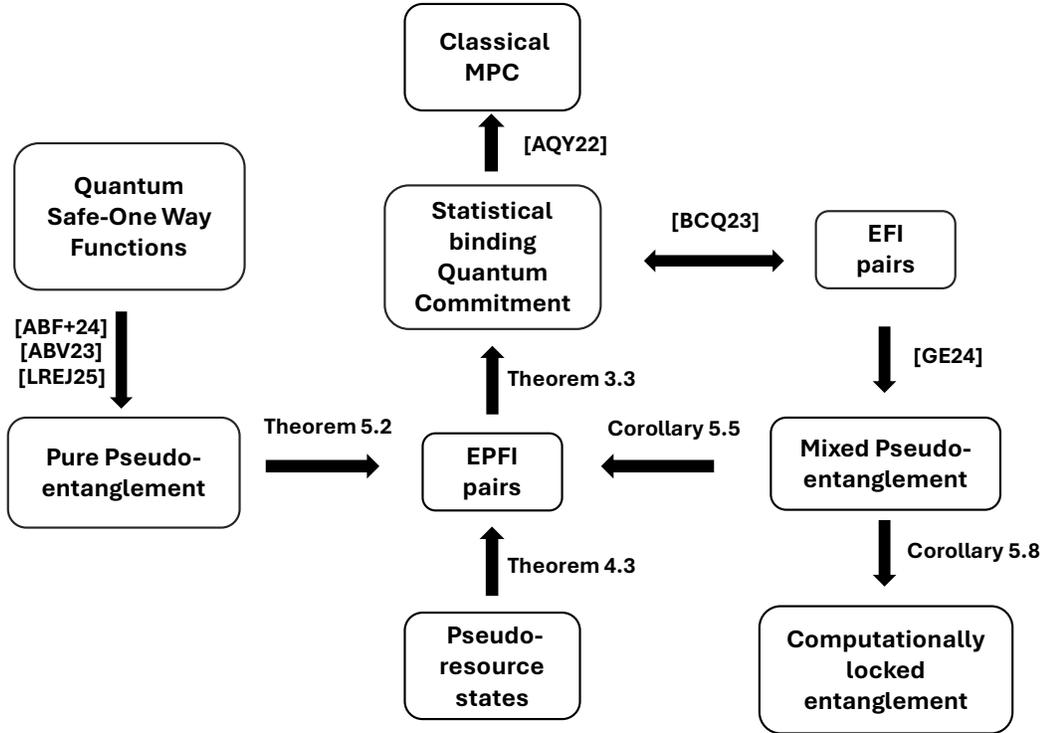


Figure 1: Summary of results and its relation with previous defined primitives.

1.1.3 Pseudoentanglement

Entanglement is the central resource in quantum information theory. In the study of resourcefulness under computational constraints, *pseudoentanglement* has received the most attention, leading to various constructions and definitions.

The first formalization of pseudoentanglement, introduced in [ABF⁺23], is restricted to families of pure states. This limitation arises not only from the construction itself but also from the choice of entanglement measure, as the entropy of entanglement lacks a well-defined operational meaning for mixed states. While later works, such as [ABV23, LREJ25], consider more general entanglement measures, their constructions are still pseudoentangled families of pure states.

Informal definition 2 (Pure η -gap pseudoentanglement). *A pair of efficiently generated families of quantum pure states is said to have η -gap pseudoentanglement if there is at least an η -gap in the entanglement entropy of the states sampled from each one of the families, while the ensembles are computationally indistinguishable.*

The proposed definition aligns with that of [ABF⁺23], with a particular emphasis on the entanglement entropy gap between states sampled from each family. The construction of EPFI pairs from families exhibiting η -gapped pseudoentanglement follows a similar approach to the one used for pseudoresources. Here, the relevant states are the reduced density matrices obtained by tracing

out the partition used to measure entanglement. Applying Fannes’ inequality [Fan73], we establish the statistical distance of the EPFI pair, while computational indistinguishability and efficient generation properties follow directly from the definition of pseudoentanglement.

Unlike pure pseudoentanglement, the entanglement in pseudoentangled mixed states cannot be quantified using the entanglement entropy. The necessity of an operational meaningful entanglement monotone motivated [ABV23] the use of the two most used measures of entanglement: the entanglement cost, E_C , and the distillable entanglement, E_D . Moreover, they proposed the use of computationally meaningful counterparts of these measures, in which the generation or distillation of entanglement has to be implementable by a poly-time algorithm. The definition of pseudoentanglement with these entanglement monotones allowed [GE24] to construct a pseudoentangled mixed state family from EFI pairs or, what it is the same, to prove mixed pseudoentanglement as a new minimal assumption for the existence of computational based cryptography, as sketched in Figure 1. Moreover, the use of other entanglement monotones also allows the existence of a maximal gap of a gap in the pseudoentangled families of $\Theta(n)$ vs 0 ⁴.

Informal definition 3 (Mixed η -gap pseudoentanglement). *A pair of efficiently generated families of quantum mixed states is said to have η -gap pseudoentanglement if there is at least an η -gap in the relative entropy of entanglement of the states sampled from each one of the families, while the ensembles are computationally indistinguishable.*

While previous definitions of pseudoentanglement have been extended to mixed states [ABV23, GE24], our formulation introduces key distinctions. We explicitly require both families to be efficiently preparable and quantify entanglement using an information-theoretic measure. The construction of EPFI pairs from mixed η -gapped pseudoentanglement follows a similar approach to prior cases, with the main difference being the inequality used to relate the regularised relative entanglement entropy to trace distance, which in this case is derived from [Win16]. Consequently, assuming a mixed η -gapped pseudoentanglement with $\eta \geq 2 + 1/\text{poly}(n)$, EPFI pairs exist.

At first glance, the use of an information-theoretic entanglement measure may seem restrictive. However, it actually represents a relaxation of previous definitions. Some families exhibit no gap in computational entanglement measures, yet EPFI pairs can still be constructed from them. Conversely, any pseudoentangled states with an $\eta \geq 2 + 1/\text{poly}(n)$ gap in their (asymptotic) computational entanglement as defined in [ABV23] measures imply the existence of EPFI pairs.

1.1.4 Computationally locked entanglement

The research of new quantum functionalities with no classical analogue has been recently motivated by the objective of finding the minimal assumption. Nevertheless, it is not clear which applications some of these new functionalities can have. Moreover, in the case of pseudoentanglement, it was proven and the minimal assumption [GE24] but no cryptographic functionality was proposed. After the construction of canonical quantum commitments and EFI pairs from pseudoentangled states, the main question that arises is the existence of a functionality that is inherently constructed from the existence of pseudoentanglement.

Informally, the *computationally locked entanglement* functionality is given by an efficiently generated family of states $\{\psi_{AB}^{k(\lambda)}\}_k$ which has high distillable entanglement, i.e. $\hat{E}_D^\epsilon(\{k, \psi_{AB}^k\}) \geq d$. This entanglement is efficiently distillable given the classical (or quantum) key k . Nevertheless,

⁴In contrast to pure pseudoentanglement, where the maximal gap is given by $\Theta(n)$ vs $\omega(\log(n))$.

without having access to the key, the family is computationally indistinguishable from a low entangled family $\{\psi_{AB}^{k(\lambda)}\}_k$, i.e., $\hat{E}_C^\epsilon(\{\psi_{AB}^{k(\lambda)}\}_k) \leq c$, where $c < d$. This construction can be seen as a dual case of the previously defined pseudoentanglement [GE24, ABF⁺23, ABV23]: in this case, the "highly entangled" family is the efficiently generated one while the "low-entangled" family does not have to. This functionality is also relaxation of our proposed definition for pseudoentanglement, in which both families have to be efficiently generated. Possible applications of such a functionality can be authenticated quantum teleportation or certified routing quantum networks. We leave as an open question if such a functionality can be built from weaker computational assumptions

1.2 Open questions

The study of quantum resources from a limited computational perspective is a promising area of research. In the case of entanglement, [LREJ25] has recently proven that in the case of pure states, the manipulation of entanglement given polynomially bounded operations diverges significantly from the unbounded framework. However, for general computational resource theories there is currently no accepted measure that captures the "amount" of a resource when one is restricted to efficient (e.g. polynomial-time) operations. A promising direction is to develop a notion of quantum relative entropy that is defined relative to a class of computationally limited operations.

Another fundamental question is the relationship between EPFI and pseudoresources with complexity classes. According to [Kre21], $PP \neq BQP$ is necessary for the existence of PRS; however, such a condition is not known for EFI pairs—and therefore our proposed primitives might be even weaker. Understanding whether the complexity condition differs from that of PRS would provide insights into a possible separation of MiniQCrypt into two distinct worlds.

