OPEN ACCESS
IOP Publishing
Reports on Progress in Physics
Rep. Prog. Phys. **88** (2025) 067601 (51pp)
https://doi.org/10.1088/1361-6633/adcd28

Extendibility limits quantum-secured communication and key distillation

Vishal Singh[1,*] **and Mark M Wilde**[2]

[1] School of Applied and Engineering Physics, Cornell University, Ithaca, NY 14850, United States of America
[2] School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14850, United States of America

E-mail: vishalsph04@gmail.com

Received 29 December 2024, revised 24 March 2025
Accepted for publication 15 April 2025
Published 3 June 2025

Corresponding editor: Dr Lorna Brigham

Abstract

Secret-key distillation from quantum states and channels is a central task of interest in quantum information theory, as it facilitates private communication over a quantum network. Here, we study the task of secret-key distillation from bipartite states and point-to-point quantum channels using local operations and one-way classical communication (one-way LOCC). We employ the resource theory of unextendible entanglement to study the transformation of a bipartite state under one-way LOCC, and we obtain several efficiently computable upper bounds on the number of secret bits that can be distilled from a bipartite state using one-way LOCC channels; these findings apply not only in the one-shot setting but also in some restricted asymptotic settings. We extend our formalism to private communication over a quantum channel assisted by forward classical communication. We obtain efficiently computable upper bounds on the one-shot forward-assisted private capacity of a channel, thus addressing a question in the theory of quantum-secured communication that has been open for some time now. Our formalism also provides upper bounds on the rate of private communication when using a large number of channels in such a way that the error in the transmitted private data decreases exponentially with the number of channel uses. Moreover, our bounds can be computed using semidefinite programs, thus providing a computationally feasible method to understand the limits of private communication over a quantum network.

Supplementary material for this article is available online

Keywords: private communication, secret-key distillation, one-shot private capacity, semidefinite programs

* Author to whom any correspondence should be addressed.

Contents

1. Introduction

1.1. Motivation

The existence of a quantum network facilitates the distribution of secret keys between distant parties [BB84, Eke91], which ensures secure communication by means of the one-time pad protocol. However, realizing an ideal quantum network can be very expensive. This motivates an in-depth study of the number of secret bits that can be established with the available resources, which, in the context of the quantum internet, are partially entangled states and quantum channels.

Our ability to distill secret keys from a bipartite state or a quantum channel depends on the operations that we can perform. The three most common settings studied in any non-local resource distillation task are as follows: local operations, local operations with one-way classical communication, and local operations with two-way classical communication. Here we consider the task of secret-key distillation from bipartite states and point-to-point channels in the presence of local operations and one-way classical communication. In what follows, we first discuss our contributions on understanding secret-key distillation from states, and thereafter we discuss our related contributions for channels.

1.2. Secret-key distillation from states

The task of distilling secret keys from a bipartite state using local operations and one-way classical communication, abbreviated as one-way LOCC, has been studied extensively in the past [DW05, RR12, KKGW21]. From an information-theoretic perspective, the main quantities of interest are the one-shot, one-way distillable key of a state and the asymptotic one-way distillable key of the state. The one-shot, one-way distillable key of a state is roughly defined as the maximum number of 'approximate' secret bits that can be distilled from a state using a one-way LOCC channel with respect to a fixed error parameter, and the asymptotic one-way distillable key of the state is the maximum rate at which secret bits can be distilled from an arbitrarily large number of independent and identically distributed copies of the state when using one-way LOCC channels.

Computing the one-shot, one-way distillable key and the asymptotic one-way distillable key is a challenging task. Lower bounds on the one-way distillable key in the one-shot regime, as well as the asymptotic regime, have been found in previous works [DW05, RR12, KKGW21]. Upper bounds on the one-shot distillable key of a state when using two-way LOCC have been found in terms of the smooth-min relative entropy of entanglement [WTB17] and the squashed entanglement [Chr06, CEH+07, CSW12, Wil16]. Naturally, these quantities also bound the one-shot, one-way distillable key from above. However, computing the smooth-min relative entropy of entanglement of a state is related to the NP-hard problem of optimizing over the set of separable states [Gur03, Gha10], and the squashed entanglement is not even known

to be computable in the Turing sense, due to it involving an optimization over a state having a system of unbounded size. Moreover, the aforementioned quantities bound the one-shot distillable key of a state, which is expected to be larger than the one-shot, one-way distillable key of the state in general, leaving room for significant improvement in the estimation of the latter quantity.

In this work, we invoke the framework of unextendibility to obtain upper bounds on the one-shot, one-way distillable key of a state, which can be computed by means of a semidefinite program. As such, to the best of our knowledge, ours is the first general upper bound on this quantity that is efficiently computable, in contrast to the smooth-min relative entropy of entanglement and the squashed entanglement. We also give an upper bound on the maximum rate at which secret bits can be distilled from an arbitrarily large number of i.i.d. copies of a state when using one-way LOCC channels, provided that the error in distillation decreases exponentially with the number of copies of the resource state.

1.3. Private communication over channels

The one-shot setting of private communication has been the subject of several studies [RR11, WTB17, Wil17, RSW17, KKGW21]. In the context of private communication, we are interested in the maximum number of private bits that can be sent through a quantum channel when using some freely available operations, which can be local operations and classical communication, local operations with only forward-classical communication, or local operations only. The corresponding quantities are called the one-shot two-way-assisted private capacity, the one-shot forward-assisted private capacity, and the one-shot unassisted private capacity, respectively. In the presence of forward-classical assistance, the task of secret-key distillation is equivalent to the task of private communication, which allows us to immediately extend our understanding of secret-key distillation from channels to private communication.

Finding efficiently computable upper bounds on the one-shot private capacity of a channel has remained an unsolved problem since early works on private capacity [CWY04, DW05]. Several upper bounds on the one-shot, two-way-assisted private capacity have been obtained [TGW14, WTB17, QSW18]. However, none of them are known to be efficiently computable. Even in the asymptotic regime, computable upper bounds on the unassisted private capacity and two-way-assisted private capacity are known only for qubit channels [FF21].

Here we contribute to this growing body of knowledge by giving upper bounds on the one-shot forward-assisted private capacity of a channel, which can be computed efficiently using a semidefinite program. We also give a semidefinite computable upper bound on the maximum rate at which private bits can be transmitted through a quantum channel when the error in transmission is required to decay exponentially with the number of channel uses.