The relation between pseudomagic and pseudoentanglement has been studied for pure states [GOL24]; however, it remains unexplored for mixed states. While the construction in [BMB⁺24] simultaneously exhibits both pseudoentanglement and pseudomagic, it is unclear whether they are independent in general. Moreover, demonstrating the possibility of constructing mixed pseudoentangled states without magic would be an intriguing result, suggesting that computational indistinguishability is independent of the resource of magic for mixed states.

Lastly, our results closely depend on Fannes-type inequalities, and proving tighter versions of them for the different resources would directly improve the security of our cryptographic constructions.

2 Preliminaries

2.1 Notation

Quantum states are represented as density matrices $\rho \in \mathcal{B}_1(\mathcal{H})$. The set of states is defined as $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}_1(\mathcal{H}) \mid \rho \geq 0, \text{tr } \rho = 1\}$. A bipartite entangled state is defined as a state that is not separable, i.e., it cannot be written as $\rho_{AB} = \sum_i p(i) \rho_A^i \otimes \rho_B^i$. A maximally bipartite entangled state is given by $|\Psi\rangle = \sum_{i=0}^{d-1} |ii\rangle / \sqrt{d} \in \mathcal{H}_A \otimes \mathcal{H}_B$. In the case of the space of dimension 2, a maximally entangled state is known as a Bell state, and it is of the form $|\Phi\rangle = (|00\rangle + |11\rangle) / \sqrt{2} \in \mathcal{H}_A \otimes \mathcal{H}_B$, with $\mathcal{H}_A = \mathcal{H}_B = (\mathbb{C}^2)^{\otimes n}$. We denote by $\mathcal{U}(\mathcal{H})$ the set of unitary operators. The fidelity of two states ρ and σ is given by $F(\rho, \sigma) = [\text{Tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})]^2$.

The probability of distinguishing two density matrices is upper-bounded by $\frac{1}{2}(1+\Delta(\rho, \sigma))$, where $\Delta(\rho, \sigma)$ is the trace distance. The states ρ and σ are said to be statistically close when a negligible function $\mu(\lambda)$ exists such that $\Delta(\rho, \sigma) \leq \mu(\lambda)$. Given a *security parameter* λ , $\mu(\lambda)$ is $\text{negl}(\lambda)$, i.e., negligible, if, for every fixed c , $\mu(\lambda) = o(1/\lambda^c)$.

In the Landau notation, given two functions $f(n)$ and $g(n)$, we write $f(n) = o(g(n))$ if $\lim_{n \rightarrow \infty} f(n)/g(n) = 0$. In the same way, $f(n) = \omega(g(n))$ if $\lim_{n \rightarrow \infty} f(n)/g(n) = \infty$. $f(n) = O(g(n))$ if there exist a constant $C > 0$ such that $\lim_{n \rightarrow \infty} f(n)/g(n) \leq C$. Similarly, $f(n) = \Omega(g(n))$ if there exist a constant $C > 0$ such that $\lim_{n \rightarrow \infty} f(n)/g(n) \geq C$. Lastly, $f(n) = \Theta(g(n))$ if both $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

2.2 LOCC maps

In the study of entanglement theory, one of the main objectives is the characterization of the entanglement. In order to understand how much entanglement a quantum state has, the first step is to manipulate the quantum state. Quantum channels are completely positive and trace preserving maps that transform quantum states into quantum states. In the study of entanglement, the relevant quantum channels are the ones that does not increase (or create) entanglement. A natural class that arises from a practical perspective is the one in which the parties are locally separated, and they are only allowed to perform classical communication.

Definition 2.1 (LOCC map [ABV23]). *A quantum channel is said to be an LOCC map*

$$\Gamma : \mathcal{H}_A \otimes \mathcal{H}_B \mapsto \mathcal{H}_{\bar{A}} \otimes \mathcal{H}_{\bar{B}}$$

if it can be implemented by a two-party interactive protocol where each party can implement arbitrary local quantum computations and the two parties can exchange arbitrary classical communication.

Definition 2.2 (Circuit description of an LOCC map [ABV23]). *Given an LOCC map Γ , its circuit description is given by two families of circuits $\{\mathcal{C}_{A,i}\}_{i \in \{1, \dots, r\}}$ and $\{\mathcal{C}_{B,i}\}_{i \in \{1, \dots, r\}}$, each of them acting on $n_A + t_A + c$ and $n_B + t_B + c$ qubits respectively, such that the following procedure implements the map Γ on an arbitrary input $\varphi_{AB} \in (\mathbb{C}^2)^{\otimes n_A} \otimes (\mathbb{C}^2)^{\otimes n_B}$:*

1. Registers A and B of n_A and n_B qubits are initialized in the state φ_{AB} . Ancilla registers A' and B' of t_A and t_B qubits are initialized in the $|0\rangle$ state. Communication register C is also initialized in the $|0\rangle$ state.
2. For $i = 1, \dots, r$, the circuit $\mathcal{C}_{A,i}$ is applied to registers A , A' and C . Then, register C is measured in the computational basis. Thirdly, the circuit $\mathcal{C}_{B,i}$ is applied to registers B , B' and C . Lastly, register C is measured in the computational basis.
3. The final output of the LOCC map in the subspace $\mathcal{H}_{\bar{A}}$ correspond to the state in the registers A and A' . In the same way, the state in the registers B and B' is the final output on $\mathcal{H}_{\bar{B}}$.

A family of LOCC maps $\{\hat{\Gamma}_\lambda\}_{\lambda \in \mathbb{N}}$ is said to be efficient if there exists a polynomial c such that for all λ , $\hat{\Gamma}_\lambda$ has a circuit description whose total number of gates, including the ancilla creation and qubit measurements, is at most $c(\lambda)$.

2.3 Entanglement measures

We will now introduce some functions that allow the quantification of entanglement. The most fundamental measure of entanglement in the case of pure states is given by the entanglement entropy.

Definition 2.3 (Entanglement entropy). *Given a bipartite state $\rho_{AB} = |\psi\rangle\langle\psi|_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, its entanglement entropy is defined as*

$$E_{A/B}(\rho_{AB}) := S(\rho_A) = S(\rho_B),$$

where $\rho_A = \text{Tr}_B(\rho_{AB})$, $\rho_B = \text{Tr}_A(\rho_{AB})$ and $S(\rho) = -\text{Tr}(\rho \log \rho)$ is the von Neumann entropy.

Nevertheless, in the case of mixed states, the entanglement entropy is not operationally meaningful. This problem leads to several measures of entanglement [PV06]. Let us introduce two of the most relevant ones.

Definition 2.4 (One-shot entanglement cost [ABV23]). *Let $\epsilon \in [0, 1]$, Γ be an LOCC map. The one-shot entanglement cost of a bipartite state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is given by*

$$E_C^\epsilon(\rho_{AB}) = \inf_{n, \Gamma} \{n | 1 - F(\rho_{AB}, \Gamma(\Phi^{\otimes n})) \leq \epsilon\},$$

where $F(\rho, \sigma)$ is the fidelity, $\Phi = |\Phi\rangle\langle\Phi|$ and $|\Phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a Bell pair.

Definition 2.5 (One-shot distillable entanglement [ABV23]). *Let $\epsilon \in [0, 1]$, Γ be an LOCC map. The one-shot distillable entanglement of a bipartite state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is given by*

$$E_D^\epsilon(\rho_{AB}) = \sup_{m, \Gamma} \{m | 1 - F(\Gamma(\rho_{AB}), \Phi^{\otimes m}) \leq \epsilon\},$$

where $F(\rho, \sigma)$ is the fidelity, $\Phi = |\Phi\rangle\langle\Phi|$ and $|\Phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a Bell pair.

Let us now define the asymptotic versions of the measures of entanglement, which describe the rate at which the entanglement can be extracted (or diluted).

Definition 2.6 (Asymptotic IID distillable entanglement). *The asymptotic IID distillable entanglement of a bipartite state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ is given by*

$$E_D^\infty(\rho) = \inf_{\epsilon \in (0, 1]} \liminf_{t \rightarrow \infty} \frac{1}{t} E_D^\epsilon(\rho_{AB}^{\otimes t}).$$

Definition 2.7 (Asymptotic IID entanglement cost). *The asymptotic IID entanglement cost of a bipartite state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ is given by*

$$E_C^\infty(\rho) = \inf_{\epsilon \in (0, 1]} \limsup_{t \rightarrow \infty} \frac{1}{t} E_C^\epsilon(\rho_{AB}^{\otimes t}).$$

Previous measures of entanglement are specially relevant since any entanglement measure $E(\rho_{AB})$ has to fulfill that $E_D^\infty(\rho_{AB}) \leq E(\rho_{AB}) \leq E_C^\infty(\rho_{AB})$, i.e., they are extremal [DHR02]. One of the entanglement entropies that will be used in this paper is the regularised relative entropy of entanglement.

Definition 2.8 (Regularised relative entropy of entanglement). *Given a bipartite state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, its regularised entropy of entanglement is given by,*

$$E_R^\infty(\rho_{AB}) = \lim_{n \rightarrow \infty} \frac{1}{n} E_R(\rho_{AB}^{\otimes n}),$$

where $E_R(\rho) := \min_{\sigma_{AB} \in \mathcal{S}_{A:B}} D(\rho_{AB} || \sigma_{AB})$ is the relative entropy of entanglement and $D(\rho || \sigma) = \text{Tr}[\rho(\log \rho - \log \sigma)]$ is the relative entropy.

2.4 Computational entanglement measures

We have previously defined the information theoretic measures of entanglement. Nevertheless, we can restrict to the case in which the operations have to be efficiently implementable, as proposed by [ABV23]. The following definitions are meaningfully defined over families of states and in the asymptotic limit.

Definition 2.9 (Computational one-shot entanglement cost [ABV23]). *Let $\epsilon : \mathbb{N}_+ \rightarrow [0, 1]$ and $\lambda \in \mathbb{N}_+$. Fix polynomial functions $n_A, n_B : \mathbb{N}_+ \rightarrow \mathbb{N}_+$. Let $\{\rho_{AB}^\lambda\}_\lambda$ be a family of quantum states such that, for any $\lambda \geq 1$, $\rho_{AB}^\lambda \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a bipartite state on $n_A(\lambda) + n_B(\lambda)$. The function $c : \mathbb{N} \rightarrow \mathbb{N}$ is an upper bound on the computational entanglement cost of the family $\{\rho_{AB}^\lambda\}_\lambda$, i.e. $\hat{E}_C^\epsilon(\{\rho_{AB}^\lambda\}_\lambda) \leq c$, if there exists an efficient LOCC map family $\{\hat{\Gamma}^\lambda\}_\lambda$ such that, for each $\lambda \geq 1$, $\hat{\Gamma}^\lambda$ takes an input $c(\lambda)$ EPR pairs, and*

$$1 - F(\rho_{AB}^\lambda, \hat{\Gamma}^\lambda(\Phi^{\otimes c})) \leq \epsilon(\lambda), \quad \forall k \in \mathbb{N}_+.$$

Definition 2.10 (Computational one-shot distillable entanglement [ABV23]). *Let $\epsilon : \mathbb{N}_+ \rightarrow [0, 1]$ and $\lambda \in \mathbb{N}_+$. Fix polynomial functions $n_A, n_B : \mathbb{N}_+ \rightarrow \mathbb{N}_+$. Let $\{\rho_{AB}^\lambda\}_\lambda$ be a family of quantum states such that, for any $\lambda \geq 1$, $\rho_{AB}^\lambda \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a bipartite state on $n_A(\lambda) + n_B(\lambda)$. The function $d : \mathbb{N} \rightarrow \mathbb{N}$ is a lower bound on the computational distillable entanglement of the family $\{\rho_{AB}^\lambda\}_\lambda$, i.e. $\hat{E}_D^\epsilon(\{\rho_{AB}^\lambda\}_\lambda) \geq d$, if there exists an efficient LOCC map family $\{\hat{\Gamma}^\lambda\}_\lambda$ such that, for each $\lambda \geq 1$, $\hat{\Gamma}^\lambda$ outputs a $2d(\lambda)$ -qubit state, and*

$$1 - F(\hat{\Gamma}^\lambda(\rho_{AB}^\lambda), \Phi^{\otimes d}) \leq \epsilon(\lambda), \quad \forall k \in \mathbb{N}_+.$$

We can adapt this definition to the case where, for each parameter $\lambda \in \mathbb{N}$, the different possible states of size λ are indexed by a classical key $k \in \{0, 1\}^{\kappa(\lambda)}$, with $\kappa : \mathbb{N}_+ \rightarrow \mathbb{N}_+$. Therefore, from now on, we will refer to the family of states as $\{\rho_{AB}^k\}_k$. Please, note that the security parameter λ is implicit in the size of the keys k . In the same way, the action of the LOCC map for the distillation of entanglement has to have access to the key k . Therefore, the distillation map is now given by $\Gamma(k, \rho^k)$ which input is the state $|k\rangle\langle k|_{A'} \otimes \rho_{AB}^k \otimes |k\rangle\langle k|_{B'}$, where the bipartition is $A'A : B'B$. This map has to efficiently distill the entanglement from states associated with all possible keys. The same applies to the cost of generating all the states associated with all possible keys. The corresponding keys of the states can be extended to the case of quantum keys (more specifically, EFI pairs), as proven by [GE24].

Definition 2.11 (Uniform computational one-shot distillable entanglement [ABV23]). *Let $\epsilon : \mathbb{N}_+ \rightarrow [0, 1]$ and $\lambda \in \mathbb{N}_+$. Fix polynomial functions $n_A, n_B : \mathbb{N}_+ \rightarrow \mathbb{N}_+$. Let $\{\rho_{AB}^k\}_{k \in \{0, 1\}^{\kappa(\lambda)}}$ be a family of quantum states such that, for any $\lambda \geq 1$, $\rho_{AB}^k \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a bipartite state on $n_A(\lambda) + n_B(\lambda)$.*

The function $d : \mathbb{N}_+ \rightarrow \mathbb{N}_+$ is a lower bound on the computational distillable entanglement of the family $\{k, \rho_{AB}^k\}$, i.e. $\hat{E}_D^\epsilon(\{k, \rho_{AB}^k\}) \geq d$, if there exists an efficient LOCC map family $\{\hat{\Gamma}^\lambda\}_\lambda$ such that, for each $\lambda \geq 1$, $\hat{\Gamma}^\lambda$ outputs a $2d(\lambda)$ -qubit state, and

$$1 - F(\hat{\Gamma}^\lambda(k, \rho_{AB}^k), \Phi^{\otimes d}) \leq \epsilon(\lambda), \quad \forall \lambda \in \mathbb{N}_+, \quad \forall k \in \{0, 1\}^{\kappa(\lambda)}.$$

Definition 2.12 (Uniform computational one-shot entanglement cost[ABV23]). Let $\epsilon : \mathbb{N}_+ \rightarrow [0, 1]$ and $\lambda \in \mathbb{N}_+$. Fix polynomial functions $n_A, n_B : \mathbb{N}_+ \rightarrow \mathbb{N}_+$. Let $\{\rho_{AB}^k\}_k$ be a family of quantum states such that, for any $\lambda \geq 1$ and $k \in \{0, 1\}^{\kappa(\lambda)}$, $\rho_{AB}^k \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a bipartite state on $n_A(\lambda) + n_B(\lambda)$. The function $c : \mathbb{N} \rightarrow \mathbb{N}$ is an upper bound on the computational entanglement cost of the family $\{k, \rho_{AB}^k\}$, i.e., $\hat{E}_C^\epsilon(\{k, \rho_{AB}^k\}) \leq c$, if there exists an efficient LOCC map family $\{\hat{\Gamma}^\lambda\}_\lambda$ such that, for each $\lambda \geq 1$, $\hat{\Gamma}^\lambda$ takes an input $c(\lambda)$ EPR pairs, and

$$1 - F(\rho_{AB}^k, \hat{\Gamma}^\lambda(k, \Phi^{\otimes c})) \leq \epsilon(\lambda), \quad \forall \lambda \in \mathbb{N}_+, \quad \forall k \in \{0, 1\}^{\kappa(\lambda)}.$$

2.5 Auxiliary lemmas

Let us now introduce the quantum information theory tools that we make use of.