1.4. Methods used in this work

The resource theory of unextendible entanglement developed in [WWW24] serves as the primary mathematical framework in our investigation. The set of free states in the resource theory of unextendible entanglement is a state-dependent set comprising of all symmetric extensions of the state in question. The set of two-extendible channels serves as the set of free operations, which was defined in [KDWW19, KDWW21]. All one-way LOCC channels are two-extendible channels, which makes the resource theory of unextendible entanglement useful for the analysis of private communication with one-way LOCC.

The unextendible entanglement of quantum channels was defined in [SW24b], which is the primary mathematical framework that we use to investigate private communication through a quantum channel assisted by one-way LOCC. In this resource theory, the set of free channels is a channel-dependent set, which consists of channels that are symmetrically-*compatible* with the channel in question, where compatible channels were defined in [HMZ16]. The set of free operations are two-extendible superchannels, which form a semidefinite relaxation of the set of one-way LOCC superchannels originally considered in [LM15, RBL18].

In the past, the unextendible entanglement of states has been used to study the *exact* and *probabilistic* distillation of secret keys from states using one-way LOCC channels in [WWW24, SW24a], and the unextendible entanglement of channels has been used to study zero-error private communication through channels in [SW24b]. By using the resource theory of unextendible entanglement to study 'approximate' secret-key distillation from states and channels, we demonstrate that this resource theory can be used to study more practical settings in which an arbitrarily small error is allowed in resource distillation.

1.5. Summary of results and organization of the paper

The main contributions of our paper are as follows: We give upper bounds on the one-shot, one-way distillable key of a bipartite state and on the one-shot, forward-assisted private capacity of point-to-point quantum channels. As mentioned previously, to the best of our knowledge, these are the first efficiently computable upper bounds on these quantities. Extending our results to the asymptotic setting, we give upper bounds on the maximum rate of distilling secret keys from i.i.d. copies of a bipartite state or channel when using one-way LOCC, albeit in a particular setting in which the error in distillation is required to decay exponentially with the number of copies of the resource. Several of our bounds can be computed using semidefinite programs, adding to their practical relevance. Finally, with this work, we demonstrate the power

Table 1. A list of our results for secret-key distillation from a bipartite state when using one-way LOCC channels, in the one-shot and asymptotic settings.

Setting	Divergence used for upper bound	Reference
One-shot setting	Smooth-min relative entropy	Theorem 2
Simplified bounds for 1-shot setting	Smooth-min relative entropy	Corollaries 1 and 2
n-Shot setting	Sandwiched Rényi relative entropy	Corollary 3
Asymptotic setting	Umegaki relative entropy	Theorem 3

Table 2. A list of our results for forward-assisted private communication from point-to-point quantum channels in the one-shot and asymptotic settings.

Setting	Divergence used for upper bound	Reference
One-shot setting	Smooth-min relative entropy	Theorem 4
Simplified bounds for 1-shot setting	Smooth-min relative entropy	Corollary 4
n-shot setting	Geometric Rényi relative entropy	Corollary 5
Asymptotic setting	Belavkin–Staszewski relative entropy	Theorem 5

of the resource theory of unextendible entanglement in studying resource distillation. Prior to our work here, it was unclear how to apply this concept to the setting of approximate key distillation and left as an open question since [WWW24].

In table 1, we present a brief summary of our results on one-way secret-key distillation from bipartite states, and in table 2, we give a brief summary of our results on forward-assisted private communication over channels. We note here that the Python codes used for calculating the semidefinite programs and producing the plots in this paper are available with the arXiv posting.

An outline of our paper is as follows:

- Section 2: definitions and notations used in the paper, along with basic facts about quantum states, channels, and superchannels.
- Section 3: Discussion on secret-key distillation from bipartite states using one-way LOCC channels, and definition of the one-shot, one-way distillable key of a state, which is the primary quantity of interest.
- Section 4: Review of the concepts of two-extendibility and the unextendible entanglement of states. Discussion on the unextendible entanglement of states induced by smooth-min relative entropy and α-sandwiched Rényi relative entropy, which are the primary ingredients in the main result obtained for one-way secret-key distillation from bipartite states.
- Section 5: Main results on one-way secret-key distillation from an arbitrary bipartite state. Numerical demonstration of the upper bounds on the one-shot, one-way distillable key of isotropic states using semidefinite programs.
- Section 6: Discussion of private communication over quantum channels using one-way LOCC superchannels. Review of the unextendible entanglement of channels induced by smooth-min relative entropy and α-geometric Rényi relative entropy. Main results on one-way private communication over an arbitrary channel. Demonstrating the upper bound on the one-shot, forward-assisted private capacity of the erasure channel using analytical expressions.

2. Notation and preliminaries

In this section, we review background material on the three major elements that we use in the rest of the work: quantum states, channels, and superchannels.

2.1. Quantum states and channels

A quantum state ρ_A is a positive semidefinite, unit-trace operator acting on a Hilbert space $\mathcal{H}_A$. We denote the set of all linear operators acting on the Hilbert space $\mathcal{H}_A$ by $\mathcal{L}(A)$ and the set of all quantum states acting on this Hilbert space by $\mathcal{S}(A)$. A bipartite quantum state ρ_{AB} acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is called separable if it can be written as