Theorem 2.13 (Holevo-Helstrom [Hol73, Hel69]). Given two mixed states ρ and σ , the best success probability to distinguish them is given by $\frac{1}{2}(1 + \Delta(\rho, \sigma))$, where $\Delta(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$. Moreover, given n -copies,

$$\Delta(\rho^{\otimes n}, \sigma^{\otimes n}) \geq 1 - \exp(-n\Delta(\rho, \sigma)/2). \quad (1)$$

Theorem 2.14 (Uhlmann's theorem [Uhl76]). Let $\rho \in \mathcal{B}_1(\mathcal{H}_1)$ and $\sigma \in \mathcal{B}_1(\mathcal{H}_1)$ be a pair of density operators, where $\rho = \text{Tr}_2(|\psi\rangle\langle\psi|)$ for $|\psi\rangle \in \mathcal{B}_1(\mathcal{H}_1 \otimes \mathcal{H}_2)$. It holds that $F(\rho, \sigma) = \max\{|\langle\psi|\eta\rangle| : |\eta\rangle \in \mathcal{B}_1(\mathcal{H}_1 \otimes \mathcal{H}_2) \text{ is a pure state s.t. } \text{Tr}_2(|\eta\rangle\langle\eta|) = \sigma\}$.

Lemma 2.15 (Fannes inequality [Fan73]). Given two density operators $\rho \in \mathcal{B}_1(\mathcal{H})$ and $\sigma \in \mathcal{B}_1(\mathcal{H})$, it holds that

$$|S(\rho) - S(\sigma)| \leq 2\Delta(\rho, \sigma) \log d + c(\Delta(\rho, \sigma)), \quad (2)$$

where $c(x) := \min\{-x \log x, 1/2e\}$ and $S(\rho) = -\text{Tr}(\rho \log \rho)$ is the von Neumann entropy.

This well known inequality of information theory can be extended to the quantum relative entropy,

Lemma 2.16 (Fannes type inequality for the quantum relative entropy [Win16]). For a closed, convex and bounded set \mathcal{F} of positive semidefinite operators, containing at least one full rank operator, let

$$\kappa = \sup_{\tau, \tau'} D_C(\tau) - D_C(\tau')$$

be the largest variation of $D_C(\tau) := \min_{\gamma \in \mathcal{C}} D(\tau||\gamma)$, where $D(\rho||\gamma) = \text{Tr} \rho(\log(\rho) - \log(\gamma))$ is the quantum relative entropy. Then, for any two states ρ and σ with $\Delta(\rho, \sigma) \leq \epsilon$,

$$|D_C(\rho) - D_C(\sigma)| \leq \epsilon\kappa + (1 + \epsilon)h\left(\frac{\epsilon}{1 + \epsilon}\right), \quad (3)$$

where $h(\cdot)$ is the binary entropy.

Moreover, in the specific case of entanglement, it can be related to the relative entropy of entanglement,

Lemma 2.17 (Fannes type inequality for the regularised relative entropy of entanglement [Win16, DH99, Chr06]). *Given two states $\rho_{AB}, \sigma_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, the difference on their regularised relative entropy of entanglement is upper bounded by*

$$|E_R^\infty(\rho_{AB}) - E_R^\infty(\sigma_{AB})| \leq \epsilon \log d + (1 + \epsilon)h\left(\frac{\epsilon}{1 + \epsilon}\right),$$

where $\Delta(\rho, \sigma) \leq \epsilon$ and $h(\cdot)$ is the binary entropy.

2.6 Quantum Commitment

We focus on the construction of *canonical quantum commitments*, which is defined as follows.

Definition 2.18 (Canonical quantum commitment [Yan22]). *Given an ensemble of polynomial-time uniformly generated quantum circuit pair $\{(Q_{\lambda,0}, Q_{\lambda,1})\}_\lambda$, a canonical quantum commitment scheme is defined by the following stages:*

- **Commit stage:** *the committer chooses the committed bit $b \in \{0, 1\}$ and performs the quantum circuit $Q_{\lambda,b}$ to the register pair (C, R) , initialized in the $|0\rangle$ state⁵. Then the committer sends the register C to the receiver, i.e., the state $\rho_{\lambda,b} := \text{Tr}_R(Q_{\lambda,b}|0\rangle\langle 0|_{CR} Q_{\lambda,b}^\dagger)$.*
- **Reveal stage:** *the committer sends the bit b and the register R to the receiver. The receiver performs $Q_{\lambda,b}^\dagger$ on (C, R) and aborts if the measured registers are not in the $|0\rangle$ state.*

Definition 2.19 (Computational hiding). *Given a canonical quantum commitment scheme in which the committed states are given by the families of mixed states $\{\rho_{\lambda,0}\}_\lambda$ and $\{\rho_{\lambda,1}\}_\lambda$, the scheme is computationally hiding if, for any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:*

$$\left| \mathbb{P}\left[\mathcal{D}(\sigma_\lambda, \rho_{\lambda,0}^{\otimes m}) = 1\right] - \mathbb{P}\left[\mathcal{D}(\sigma_\lambda, \rho_{\lambda,1}^{\otimes m}) = 1\right] \right| \leq \nu(\lambda).$$

Definition 2.20 (Honest statistical binding [Yan22]). *A canonical quantum commitment scheme satisfies honest statistical binding if, for any auxiliary state $|\psi\rangle$ and any unitary $U \in \mathcal{U}(\mathcal{H})$ there exists a negligible function $\nu(\lambda) > 0$ such that:*

$$\left\| \left(Q_{\lambda,1} \otimes \text{Id}_Z |0\rangle\langle 0|_{CR} Q_{\lambda,1}^\dagger \otimes \text{Id}_Z \right) \left(\text{Id}_C \otimes U_{RZ} \right) \left(Q_{\lambda,0} |0\rangle_{CR} \otimes |\psi\rangle_Z \right) \right\|_2 \leq \nu(\lambda). \quad (4)$$

⁵For simplicity we write the tensor product of k registers in the $|0\rangle$ state as $|0\rangle$ (instead of $|0\rangle^{\otimes k}$), when it is clear from the context.

Informally, the honest-binding property allows the receiver to cheat only in the reveal stage of the commitment functionality. As proven by [Yan22], honest binding in the canonical quantum commitment is equivalent to the notion of sum-binding [Unr16]. Moreover, since sum-binding is equivalent to AQY binding [AQY21, MY22], oblivious transfer and multiparty computing can be constructed from it [BCKM21, GLSV21]. From now on, we will refer to the honest statistical binding commitments as statistical binding commitments.

We notice that the construction of [Yan22] can be modified with commitments generated by a pair of uniformly generated families of quantum circuits $\left(\{Q_0^{k(\lambda)}\}_{k \in \{0,1\}^{\kappa(\lambda)}}, \{Q_1^{k'(\lambda)}\}_{k' \in \{0,1\}^{\kappa(\lambda)}}\right)$.

To commit to a bit $b \in \{0, 1\}$, the committer first chooses a secret key k (or k') uniformly at random and then applies the corresponding circuit $Q_b^{k(\lambda)}$, preparing the state $|\Psi_b^{k(\lambda)}\rangle_{CR} = Q_b^{k(\lambda)} |0\rangle_{CR}$. Then, they send the commitment register C as in Definition 2.18. In the reveal phase, the committer sends to the receiver the chosen key in the reveal stage together with b and the register R .

The statistical binding property in this setting requires that for all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$,

$$\left\| \left(Q_1^{k'(\lambda)} \otimes \text{Id}_Z |0\rangle \langle 0|_{CR} Q_1^{\dagger k'(\lambda)} \otimes \text{Id}_Z \right) \left(\text{Id}_C \otimes U_{RZ} \right) \left(Q_0^{k(\lambda)} |0\rangle_{CR} \otimes |\psi\rangle_Z \right) \right\|_2 \leq \nu(\lambda), \quad (5)$$

Likewise, the computational hiding property in this case is given by,

$$\left| \mathbb{P}_{k(\lambda)} \left[\mathcal{D}(\sigma_\lambda, \rho_{k(\lambda),0}^{\otimes m}) = 1 \right] - \mathbb{P}_{k'(\lambda)} \left[\mathcal{D}(\sigma_\lambda, \rho_{k'(\lambda),1}^{\otimes m}) = 1 \right] \right| \leq \nu(\lambda). \quad (6)$$

When using families of algorithms for committing instead of a pair of algorithms, the condition on the binding is stronger, i.e., the committing states have to be pairwise honest statistically binding. In this case, the definition of honest statistical binding for families of quantum circuits (Eq. 5) implies the definition given by Definition 2.20. Moreover, since we have an honest committer, we still consider the mixture over the keys in the hiding property.

3 EPFI pairs imply quantum commitments

In this section, we focus on the definition of EPFI and show how to construct quantum commitments from it.

We start by recalling the definition of EFI pairs [BCQ23].