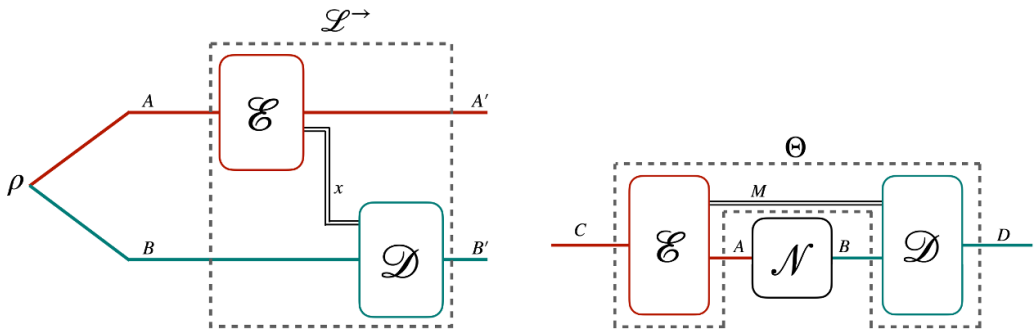
$$\rho_{AB} = \sum_{x\in\mathcal{X}} p(x)\, \sigma_A^x \otimes \tau_B^x, \tag{1}$$

where $\{p(x)\}_{x\in\mathcal{X}}$ is a probability distribution and $\{\sigma_A^x\}_{x\in\mathcal{X}}$ and $\{\tau_B^x\}_{x\in\mathcal{X}}$ are sets of states. Any quantum state that is not separable is said to be entangled. The maximally entangled state vector in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is denoted as follows:

$$|\Phi^d\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B, \tag{2}$$

where $\{|i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis and d is the Schmidt rank of the state. We denote the correponding density operator as $\Phi_{AB}^d \equiv |\Phi^d\rangle\langle\Phi^d|_{AB}$.

A quantum channel $\mathcal{N}_{A\to B}$ is a completely positive (CP) and trace-preserving (TP) linear map that takes an operator acting on the Hilbert space $\mathcal{H}_A$ as input and outputs an operator acting



(a) One-way LOCC channel (b) One-way LOCC superchannel

Figure 1. (a) Schematic diagram of a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'}$, as defined in (5), acting on a bipartite state ρ_{AB}. (b) Schematic diagram of a one-way LOCC superchannel $\Theta_{(A\to B)\to(C\to D)}$, defined in (6) with M being a classical system, acting on a channel $\mathcal{N}_{A\to B}$.

on the Hilbert space $\mathcal{H}_B$. We denote the Choi operator of a channel $\mathcal{N}_{A\to B}$ by $\Gamma^{\mathcal{N}}_{RB}$, which is defined as follows:

$$\Gamma^{\mathcal{N}}_{RB} := \mathcal{N}_{A\to B}\left(d\Phi^{d}_{RA}\right), \tag{3}$$

where Φ^{d}_{RA} is the maximally entangled state of Schmidt rank d and system R is isomorphic to system A. The normalized Choi operator is called the Choi state of the channel, and it is defined as follows:

$$\Phi^{\mathcal{N}}_{RB} := \mathcal{N}_{A\to B}\left(\Phi^{d}_{RB}\right). \tag{4}$$

An important class of channels that is central to our work consists of one-way LOCC channels. We use the symbol $\mathcal{L}^{\rightarrow}$ for a one-way LOCC channel.

A one-way LOCC channel is a quantum channel that acts on a bipartite state, and it can be physically described by the following sequence of operations: Say Alice and Bob share a bipartite state ρ_{AB}. Alice applies a quantum instrument $\{\mathcal{E}^{x}_{A\to A'}\}_{x\in\mathcal{X}}$ on her system, where x is a classical label corresponding to the outcome of the instrument. She sends the classical label x to Bob through an ideal classical channel. Bob then applies a quantum channel $\mathcal{D}^{x}_{B\to B'}$ based on the label x that he received from Alice (see figure 1(a)). A one-way LOCC channel can be mathematically described as follows:

$$\mathcal{L}^{\rightarrow}_{AB\to A'B'} = \sum_{x\in\mathcal{X}} \mathcal{D}^{x}_{A\to B}\otimes\mathcal{E}^{x}_{A\to A'}, \tag{5}$$

where $\{\mathcal{E}^{x}_{A\to A'}\}_{x\in\mathcal{X}}$ is a quantum instrument and $\{\mathcal{D}^{x}_{B\to B'}\}_{x\in\mathcal{X}}$ is a set of quantum channels.

2.2. Quantum superchannels

A quantum superchannel $\Theta_{(A\to B)\to(C\to D)}$ is a linear map that transforms a quantum channel to another quantum channel. Since quantum channels are CP and TP maps, a superchannel is a completely CPTP-preserving map (see definition 1 for a formal definition). It can be perceived as a mathematical model for any physical transformation a quantum channel can undergo, as long as the resulting map is also a quantum channel. Quantum superchannels were introduced in [CDP08] and further investigated in [Gou19], both of which provide a detailed discussion. Here, we include a brief discussion on superchannels relevant to this work.

Definition 1 (superchannel). Let $\mathcal{T}_{A\to B}:\mathcal{L}(A)\to\mathcal{L}(B)$ be a linear map. Let the space of all such maps be denoted by $\mathbb{L}^{AB}$. A linear map $\Theta_{(A\to B)\to(C\to D)}:\mathbb{L}^{AB}\to\mathbb{L}^{CD}$ is a superchannel if

1. It is completely CP preserving; i.e. $(\mathrm{id}_{(E)\to(E)}\otimes\Theta_{(A\to B)\to(C\to D)})(\mathcal{T}_{EA\to EB})$ is a CP map if $\mathcal{T}_{EA\to E'B}$ is a CP map, for all possible dimensions of system E.
2. It is TP preserving; i.e. $\Theta_{(A\to B)\to(C\to D)}(\mathcal{T}_{A\to B})$ is a TP map if $\mathcal{T}_{A\to B}$ is a TP map.

According to the fundamental theorem of superchannels [CDP08], every superchannel can be decomposed into a pre-processing channel $\mathcal{E}_{C\to MA}$ and a post-processing channel $\mathcal{D}_{MB\to D}$ connected by a memory system M. That is, for every superchannel $\Theta_{(A\to B)\to(C\to D)}$, there exist $\mathcal{E}_{C\to MA}$ and $\mathcal{D}_{MB\to D}$ such that

$$\Theta_{(A\to B)\to(C\to D)}\left(\mathcal{N}_{A\to B}\right) = \mathcal{D}_{MB\to D}\circ\mathcal{N}_{A\to B}\circ\mathcal{E}_{C\to MA}. \tag{6}$$

Quantum superchannels are a powerful tool in analyzing communication tasks over a quantum channel, as any communication protocol can be modeled as a superchannel.

A special class of superchannels that is relevant to this work is the class of one-way LOCC superchannels. This is the set of superchannels that can be simulated by local operations and forward classical communication (see figure 1(b)). In particular, if system M in (6) is set to be a classical system, then every superchannel $\Theta_{(A\to B)\to(C\to D)}$ that has the form given in (6) is a one-way LOCC superchannel.

3. One-way secret-key distillation

In principle, the existence of a quantum network ensures unconditional secret key distribution [BB84, Eke91]. Alice and Bob can often manipulate a shared entangled state by

means of local operations to obtain a maximally classically-correlated state that is completely independent of the system of any eavesdropper. The maximally-classically correlated state can then be used as a key to encrypt some classical data that Alice intends to send to Bob using the one-time-pad scheme. Since the eavesdropper is independent of the key shared between Alice and Bob, it is impossible for them to decode the encrypted data irrespective of their computational power. The state thus established between Alice, Bob, and an eavesdropper is called a tripartite key state, and it can be expressed in the following form:

$$\tau_{ABE} = \frac{1}{K}\sum_{i=0}^{k-1} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E, \tag{7}$$

where σ_E is an arbitrary quantum state.

In general, the task of secret-key distillation is a three party problem due to the involvement of the eavesdropper. However, a crucial discovery was made in [HHHO05, HHHO09], establishing an equivalence between the tripartite scenario and a bipartite scenario involving the concept of a *private state*. In the next section, we briefly review the structure of bipartite private states, which plays an important role in this work.

3.1. Bipartite private states

A bipartite private state $\gamma^k_{ABA'B'}$ is the most general form of a quantum state that furnishes a secret key of $\log_2 k$ bits upon local measurements of systems A and B. Therefore, to establish a secret key whose secrecy is ensured by the laws of quantum mechanics, one needs to establish a bipartite private state.

It was shown in [HHHO05, HHHO09] that a private state $\gamma^k_{ABA'B'}$ holding $\log_2 k$ secret key bits can always be written in the following form:

$$\gamma^k_{ABA'B} = V_{ABA'B'}\left(\Phi^k_{AB}\otimes\tau_{A'B'}\right)V^\dagger_{ABA'B'}, \tag{8}$$

where Φ^k_{AB} is a maximally entangled state of Schmidt rank k, the operator $\tau_{A'B'}$ is an arbitrary bipartite state, and $V_{ABA'B'}$ is called a twisting unitary, defined as follows:

$$V_{ABA'B'} = \sum_{i=0}^{k-1} |i\rangle\langle i|_A \otimes I_B \otimes U^i_{A'B'}, \tag{9}$$

with $U^i_{A'B'}$ being some unitary operator. The private state in (8) can then be written more explicitly as follows:

$$\gamma^k_{ABA'B} = \sum_{i,j=0}^{k-1} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B \otimes U^i_{A'B'}\tau_{A'B'}\left(U^j_{A'B'}\right)^\dagger. \tag{10}$$

Systems A and B are said to be the key systems, and systems A' and B' are said to be the shield systems.

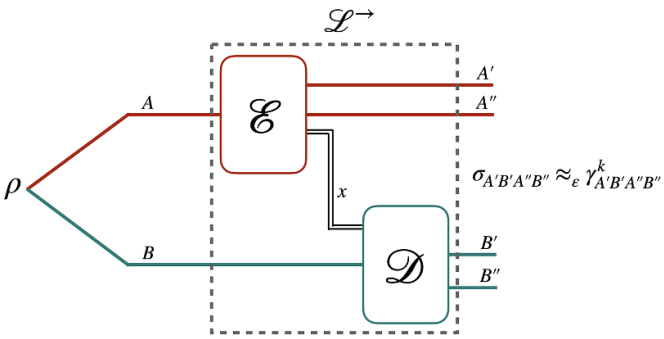


Figure 2. Schematic diagram of approximate distillation of a bipartite private state $\gamma^k_{A'B'A''B''}$ from a state ρ_{AB} using a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$, where the error in distillation, denoted by ε, is defined in (11).

3.2. One-shot, one-way distillable key of a state

Let us now consider the task of distilling secret keys from a bipartite state shared between two parties using local operations and one-way classical communication. Since the distillation of a secret key is equivalent to the distillation of a bipartite private state, we consider the task of distilling a private state from bipartite resource state using one-way LOCC channels. However, distilling private states exactly, or even probabilistically, is a very restrictive task [SW24a], and one must relax this setting to allow for any practical distillation of secret keys.

The task of distilling approximate secret keys using one-way LOCC channels has been a subject of significant interest in several prior works [DW05, RR12, KKGW21] (see figure 2 for a schematic diagram). The error in distillation of secret keys from a state ρ_{AB} using a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ is measured by the infidelity, defined as

$$p_{\text{err}}(\mathcal{L}^{\rightarrow};\rho_{AB}) := \inf_{\gamma^k_{A'B'A''B''}} \left(1 - F\left(\gamma^k, \mathcal{L}^{\rightarrow}(\rho_{AB})\right)\right), \tag{11}$$

where the infimum is over all bipartite private states holding $\log_2 k$ secret bits and $F(\cdot,\cdot)$ denotes the fidelity between two states, which is defined as follows:

$$F(\rho,\sigma) := \left(\text{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right]\right)^2. \tag{12}$$

The reason for choosing infidelity to be the metric of error is motivated from the 'γ^k-privacy test' [HHH+08b, HHH+08a] (see [KW24, section 15.1.3] for a detailed discussion. The γ^k-privacy test is a POVM $\{\Pi^\gamma_{ABA'B'}, I_{ABA'B'} - \Pi^\gamma_{ABA'B'}\}$, where

$$\Pi^\gamma_{ABA'B'} := V_{ABA'B'}\left(\Phi^k_{AB}\otimes I_{A'B'}\right)V^\dagger_{ABA'B'}. \tag{13}$$

The one-shot, one-way distillable key of a state is the quantity that describes the number of bits of secret key that can be established between two parties holding a resource state ρ_{AB}, with some error tolerance ε, when using one-way LOCC channels.

Definition 2 (one-shot, one-way distillable key). For $\varepsilon \in [0,1]$, the one-shot, one-way distillable key of a state ρ_{AB} is defined as follows:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) := \sup_{\substack{k\in\mathbb{N},\gamma^k_{A'B'A''B''},\\ \mathcal{L}^{\rightarrow}\in 1\text{WL}}} \left\{ \begin{array}{c} \log_2 k : \\ F\left(\mathcal{L}^{\rightarrow}(\rho_{AB}),\gamma^k\right) \geqslant 1-\varepsilon \end{array} \right\}, \quad (14)$$

where 1WL stands for the set of all one-way LOCC channels.