Definition 3.1 (EFI pair). *A pair of mixed states $(\rho_{0,\lambda}, \rho_{1,\lambda})$ is an EFI pair, if*

- **Efficient generation:** *there exists a QPT algorithm A that on input $(1^\lambda, b)$ outputs $\rho_{b,\lambda}$.*
- **Statistical distance:** $\Delta(\rho_{0,\lambda}, \rho_{1,\lambda}) \geq \Omega\left(\frac{1}{\text{poly}(\lambda)}\right)$.
- **Computationally indistinguishability:** *for any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:*

$$\left| \mathbb{P} \left[\mathcal{D}(\sigma_\lambda, \rho_{\lambda,0}^{\otimes m}) = 1 \right] - \mathbb{P} \left[\mathcal{D}(\sigma_\lambda, \rho_{\lambda,1}^{\otimes m}) = 1 \right] \right| \leq \nu(\lambda).$$

As aforementioned, it was proven that EFI pairs of states are equivalent to quantum commitments [BCQ23]. In this work, we define EPFI pairs by refining the requirements for EFI pairs.

Definition 3.2 (EPFI pair). A pair of ensembles of mixed states $(\{\psi_{k(\lambda)}\}_{k(\lambda)}, \{\phi_{k'(\lambda)}\}_{k'(\lambda)})$ indexed by $k, k' \in \{0, 1\}^{\kappa(\lambda)}$ is an **Efficiently generated, pairwise far and computational indistinguishable pair** (EPFI pair), if

- **Efficient generation:** Given $k(\lambda)$ (or $k'(\lambda)$), there exists a QPT algorithm A that on input $(1^\lambda, k, b)$ (or $(1^\lambda, k', b)$) outputs $\psi_{k(\lambda)}$ (or $\phi_{k'(\lambda)}$).
- **Pairwise statistically far:** For all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$,

$$\Delta(\psi_{k(\lambda)}, \phi_{k'(\lambda)}) \geq \Omega\left(\frac{1}{\text{poly}(\lambda)}\right).$$

- **Computationally indistinguishability:** for any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:

$$\left| \mathbb{P}_{k(\lambda)} \left[\mathcal{D}(\sigma_\lambda, \psi_{k(\lambda)}^{\otimes m}) = 1 \right] - \mathbb{P}_{k'(\lambda)} \left[\mathcal{D}(\sigma_\lambda, \phi_{k'(\lambda)}^{\otimes m}) = 1 \right] \right| \leq \nu(\lambda).$$

The main difference between both primitives is that each element of each ensemble has to be statistically far in terms of trace distance from every element of the other ensemble, while computationally indistinguishability holds for the ensemble itself.

We can now prove the main result of this section, which is the construction of a canonical quantum commitment from EPFI.

Theorem 3.3. Assuming the existence of EPFI pairs of mixed states, there exists statistically binding and computationally hiding canonical quantum commitments.

Proof. Let $\{Q_\psi^k\}_k$ and $\{Q_\phi^{k'}\}_{k'}$ be the two families of algorithms that generate the corresponding families of states $\{\psi_k\}_k$ and $\{\phi_{k'}\}_{k'}$ ⁶. The construction of the canonical quantum commitment is as follows. Let the algorithms $\{Q_{b,\lambda}^k\}_k$ with $b = \{0, 1\}$ corresponds to the aforementioned $\{Q_\psi^k\}_k$ and $\{Q_\phi^{k'}\}_{k'}$, i.e., each family of states corresponds to one value of b . The committer generates λ copies of the state by applying $\bigotimes_{i=1}^{\text{poly}(\lambda)} (Q_{b,\lambda}^k)_i$. Then, the committed state defined in Definition 2.18 is given by $\rho_{C,b}^{\otimes \text{poly}(\lambda)}$, where $\rho_{C,b} = \text{Tr}_R(Q_b^k |0\rangle\langle 0|_{CR} Q_b^{k\dagger})$ is a state from the EPFI ensemble (Definition 3.2). For the opening, the committer sends the λ registers R , together with the key k ⁷ and the committed bit b .

Let us first prove honest statistical binding. Given the two states ψ_k and $\phi_{k'}$, $\Delta(\psi_k, \phi_{k'}) \geq \Omega(1/\text{poly}(\lambda))$ by definition of the EPFI. Lastly, by taking polynomially many copies of the states, $\Delta(\psi_k^{\otimes \text{poly}(\lambda)}, \phi_{k'}^{\otimes \text{poly}(\lambda)}) \geq 1 - \text{negl}(\lambda)$ by Theorem 2.13. Moreover, due to the fact that $(F(\rho, \sigma))^2 + (\Delta(\rho, \sigma))^2 \leq 1$,

$$F\left(\psi_k^{\otimes \text{poly}(\lambda)}, \phi_{k'}^{\otimes \text{poly}(\lambda)}\right) \leq \sqrt{1 - \left(\Delta\left(\psi_k^{\otimes \text{poly}(\lambda)}, \phi_{k'}^{\otimes \text{poly}(\lambda)}\right)\right)^2} \leq \text{negl}(\lambda). \quad (7)$$

⁶We omit the security parameter λ for simplicity.

⁷Please, note that the construction can be extended to quantum keys, i.e., the key is a quantum state, in the subspace of the registers R .

Therefore, by Uhlman’s theorem (Theorem 2.14), the scheme satisfies honest binding (Eq. 5).

Computational hiding follows from the computational indistinguishability property of the EPFI pairs: without the key, a distinguisher cannot infer the ensemble from which the state has been sampled, satisfying Eq. 6. □

4 Pseudoresources and quantum cryptography

In this section, we establish a foundational connection between computational-based quantum cryptography and resource theories. We begin by briefly introducing the formalism of resource theories, define the concept of *pseudoresource*, and finally discuss how the existence of pseudoresources implies the existence of EFI pairs of ensembles and, thus, computational based cryptography.

4.1 Resource theory and pseudoresources

Quantum resource theories provide a systematic framework for studying properties of quantum systems that are crucial for quantum information processing tasks [CG19]. A quantum resource theory $\mathcal{R} = (\mathcal{F}, \mathcal{O})$ is characterized by a set of free states \mathcal{F} , and a set of free operations \mathcal{O} . The free states, defined as $\mathcal{F}(\mathcal{H}) \subseteq \mathcal{S}(\mathcal{H})$, represent states that lack the resource of interest. A completely positive trace-preserving (CPTP) map $\Lambda : \mathcal{B}(\mathcal{H}_1) \rightarrow \mathcal{B}(\mathcal{H}_2)$ belongs to the set \mathcal{O} if, for every $\sigma \in \mathcal{F}$, it holds that $\Lambda(\sigma) \in \mathcal{F}$. For instance, in the case of entanglement, the free states consist of the set of separable states, and we can pick the set of free operations as LOCC maps.

The set of properties that defines the resourced families of states that are necessary for our construction are:

1. The set of free states, $\mathcal{F}(\mathcal{H})$, is convex and closed.
2. $\mathcal{F}(\mathcal{H})$ contains a full-rank state.

We notice that in our case, we only consider finite dimension states and therefore property 1 implies that $\mathcal{F}(\mathcal{H})$ is bounded, which is also required. These properties are a relaxation of the *Brandão-Plenio axioms* [BP10], and they are satisfied by many resource theories such as magic, coherence, entanglement or athermality [CG19].

There exist several measures for quantifying resources in quantum information theory, ranging from geometric to witness-based approaches. Typically, these measures assess the resource content of a state by evaluating its “distance” from the set of free states. In this work, we focus on entropic measures, and more specifically, on the *relative entropy of resource*.

Definition 4.1 (Relative entropy of resource). *Given a state $\rho \in \mathcal{S}(\mathcal{H})$ and a set of free states $\mathcal{F}(\mathcal{H}) \subseteq \mathcal{S}(\mathcal{H})$, its relative entropy of resource is defined as*

$$R_{rel}(\rho) := \min_{\sigma \in \mathcal{F}} D(\rho || \sigma), \tag{8}$$

where $D(\rho || \sigma) = \text{Tr}[\rho(\log(\rho) - \log(\sigma))]$ is the quantum relative entropy.

When taking into account computationally bounded operations, families of states that can be distinguished in the asymptotic regime might become indistinguishable against polynomially bounded

quantum adversaries. This property becomes even more interesting when these states have very different properties. We focus on the case in which both families have a substantial difference in terms of resources.