In the above definition, the supremum is over every positive integer k, every private state $\gamma^k_{A'B'A''B''}$ holding $\log_2 k$ secret key bits, and every one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$.

4. Two-extendibility

In this section we review the concepts of two-extendibility for states and channels. The resource theory of k-extendibility was developed in [KDWW19, KDWW21] as a semidefinite relaxation of the resource theory of entanglement, and the resource theory of two-extendibility is a special case when $k=2$. A state-dependent resource theory of extendibility was developed in [WWW24], which is the framework that we employ to study the task of secret-key distillation with one-way LOCC channels.

4.1. Two-extendible states and channels

Let us first discuss two-extendible states [DPS04], also known as *symmetrically extendible states* [Wer89], *two-shareable states* [Yan06], and *anti-degradable states* [LDS18].

Definition 3 (two-extendible state). A bipartite state ρ_{AB} is said to be two-extendible if there exists a state ω_{ABE} such that the following conditions hold:

$$\mathrm{Tr}_E[\omega_{ABE}] = \rho_{AB}, \quad (15)$$

and

$$W_{BE}\left(\omega_{ABE}\right) W_{BE}^{\dagger} = \omega_{ABE}, \quad (16)$$

where the unitary swap operator W is defined as follows:

$$W_{BE} := \sum_{k,k'=0}^{d-1} |k\rangle\langle k'|_B \otimes |k'\rangle\langle k|_E. \quad (17)$$

Note that the system E should be isomorphic to the system B for (15) and (16) to hold. The state ω_{ABE} is said to be a two-extension of the state ρ_{AB} if the conditions in (15) and (16) are met.

Remark 1. All bipartite separable states are two-extendible. Consider an arbitrary bipartite separable state $\rho_{AB} := \sum_{x\in\mathcal{X}} p(x)\sigma^x_A \otimes \tau^x_B$, where $\{p(x)\}_{x\in\mathcal{X}}$ is a probability distribution and $\{\sigma^x_A\}_{x\in\mathcal{X}}$ and $\{\tau^x_B\}_{x\in\mathcal{X}}$ are sets of quantum states. One can always construct the following two-extension of ρ_{AB}:

$$\omega_{ABE} := \sum_{x\in\mathcal{X}} p\left(x\right)\sigma^x_A \otimes \tau^x_B \otimes \tau^x_E, \quad (18)$$

which shows that all bipartite separable states are two-extendible. However, all two-extendible states are not separable. A simple example is the following isotropic state [HH99]:

$$\zeta_{AB} = \frac{5}{8}\Phi_{AB} + \frac{1}{8}\left(I_{AB} - \Phi_{AB}\right) = \frac{1}{2}\Phi_{AB} + \frac{1}{8}I_{AB}, \quad (19)$$

where A and B are two-dimensional systems, Φ_{AB} is a two-qubit maximally entangled state, and I_{AB} is the identity operator. This state is two-extendible with the following two-extension:

$$\omega_{ABE} = \frac{1}{4}\Phi_{AB}\otimes I_E + \frac{1}{4}\Phi_{AE}\otimes I_B, \quad (20)$$

but ζ_{AB} has non-zero distillable entanglement [HH99], and hence, it is not a separable state.

A family of semidefinite relaxations of one-way LOCC channels was developed in [KDWW19, KDWW21], called k-extendible channels. The set of k-extendible channels serves as the set of free channels in [KDWW19, KDWW21]. Setting $k=2$, we obtain the set of two-extendible channels, which serves as the set of free operations in the state-dependent resource theory of unextendibility developed in [WWW24]. Here we briefly discuss the idea of two-extendible channels.

Definition 4 (two-extendible channel). A bipartite channel $\mathcal{N}_{AB\to A'B'}$ is said to be two-extendible if there exists a channel $\mathcal{P}_{ABE\to A'B'E'}$ such that the following conditions hold:

$$\mathrm{Tr}_{E'}\circ\mathcal{P}_{ABE\to A'B'E'} = \mathcal{N}_{AB\to A'B'}\otimes\mathrm{Tr}_E, \quad (21)$$

and

$$\mathcal{W}_{B'E'}\circ\mathcal{P}_{ABE\to A'B'E'} = \mathcal{P}_{ABE\to A'B'E'}\circ\mathcal{W}_{BE}, \quad (22)$$

where $\mathcal{W}_{BE} := W_{BE}(\cdot)W^{\dagger}_{BE}$ with W_{BE} defined in (17). The conditions in (21) and (22) are known as the channel extension condition and the permutation covariance condition, respectively.

The channel $\mathcal{P}_{ABE\to A'B'E'}$ is said to be a two-extension of $\mathcal{N}_{AB\to A'B'}$ if the channel extension and permutation covariance conditions, mentioned in (21) and (22) respectively, hold.

If a channel $\mathcal{N}_{AB\to A'B'}$ is two-extendible, then it is non-signaling from B to A [HSW23, appendix A]; that is,

$$\mathrm{Tr}_{B'}\circ\mathcal{N}_{AB\to A'B'} = \mathrm{Tr}_{B'}\circ\mathcal{N}_{AB\to A'B'}\circ\mathcal{R}^{\pi}_B, \quad (23)$$

where $\mathcal{R}^{\pi}_B$ is a channel that traces out the input and replaces it with a maximally mixed state. Moreover, all one-way LOCC

channels are two-extendible, as can be seen from a simple construction. An arbitrary one-way LOCC channel can be written in the following form:

$$\mathcal{N}_{AB\to A'B'} = \sum_{x\in\mathcal{X}} \mathcal{E}^x_{A\to A'} \otimes \mathcal{F}^x_{B\to B'}, \tag{24}$$

where $\{\mathcal{E}^x_{A\to A'}\}_{x\in\mathcal{X}}$ is a quantum instrument and $\{\mathcal{F}^x_{B\to B'}\}_{x\in\mathcal{X}}$ is a set of quantum channels. A two-extension of this channel can be constructed as follows:

$$\mathcal{P}_{ABE\to A'B'E'} = \sum_{x\in\mathcal{X}} \mathcal{E}^x_{A\to A'} \otimes \mathcal{F}^x_{B\to B'} \otimes \mathcal{F}^x_{E\to E'}. \tag{25}$$

Hence, every one-way LOCC channel is two-extendible.

On the contrary, all two-extendible channels cannot be simulated by local operations and one-way classical communication. Consider the example of a bipartite channel that traces out the input and replaces it with the state mentioned in (20), which can be mathematically represented as follows:

$$\mathcal{N}_{AB\to A'B'}(\cdot) = \mathrm{Tr}[\cdot]\left(\frac{1}{2}\Phi_{AB} + \frac{1}{2}\frac{I_{AB}}{4}\right). \tag{26}$$

Since this channel is capable of taking a separable state as input and establishing an entangled state, it is not a one-way LOCC channel. However, one can construct the following two-extension of the channel:

$$\mathcal{P}_{ABE\to A'B'E'}(\cdot) := \mathrm{Tr}[\cdot]\left(\frac{1}{4}\Phi_{A'B'}\otimes I_{E'} + \frac{1}{4}\Phi_{A'E'}\otimes I_{B'}\right). \tag{27}$$

Therefore, the channel defined in (26) is an example of a two-extendible channel that is not a one-way LOCC channel.

4.2. Unextendible entanglement of states

Let $\mathbb{R}$ denote the field of real numbers. A generalized divergence [PV10] is a functional $\mathbf{D}\colon \mathcal{S}(A)\times\mathcal{S}(A)\to\mathbb{R}\cup\{+\infty\}$, such that, for arbitrary states $\rho_A,\sigma_A\in\mathcal{S}(A)$ and an arbitrary channel $\mathcal{N}_{A\to B}$, the data-processing inequality holds

$$\mathbf{D}(\rho_A\|\sigma_A) \geqslant \mathbf{D}(\mathcal{N}_{A\to B}(\rho_A)\,\|\mathcal{N}_{A\to B}(\sigma_A)). \tag{28}$$

Some examples of divergences that commonly appear in quantum information theory are the quantum relative entropy [Ume62], Petz–Rényi relative entropies [Pet86], sandwiched Rényi relative entropies [MLDS+13, WWY14], and geometric Rényi relative entropies [Mat13, FF21].

The generalized unextendible entanglement of a bipartite state has been defined in [WWW24]. We include a short discussion on the topic for necessary development.

Definition 5 ([WWW24]). The generalized unextendible entanglement of a bipartite state ρ_{AB}, induced by a generalized divergence $\mathbf{D}$ between states, is defined as

$$\mathbf{E}^u(\rho_{AB}) := \inf_{\omega_{ABE}\in\mathcal{S}(ABE)} \frac{1}{2}\left\{\begin{array}{c}\mathbf{D}(\rho_{AB}\|\,\mathrm{Tr}_B[\omega_{ABE}]):\\ \mathrm{Tr}_E[\omega_{ABE}]=\rho_{AB}\end{array}\right\}, \tag{29}$$

where the optimization is over every state ρ_{ABE} that is an extension of the state ρ_{AB}. We also adopt the following alternative notations sometimes because they can be helpful to make the bipartition $A|B$ clear:

$$\mathbf{E}^u(A;B)_\rho \equiv \mathbf{E}^u(\rho_{A:B}) \equiv \mathbf{E}^u(\rho_{AB}). \tag{30}$$

Let us define the following set of extensions of a bipartite state ρ_{AB}:

$$\mathrm{Ext}(\rho_{AB}) := \{\omega_{ABE} : \mathrm{Tr}_{BE}[\omega_{ABE}] = \rho_{AB}\}, \tag{31}$$

where E is isomorphic to B. This allows us to write the generalized unextendible entanglement of ρ_{AB}, induced by the generalized divergence $\mathbf{D}$, as

$$\mathbf{E}^u(\rho_{AB}) = \inf_{\omega_{ABE}\in\mathrm{Ext}(\rho_{AB})} \frac{1}{2}\mathbf{D}(\rho_{AB}\|\,\mathrm{Tr}_E[\omega_{ABE}]). \tag{32}$$

Alternatively, one can define the set of state-dependent free states as follows:

$$\mathcal{F}(\rho_{AB}) := \{\mathrm{Tr}_B[\omega_{ABE}] : \omega_{ABE}\in\mathrm{Ext}(\rho_{AB})\}. \tag{33}$$

The generalized unextendible entanglement of the state ρ_{AB} can then be written as follows:

$$\mathbf{E}^u(\rho_{AB}) = \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2}\mathbf{D}(\rho_{AB}\|\sigma_{AB}). \tag{34}$$

Theorem 1 ([WWW24]). *The generalized unextendible entanglement of bipartite state does not increase under the action of a two-extendible channel. That is,*

$$\mathbf{E}^u(\rho_{AB}) \geqslant \mathbf{E}^u(\mathcal{N}_{AB\to A'B'}(\rho_{AB})), \tag{35}$$

where $\mathcal{N}_{AB\to A'B'}$ is a two-extendible channel.

Proof. See theorem 2 in [WWW24]. □

A direct consequence of theorem 1 is that the generalized unextendible entanglement of a bipartite state does not increase under the action of one-way LOCC channels.

The generalized unextendible entanglement provides a framework for quantifying the unextendibility of a bipartite state ρ_{AB} with respect to the system B. A different measure for unextendibility was considered in [KDWW19, KDWW21], where the divergence was measured from the fixed set of two-extendible states. However, in definition 5, the divergence is measured by means of a set of states that depend on the input state itself. Although both measures are equal to the minimal possible value of $\mathbf{D}$ when ρ_{AB} is two-extendible, they are not equal in general.