Definition 4.2 (η -gap pseudoresource). *Let $\lambda \in \mathbb{N}_+$ and $\eta : \mathbb{N}_+ \rightarrow \mathbb{N}_+$ be arbitrary. A pair of families $\{\psi_{k(\lambda)}\}_{k(\lambda)}$ and $\{\phi_{k'(\lambda)}\}_{k'(\lambda)}$ of (potentially mixed) states indexed by $k(\lambda), k'(\lambda) \in \{0, 1\}^{\kappa(\lambda)}$ is said to have η -gap pseudoresourced \mathcal{R} if,*

1. **Efficient generation:** *Given $k(\lambda)$ (or $k'(\lambda)$), there exists a QPT algorithm A that on input $(1^\lambda, k, b)$ (or $(1^\lambda, k', b)$) outputs $\psi_{k(\lambda)}$ (or $\phi_{k'(\lambda)}$).*
2. **Resource gap:** *For all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$,*

$$|R_{rel}(\psi_{k(\lambda)}) - R_{rel}(\phi_{k'(\lambda)})| \geq \eta,$$

where $R_{rel}(\rho)$ is the relative entropy of resource \mathcal{R} .

3. **Computational indistinguishability:** *For any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:*

$$\left| \mathbb{P}_{k(\lambda)}[\mathcal{D}(\sigma_\lambda, \psi_{k(\lambda)}^{\otimes m}) = 1] - \mathbb{P}_{k'(\lambda)}[\mathcal{D}(\sigma_\lambda, \phi_{k'(\lambda)}^{\otimes m}) = 1] \right| \leq \nu(\lambda).$$

The concept of pseudoresource has been introduced before for generic measures of resources, also known as resource monotones [HBK24, BMB⁺24]. Nevertheless, we focus on the concrete measure of relative entropy of resource, which is the most important entropic measure for quantum resource theories.

4.2 Pseudoresources imply EPFI pairs

We prove now the main technical contribution of our result.

Theorem 4.3 (Pseudoresource implies EPFI pairs). *For any $\eta \geq 2 + 1/\text{poly}(n)$, assuming the existence of η -gap pseudoresource with $\kappa := \sup_{\tau, \tau'} R_{rel}(\tau) - R_{rel}(\tau') = \text{polylog}(d)$, then EPFI pairs exist.*

Proof. The construction of an EPFI pair given a pair of pseudoresourced families of states is straightforward: each family of the pseudoresourced states corresponds to an EFI ensemble. The efficient generation of the EPFI pairs together with the property of computational indistinguishability follow from the definition of η -gap pseudoresource.

To prove statistical distance, it follows from Equation (3) that, for every $k, k' \in \{0, 1\}^{\kappa(\lambda)}$

$$\Delta(\psi_{k(\lambda)}, \phi_{k'(\lambda)}) \geq \frac{|R_{rel}(\psi_{k(\lambda)}) - R_{rel}(\phi_{k'(\lambda)})| - 2}{\kappa}.$$

Moreover, by taking into account that $\eta \geq 2 + 1/\text{poly}(n)$ and $\kappa = \text{polylog}(d)$,

$$\Delta(\psi_{k(\lambda)}, \phi_{k'(\lambda)}) \geq \Omega\left(\frac{1}{\text{poly}(n)}\right) \quad \forall k, k' \in \{0, 1\}^{\kappa(\lambda)}.$$

□

Remark 4.4. *The construction of EPFI pairs from pseudorandom families of states is given by the asymptotic continuity of the relative entropy of resource. Nevertheless, a similar construction holds for any resource monotone which is asymptotically continuous.*

Therefore, just assuming the existence of pseudoresource families which relative entropy of resource presents a gap larger than $1/\text{poly}(n)$, EFI pairs of ensembles and thus, quantum commitments and all the primitives that follow from it such as oblivious transfer and multiparty computing can be constructed. Constructions such as the one of pseudoresources from pseudo-random density matrices [BMB⁺24] hold⁸. A similar construction was also proposed by [GLG⁺24] for the specific case of pseudomagic⁹. Nevertheless, we generalize the result for any pseudoresource.

5 Cryptography from pseudoentanglement

Since the proposal of the notion of pseudoentanglement [ABF⁺23], different definitions of the same phenomena have been proposed [ABV23, GE24, LREJ25], extending the definition to mixed states and using different measures of entanglement that allow to obtain a maximal separation in terms of entanglement between both families of states. Nevertheless, all definitions capture the same phenomena: given two families of states that are efficiently generated, both families present a gap in the entanglement, yet they are computationally indistinguishable.

Despite it was proven that the existence of (mixed states) pseudoentanglement as a minimal assumption for computational based cryptography [GE24], no cryptographic primitives have been constructed from it as far as we are concerned. The goal of this section is to establish a direct connection between the different definitions of pseudoentanglement and cryptography. The first subsection studies the construction of EPFI pairs from pure state pseudoentanglement, while the second extend this result to the case of mixed states. Lastly, we proposed a new functionality that it is intrinsically dependent to the resource of entanglement.

5.1 Pure state pseudoentanglement implies EPFI pairs

Let us first define the notion of pure state pseudoentanglement [ABF⁺23].

Definition 5.1 (Pure η -gap pseudoentanglement). *Let $\lambda \in \mathbb{N}_+$ and $\eta : \mathbb{N}_+ \rightarrow \mathbb{N}_+$ be arbitrary. A pair of ensembles of bipartite pure states $\{|\psi^{k(\lambda)}\rangle_{AB}\}_{k(\lambda)}$, $\{|\phi^{k'(\lambda)}\rangle_{AB}\}_{k'(\lambda)}$ indexed by $k, k' \in \{0, 1\}^{\kappa(\lambda)}$ is said to have pure η -pseudoentanglement if,*

1. **Efficient generation:** *Given $k(\lambda)$ (or $k'(\lambda)$), there exists a QPT algorithm A that on input $(1^\lambda, k, b)$ (or $(1^\lambda, k', b)$) outputs $|\psi^{k(\lambda)}\rangle_{AB}$ (or $|\phi^{k'(\lambda)}\rangle_{AB}$).*
2. **Entanglement gap:** *For all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$,*

$$|E(|\psi^{k(\lambda)}\rangle_{AB}) - E(|\phi^{k'(\lambda)}\rangle_{AB})| \geq \eta,$$

where $E(\rho)$ is the entanglement entropy.

⁸Please, note that in [BMB⁺24] EFI pairs are constructed assuming the existence of pseudo-random density matrices.

⁹The construction of pseudomagic states of [GLG⁺24] actually implies our proposed primitive of EPFI pairs, as it is proven in SM V.B of [GLG⁺24].

3. **Computational indistinguishability:** For any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:

$$\left| \mathbb{P}_{|\varphi\rangle \leftarrow \{|\psi^{k(\lambda)}\rangle_{AB}\}_{k(\lambda)}}[\mathcal{D}(\sigma_\lambda, |\varphi\rangle^{\otimes m}) = 1] - \mathbb{P}_{|\varphi\rangle \leftarrow \{|\phi^{k'(\lambda)}\rangle_{AB}\}_{k'(\lambda)}}[\mathcal{D}(\sigma_\lambda, |\varphi\rangle^{\otimes m}) = 1] \right| \leq \nu(\lambda).$$

Having introduced the definition of pseudoentanglement, we can prove the main statement of this section.

Theorem 5.2 (Pure pseudoentanglement implies EPFI pairs). *For any $\eta \geq 1/2e + 1/\text{poly}(n)$ and assuming the existence of pure η -gap pseudoentanglement, then EPFI pairs exist.*

Proof. The construction of an EPFI pair given a pair of pseudoentangled pair of families of pure states is slightly different to the one of Theorem 4.3. We define the two families by with the reduced density matrices of the pseudoentangled states:

$$\{\rho_{A,\psi}^{k(\lambda)}\}_{k(\lambda)} = \left\{ \text{Tr}_B (|\psi^{k(\lambda)}\rangle\langle\psi^{k(\lambda)}|_{AB}) \right\}_{k(\lambda)}, \text{ and } \{\sigma_{A,\phi}^{k'(\lambda)}\}_{k'(\lambda)} = \left\{ \text{Tr}_B (|\phi^{k'(\lambda)}\rangle\langle\phi^{k'(\lambda)}|_{AB}) \right\}_{k'(\lambda)},$$

where the entanglement is measured across the cut $(A : B)$. The properties of efficient generation and computational indistinguishability of the EPFI pairs follow from the definition of η -gap pure pseudoentanglement.