The unextendible entanglement is a measure of entanglement between two systems, and as such, it is expected to obtain

its maximum value for the maximally entangled state. This is indeed the case, as is evident from the following argument. An arbitrary bipartite state ρ_{AB} can be established between Alice and Bob with the help of a maximally entangled state $\Phi^d_{A_0B_0}$ of sufficiently large Schmidt rank and a one-way LOCC channel, where $\dim(A_0) = \dim(B_0) = \min\{\dim(A), \dim(B)\}$. A simple protocol to perform this transformation is as follows: Alice prepares the state $\rho_{AA'}$ locally. We can assume $\dim(A') \leqslant \dim(A)$ without loss of generality. She uses the maximally entangled state $\Phi^d_{A_0B_0}$ to implement the teleportation protocol and send the state on system A' to Bob, thus establishing the state ρ_{AB} between Alice and Bob. The aforementioned protocol can be mathematically represented as the following one-way LOCC channel [KW24, chapter 5]:

$$\mathcal{L}^{\rho,\rightarrow}_{A_0B_0\rightarrow AB}\left(\Phi^d_{A_0B_0}\right) = \sum_{x,z=0}^{d-1} \operatorname{Tr}_{A_0A'}\left[\Phi^{z,x}_{A_0A'} W^{z,x}_{B_0}\left(\rho_{AA'}\otimes\Phi_{A_0B_0}\right)\left(W^{z,x}_{B_0}\right)^\dagger\right], \quad (36)$$

where $\{W^{z,x}\}_{z,x}$ is the set of Heisenberg–Weyl operators and $\Phi^{z,x}_{A_0A'} := W^{z,x}_{A_0}\Phi^d_{A_0A'}(W^{z,x}_{A_0})^\dagger$. Since the generalized unextendible entanglement of a bipartite state does not increase under the action of a one-way LOCC channel, the following inequality holds for every state ρ_{AB}:

$$\mathbf{E}^u(\rho_{AB}) = \mathbf{E}^u\left(\mathcal{L}^{\rho,\rightarrow}_{A_0B_0\rightarrow AB}\left(\Phi^d_{A_0B_0}\right)\right) \leqslant \mathbf{E}^u\left(\Phi^d_{A_0B_0}\right), \quad (37)$$

where $\mathcal{L}^{\rho,\rightarrow}_{A_0B_0\rightarrow AB}$ is the channel defined in (36) and $d := \min\{\dim(A), \dim(B)\}$.

4.2.1. Smooth-min unextendible entanglement. The unextendible entanglement of states was studied in detail in [WWW24] for several different underlying divergences, with applications in finding efficiently computable upper bounds on the probabilistic and exact one-way distillable entanglement and key of a state. A stronger no-go theorem for probabilistic key distillation was obtained in [SW24a] using the min-relative entropy as the underlying divergence for the unextendible entanglement. In this work, we are specifically interested in the unextendible entanglement of a state induced by the smooth-min relative entropy to understand the limits of one-shot approximate distillable key of a bipartite state using one-way LOCC channels. As a special case of (29), we define the smooth min-unextendible entanglement as follows:

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) := \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2} D^\varepsilon_{\min}(\rho_{AB}\|\sigma_{AB}), \quad (38)$$

where the set $\mathcal{F}(\rho_{AB})$ was defined in (33) and

$$D^\varepsilon_{\min}(\rho\|\sigma) := -\log_2 \inf_{0\leqslant\Lambda\leqslant I}\{\operatorname{Tr}[\Lambda\sigma] : \operatorname{Tr}[\Lambda\rho] \geqslant 1-\varepsilon\} \quad (39)$$

is the smooth-min relative entropy [BD10, BD11], also known as the hypothesis testing relative entropy [WR12].

We will often use the following quantity in our discussions:

$$J^\varepsilon_{\min}(\rho_{AB}) := 2^{-2E^{u,\varepsilon}_{\min}(\rho_{AB})}, \quad (40)$$

which we will abbreviate as $J^\varepsilon_{\min}$ when the state it acts upon is obvious from the context. The quantity $J^\varepsilon_{\min}(\rho_{AB})$ can alternatively be written as follows:

$$J^\varepsilon_{\min}(\rho_{AB}) = \sup_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \inf_{0\leqslant\Lambda\leqslant I}\{\operatorname{Tr}[\Lambda\sigma] : \operatorname{Tr}[\Lambda\rho] \geqslant 1-\varepsilon\}. \quad (41)$$

The set $\mathcal{F}(\rho_{AB})$ is a convex set of quantum states, and the set $\{\Lambda : 0 \leqslant \Lambda \leqslant I : \operatorname{Tr}[\Lambda\rho] \geqslant 1-\varepsilon\}$ is a convex set of measurement operators for a fixed state ρ. Therefore, using Sion's minimax theorem [Sio58], we can interchange the supremum and infimum to arrive at the following equality:

$$J^\varepsilon_{\min}(\rho_{AB}) = \inf_{0\leqslant\Lambda\leqslant I} \sup_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})}\{\operatorname{Tr}[\Lambda\sigma] : \operatorname{Tr}[\Lambda\rho] \geqslant 1-\varepsilon\}. \quad (42)$$

The above equality gives an interpretation for the quantity $J^\varepsilon_{\min}(\rho_{AB})$ in the hypothesis testing setting. Given a quantum state ρ_{AB} and an arbitrary state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$, the quantity $J^\varepsilon_{\min}(\rho_{AB})$ denotes the minimum type-II error probability in the worst case when the type-I error probability is guaranteed to be less than ε. Note that the quantity $J^\varepsilon_{\min}$ decreases monotonically with increasing smooth-min unextendible entanglement. As such, $J^\varepsilon_{\min}$ is smaller for highly entangled states and larger for weakly entangled states, and the minimum value is achieved for the maximally entangled state due to (37).

Proposition 1. *The unextendible entanglement of a maximally entangled state with Schmidt rank d is equal to the following:*

$$E^{u,\varepsilon}_{\min}\left(\Phi^d_{AB}\right) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \quad (43)$$

Proof. See appendix A. □

Proposition 2. *The smooth-min unextendible entanglement of a state ρ_{AB} is bounded as follows:*

$$-\frac{1}{2}\log_2(1-\varepsilon) \leqslant E^{u,\varepsilon}_{\min}(\rho_{AB}) \leqslant \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), \quad (44)$$

where $d := \min\{\dim(A), \dim(B)\}$ with $\dim(A)$ and $\dim(B)$ being the dimensions of system A and B, respectively.

Consequently,

$$\frac{1-\varepsilon}{d^2} \leqslant J^\varepsilon(\rho_{AB}) \leqslant 1-\varepsilon. \quad (45)$$

Proof. See appendix B. □

The smooth-min unextendible entanglement of a bipartite state can be computed using a semidefinite program (see appendix H).