We now prove that for all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$, $\rho_{A,\psi}^{k(\lambda)}$ and $\sigma_{A,\phi}^{k'(\lambda)}$ are statistically far. We have that

$$\Delta(\rho_{A,\psi}^{k(\lambda)}, \sigma_{A,\phi}^{k'(\lambda)}) \geq \frac{|S(\rho_{A,\psi}^{k(\lambda)}) - S(\sigma_{A,\phi}^{k'(\lambda)})| - c}{2n(\lambda)} = \frac{|E(|\psi^{k(\lambda)}\rangle_{AB}) - E(|\phi^{k'(\lambda)}\rangle_{AB})| - c}{2n(\lambda)},$$

where the first inequality follows from Lemma 2.15, and the last equality uses the definition of the entanglement entropy. Therefore, using the fact that for all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$ the entanglement entropies of pairwise sampled states from the ensembles is $\eta \geq 1/2e + 1/\text{poly}(n)$,

$$\Delta(\rho_{A,\psi}^{k(\lambda)}, \sigma_{A,\phi}^{k'(\lambda)}) \geq \Omega\left(\frac{1}{\text{poly}(\lambda)}\right) \quad \forall k, k' \in \{0, 1\}^{\kappa(\lambda)}.$$

□

Every known construction of pseudoentanglement from pure state ensembles [ABF⁺23, ABV23, LREJ25] exhibits an entanglement entropy gap of at least $1/2e + 1/\text{poly}(n)$, making them suitable for constructing EPFI pairs. While the definitions in [ABV23, LREJ25] allow for a larger gap when considering computationally efficient entanglement measures, it is the information-theoretic measure of entanglement entropy that determines the relationship between the gap and trace distance, and thus enables the construction of EPFI pairs. The connection between information-theoretic and computationally meaningful entanglement measures, along with its cryptographic implications, is explored in more detail in the following section.

Remark 5.3. *We notice that in the proof of Theorem 5.2, we do not need indistinguishability between the pure states, but only of subsystem A (or B). In this case, we can also achieve EPFI pairs under a weaker notion of pure-state pseudoentanglement.*

The use of entanglement entropy as a measure of entanglement in the case of pure states require a lower bound of $\omega(\log n)$ for the low entangled family. However, when computational measures of entanglement are taken into account, the entanglement gap can be even larger for pure states, i.e., $\Omega(n)$ vs. $o(1)$ for other entanglement measures as proven in [LREJ25]. While it is true that entanglement entropy losses its operational meaning when it comes to quantify the distillable entanglement (or entanglement cost) taking into account computational efficiency, it is relevant for the construction of EPFI pairs.

5.2 Mixed state pseudoentanglement implies EPFI pairs

Let us now study the pseudoentanglement in the case of mixed states. The main result of this subsection is the construction of EPFI pairs from pseudoentangled mixed states. Let us first introduce our proposed definition of pseudoentanglement for mixed states.

Definition 5.4 (Mixed η -gap pseudoentanglement). *Let $\lambda \in \mathbb{N}_+$ and $\eta : \mathbb{N}_+ \rightarrow \mathbb{N}_+$ be arbitrary. A pair of families of mixed bipartite states $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ and $\{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}$ indexed by $k, k' \in \{0, 1\}^{\kappa(\lambda)}$ is said to have mixed η -gap pseudoentanglement if :*

1. **Efficient generation:** *Given $k(\lambda)$ (or $k'(\lambda)$), there exists a QPT algorithm A that on input $(1^\lambda, k, b)$ (or $(1^\lambda, k', b)$) outputs $\psi_{AB}^{k(\lambda)}$ (or $\phi_{AB}^{k'(\lambda)}$).*
2. **Entanglement gap:** *For all $k, k' \in \{0, 1\}^{\kappa(\lambda)}$,*

$$\left| E_R^\infty \left(\psi_{AB}^{k(\lambda)} \right) - E_R^\infty \left(\phi_{AB}^{k'(\lambda)} \right) \right| \geq \eta.$$

3. **Computational indistinguishability:** *For any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:*

$$\left| \mathbb{P}_{\rho \leftarrow \{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}} [\mathcal{D}(\sigma_\lambda, \rho^{\otimes m}) = 1] - \mathbb{P}_{\rho \leftarrow \{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}} [\mathcal{D}(\sigma_\lambda, \rho^{\otimes m}) = 1] \right| \leq \nu(\lambda).$$

Our definition is based on the ones proposed by [ABV23, GE24] but with two modifications. Foremost, both families of states have to be efficiently generated, contrary to previous definitions in which only the low entangled family was the efficiently generated one. The other major difference is that we consider the (regularised) relative entropy of entanglement, instead of the computational distillable entanglement or the computational entanglement cost, which was used in those results.

Unlike in [ABV23, GE24], our proposed definition of pseudoentanglement is defined in the asymptotic IID setting without taking into account computational entanglement measures. As proposed in [ABV23], their pseudoentanglement construction can be extended to the computational asymptotic IID setting by taking into account taking into account the measures,

$$\hat{E}_C^\infty(\rho_{AB}) = \inf_{\epsilon \in (0, 1]} \limsup_{t \rightarrow \infty} \frac{1}{t} \hat{E}_C^\epsilon(\rho_{AB}^{\otimes t}),$$

$$\hat{E}_D^\infty(\rho_{AB}) = \inf_{\epsilon \in (0, 1]} \liminf_{t \rightarrow \infty} \frac{1}{t} E_D^\epsilon(\rho_{AB}^{\otimes t}),$$

where $\hat{E}_C^\epsilon(\rho)$ and $\hat{E}_D^\epsilon(\rho)$ are defined in Definition 2.12 and Definition 2.11. Let us now show that our definition is a relaxation in the condition of the entanglement gap with respect to the ones of [ABV23, GE24] in the asymptotic IID setting.

Given a “highly entangled” family $\{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}$ such that $\hat{E}_D^\infty(\{k', \phi_{AB}^{k'}\}) \geq d(\lambda)$ and a “low entangled” family $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ such that $\hat{E}_C^\infty(\{k, \psi_{AB}^k\}) \leq c(\lambda)$ with $c(\lambda) < d(\lambda)$. Therefore, given two states $\phi_{AB}^{k'(\lambda)}$ and $\psi_{AB}^{k(\lambda)}$,

$$d(\lambda) - c(\lambda) \leq \hat{E}_D^\infty(\{k', \phi_{AB}^{k'}\}) - \hat{E}_C^\infty(\{k, \psi_{AB}^k\}) \leq E_R^\infty(\phi_{AB}^{k'(\lambda)}) - E_R^\infty(\psi_{AB}^{k(\lambda)})$$

for all k and k' , since for any family $\hat{E}_D^\infty \leq E_D^\infty \leq E_R^\infty \leq E_C^\infty \leq \hat{E}_C^\infty$ under LOCC operations.

Corollary 5.5 (Mixed pseudoentanglement implies EPFI pairs). *For $\eta \geq 2 + 1/\text{poly}(n)$ and assuming the existence of mixed η -pseudoentanglement, then EPFI pairs exist.*

Please, note that the construction is similar to the one of Theorem 4.3, but taking into account that in this case the studied resource is the entanglement. In the case of entanglement, the regularised relative entropy of resource is equivalent to the regularised relative entropy of entanglement, which asymptotically continuity bound is given by Lemma 2.17.

Therefore, every state that has a large pseudoentangled gap $d(\lambda) - c(\lambda) \geq 2 + 1/\text{poly}(n)$ are eligible for building EPFI pairs. On the other hand, there potentially exist pairs of families of mixed states which does not present a gap in the computational measures of entanglement, i.e., they are not pseudoentangled following the definition of [ABV23, GE24], but from which EPFI pairs can be constructed.

5.3 Beyond EPFI: computationally locked entanglement

Previous definitions of pseudoentanglement focus on efficiently generated states with low entanglement that are computationally indistinguishable from highly entangled states. This is an analog of the “classical” concept of pseudorandomness: a simple object (such as a pseudorandom string or pseudoentangled state) that can replace a complex one (resp. random string or highly entangled state).

On the other hand, given how central entanglement is in quantum information, and the plethora of applications that require highly entangled states, we can flip this question and ask for efficiently generated states with high entanglement that are computationally indistinguishable from low entangled ones (that may be efficiently generated or not). We denote this as *computationally locked entanglement*, and it can be used to conceal entanglement that could be distilled only with the help of a secret key. We notice that pseudoentangled states where both low- and high-entangled families are efficiently generated (as in our definition of pseudoentanglement) exhibit computationally locked entanglement.

Definition 5.6 (Computationally locked entanglement). *Let $\lambda \in \mathbb{N}$, $n : \mathbb{N} \rightarrow \mathbb{N}$ be a polynomially bounded function, $\epsilon : \mathbb{N} \rightarrow [0, 1]$ and $c, d : \mathbb{N} \rightarrow \mathbb{N}$ with $c < d$. A family of $2n(\lambda)$ -qubit bipartite states $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ is said to have computationally locked entanglement (ϵ, c, d) if there is a family of $2n(\lambda)$ -qubit bipartite states $\{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}$, such that:*

1. The computational entanglement cost of the family $\{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}$ is upper bounded as $\hat{E}_C^\epsilon(\{k, \phi_{AB}^{k'}\}) \leq c$.
2. Given $k(\lambda)$, there exists a QPT algorithm A that on input $(1^\lambda, k, b)$ outputs $\psi_{AB}^{k(\lambda)}$.
3. The computational distillable entanglement of the family $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ is lower bounded as $\hat{E}_D^\epsilon(\{k, \psi_{AB}^k\}) \geq d$.
4. For any non-uniform QPT distinguisher \mathcal{D} with advice σ_λ and any $m \in \text{poly}(\lambda)$, there exists a negligible function $\nu(\lambda) > 0$ such that:

$$\left| \mathbb{P}_{\rho \leftarrow \{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}} [\mathcal{D}(\sigma_\lambda, \rho^{\otimes m}) = 1] - \mathbb{P}_{\rho \leftarrow \{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}} [\mathcal{D}(\sigma_\lambda, \rho^{\otimes m}) = 1] \right| \leq \nu(\lambda).$$

Computational locked entanglement can be viewed as a “dual” notion to pseudoentanglement, as defined in [ABV23, GE24]. An example of computational locked entanglement is the construction of pseudorandom density matrices [BMB⁺24]. However, in this case, the “low-entangled” family is also efficiently generated. It would be interesting to investigate how pseudoentanglement and computationally locked states relate to each other, i.e., if one implies the other, or if they are incomparable.

We now prove the intuitive consequences of computationally locked states for parties that do not have access to the key.

Lemma 5.7. *Given a family of $2n(\lambda)$ -qubit bipartite states $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ that have computationally locked entanglement (ϵ, c, d) , where $c < d$, its computational distillable entanglement without access to the key k is upper bounded as $\hat{E}_D^\epsilon(\{\psi_{AB}^k\}) \leq c$, as defined in Definition 2.10 .*

Proof. It can be proven by contradiction. Suppose there exist a family of states $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ that have computationally locked entanglement as defined in Definition 5.6 such that, not given the keys k , $\hat{E}_D^\epsilon(\{\psi_{AB}^k\}) > c$. As proven in [ABV23], $\hat{E}_D^\epsilon < \hat{E}_C^\epsilon$. Moreover, $\hat{E}_C^\epsilon(\{k', \phi_{AB}^{k'(\lambda)}\}) < c$ by construction. Then, if there is a poly time algorithm that is able to distill $\hat{E}_D^\epsilon(\{\psi_{AB}^{k(\lambda)}\}) > c$, it would be able to distinguish between the pair of families $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ and $\{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}$ which is not possible by definition. \square

Corollary 5.8. *Given a $2n(\lambda)$ -qubit bipartite states $\{\psi_{AB}^{k(\lambda)}\}_{k(\lambda)}$ which has computationally locked entanglement (ϵ, d) , i.e., w.r.t. a family of $2n(\lambda)$ -qubit separable bipartite states $\{\phi_{AB}^{k'(\lambda)}\}_{k'(\lambda)}$, no entanglement can be distilled without the respective keys k .*

An application of the computationally locked functionality is an authenticated quantum teleportation protocol. The scheme is similar to the original quantum teleportation [BBC⁺93] but in this case the receiver cannot access the teleported state without using a secret key in each interaction, being not necessary to authenticate the classical channel before or during the teleportation protocol. Moreover, the family of states with its corresponding keys can be used a polynomial number of times, unlike in the Clifford encryption scheme [DLT02, ABOE08].

Further applications of computationally locked entanglement for quantum networks in which there is a necessity of distributing entanglement while preventing the users for accessing it.

Since quantum networks routing is based on the principle of entanglement swapping [BDCZ98, Cal17], encoding the nodes of the quantum network with computationally locked entanglement allows certifying the routing of the network.

Acknowledgments

Álvaro Yángüez thanks Pere Munar, Lorenzo Leone, Asad Raza, Ludovico Lami, Salvatore F.E. Oliviero and Francesco Anna Mele for helpful discussions. Alex B. Grilo and Álvaro Yángüez are supported by the European Union’s Horizon Europe Framework Programme under the Marie Skłodowska Curie Grant No. 101072637, Project Quantum-Safe Internet (QSI).

References

- [ABF⁺23] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement, 2023.
- [ABOE08] Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations, 2008.
- [ABV23] Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. Computational entanglement theory, 2023.
- [AQY21] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states, 2021.
- [BBC⁺93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.
- [BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In *Advances in Cryptology—CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 467–496. Springer, 2021.
- [BCP14] T. Baumgratz, M. Cramer, and M. B. Plenio. Quantifying coherence. *Phys. Rev. Lett.*, 113:140401, Sep 2014.
- [BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:21, Dagstuhl, Germany, 2023. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
- [BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.

- [BMB⁺24] Nikhil Bansal, Wai-Keong Mok, Kishor Bharti, Dax Enshan Koh, and Tobias Haug. Pseudorandom density matrices, 2024.
- [BP10] Fernando G. S. L. Brandão and Martin B. Plenio. A reversible theory of entanglement and its relation to the second law. *Communications in Mathematical Physics*, 295(3):829–851, February 2010.
- [Cal17] Marcello Caleffi. Optimal routing for quantum networks. *IEEE Access*, 5:22299–22312, 2017.
- [CG19] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2), April 2019.
- [Chr06] Matthias Christandl. The structure of bipartite quantum states - insights from group theory and cryptography, 2006.
- [DH99] Matthew J. Donald and Michał Horodecki. Continuity of relative entropy of entanglement, 1999.
- [DHR02] Matthew J. Donald, Michał Horodecki, and Oliver Rudolph. The uniqueness theorem for entanglement measures. *Journal of Mathematical Physics*, 43(9):4252–4272, September 2002.
- [DLT02] D.P. DiVincenzo, D.W. Leung, and B.M. Terhal. Quantum data hiding. *IEEE Transactions on Information Theory*, 48(3):580–598, March 2002.
- [Fan73] Mark Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31:291–294, 1973.
- [GE24] Manuel Goulão and David Elkouss. Pseudo-entanglement is necessary for efi pairs, 2024.
- [GLG⁺24] Andi Gu, Lorenzo Leone, Soumik Ghosh, Jens Eisert, Susanne F. Yelin, and Yihui Quek. Pseudomagic quantum states. *Physical Review Letters*, 132(21), May 2024.
- [GLSV21] Alex B Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 531–561. Springer, 2021.
- [GOL24] Andi Gu, Salvatore F. E. Oliviero, and Lorenzo Leone. Magic-induced computational separation in entanglement theory, 2024.
- [HBK24] Tobias Haug, Kishor Bharti, and Dax Enshan Koh. Pseudorandom unitaries are neither real nor sparse nor noise-robust, 2024.
- [HC17] Mark Howard and Earl Campbell. Application of a resource theory for magic states to fault-tolerant quantum computing. *Phys. Rev. Lett.*, 118:090501, Mar 2017.
- [Hel69] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

- [HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009.
- [Hol73] A.S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973.
- [Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
- [LREJ25] Lorenzo Leone, Jacopo Rizzo, Jens Eisert, and Sofiene Jerbi. Entanglement theory with limited computational resources, 2025.
- [MY22] Tomoyuki Morimae and Takashi Yamakawa. *Quantum Commitments and Signatures Without One-Way Functions*, page 269–295. Springer Nature Switzerland, 2022.
- [PV06] Martin B. Plenio and S. Virmani. An introduction to entanglement measures, 2006.
- [SAP17] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. Colloquium: Quantum coherence as a resource. *Rev. Mod. Phys.*, 89:041003, Oct 2017.
- [Uh176] A. Uhlmann. The “transition probability” in the state space of a $*$ -algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.
- [Unr16] Dominique Unruh. Collapse-binding quantum commitments without random oracles. Cryptology ePrint Archive, Paper 2016/508, 2016.
- [VHMGE14] Victor Veitch, S A Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. The resource theory of stabilizer quantum computation. *New Journal of Physics*, 16(1):013009, January 2014.
- [Win16] Andreas Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, March 2016.
- [Yan22] Jun Yan. General properties of quantum bit commitments (extended abstract). In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 628–657, Cham, 2022. Springer Nature Switzerland.