4.2.2. α-sandwiched unextendible entanglement. Another quantity that is relevant to this work is the α-sandwiched unextendible entanglement [WWW24], which is defined as follows:

$$\widetilde{E}^{u}_{\alpha}(\rho_{AB}) := \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2}\widetilde{D}_{\alpha}(\rho_{AB}\|\sigma_{AB}) \qquad \forall \alpha \in (1,\infty), \tag{46}$$

where

$$\widetilde{D}_{\alpha}(\rho\|\sigma) := \frac{1}{\alpha-1}\log_2 \operatorname{Tr}\left[\left(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right)^{\alpha}\right] \tag{47}$$

is the α-sandwiched Rényi relative entropy [MLDS+13, WWY14]. The α-sandwiched unextendible entanglement was defined for all $\alpha \in (0,1)\cup(1,\infty)$ in [WWW24], but we restrict our development here to $\alpha \in (1,\infty)$, due to technical reasons that will become apparent in section 5.

Consider the special case when $\alpha \to \infty$. It was shown in [MLDS+13, theorem 5] that the α-sandwiched relative entropy is equal to the max-relative entropy [Dat09] when $\alpha \to \infty$; that is,

$$D_{\max}(\rho\|\sigma) = \lim_{\alpha\to\infty} \widetilde{D}_{\alpha}(\rho\|\sigma). \tag{48}$$

Corresponding to the max-relative entropy, the max-unextendible entanglement is defined as follows:

$$E^{u}_{\max}(\rho_{AB}) := \frac{1}{2}\inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} D_{\max}(\rho_{AB}\|\sigma_{AB}). \tag{49}$$

Besides monotonicity under two-extendible channels, the α-sandwiched unextendible entanglement has several other properties desirable in a resource monotone. We state some of the relevant properties below.

- **Subadditivity:** The α-sandwiched unextendible entanglement obeys the following subadditivity inequality [WWW24, proposition 13] for all $\alpha \in \left[\frac{1}{2},1\right)\cup(1,\infty)$:

$$\widetilde{E}^{u}_{\alpha}(\rho_{A_1B_1}\otimes\sigma_{A_2B_2}) \leqslant \widetilde{E}^{u}_{\alpha}(\rho_{A_1B_1}) + \widetilde{E}^{u}_{\alpha}(\sigma_{A_2B_2}). \tag{50}$$

- **Additivity of max-unextendible entanglement:** The max-unextendible entanglement is additive under tensor product of states [WWW24, proposition 14]; that is,

$$E^{u}_{\max}(\rho_{A_1B_1}\otimes\sigma_{A_2B_2}) = E^{u}_{\max}(\rho_{A_1B_1}) + E^{u}_{\max}(\sigma_{A_2B_2}). \tag{51}$$

- **Monotonicity in α:** The α-sandwiched unextendible entanglement of a state increases monotonically with increasing α, which follows from the fact that the α-sandwiched Rényi relative entropy between two states increases monotonically with α [MLDS+13, theorem 7].
- **Semidefinite representation:** The max-unextendible entanglement can be computed using a semidefinite program [WWW24] (see appendix H for a review).

The max-unextendible entanglement of a state can be written as a limiting case of the α-sandwiched unextendible entanglement as follows:

$$\lim_{\alpha\to\infty}\widetilde{E}^{u}_{\alpha}(\rho_{AB}) = \sup_{\alpha\in(1,\infty)}\frac{1}{2}\inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})}\widetilde{D}_{\alpha}(\rho_{AB}\|\sigma_{AB}) \tag{52}$$

$$= \frac{1}{2}\inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})}\sup_{\alpha\in(1,\infty)}\widetilde{D}_{\alpha}(\rho_{AB}\|\sigma_{AB}) \tag{53}$$

$$= \frac{1}{2}\inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} D_{\max}(\rho_{AB}\|\sigma_{AB}) \tag{54}$$

$$= E^{u}_{\max}(\rho_{AB}), \tag{55}$$

where the first equality follows from the monotonicity of the α-sandwiched unextendible entanglement in α. The α-sandwiched Rényi relative entropy $\widetilde{D}_{\alpha}(\rho\|\sigma)$ is lower-semicontinuous with respect to σ [MO21, lemma IV.8] (see also [DKQ+23, remark 38]), and it increases monotonically with $\alpha \in (1,\infty)$. Therefore, we can use the Mosonyi–Hiai minimax theorem from [MH11, corollary A.2] to arrive at the second equality above. The last two equalities follow from the equality in (48) and the definition of the max-unextendible entanglement, respectively.

The subadditivity of α-sandwiched unextendible entanglement is useful in the analysis of one-shot, one-way secret-key distillation from independent and identically distributed (i.i.d.) copies of a bipartite state, as we shall see in section 5.2.

5. Limits on secret-key distillation from bipartite states

In this section we use the framework of unextendible entanglement discussed in section 4 to obtain upper bounds on the one-shot, one-way distillable key of a state defined in (14).

Consider a quantum state $\psi^{\gamma}_{ABA'B'E}$, which is an extension of a private state $\gamma^{k}_{ABA'B'}$ with system E held by an eavesdropper. The reduced state of $\psi^{\gamma}_{ABA'B'E}$ on systems AE is a product state, with the reduced state on system A being the maximally mixed state. This is evident from the equivalence between a bipartite private state and a tripartite secret-key state. It was further shown in [WWW24, appendix K] that applying a twisting unitary on the joint systems of Alice and the eavesdropper is also insufficient to establish any correlations between Alice's key system, A, and the eavesdropper's system, E. We state this formally in lemma 1, which we later use to establish the main results of this work.

Lemma 1 ([WWW24]). *Let $\psi^{\gamma}_{ABA'B'EE'R}$ be a purification of a bipartite private state $\gamma^{k}_{ABA'B'}$. For every purification for which system E is isomorphic to B and system E' is isomorphic to B', the following equality holds:*

$$\operatorname{Tr}_{A'BB'E'R}\left[W^{\dagger}_{AEA'E'}\psi^{\gamma}W_{AEA'E'}\right] = \pi_A\otimes\sigma_E, \tag{56}$$

where τ_E is a quantum state, π_A is the maximally mixed state, and $W_{AEA'E'}$ is a twisting unitary of the form given in (9).

Proof. See [WWW24, appendix K]. □

The fact that Alice's system is in a product state with the eavesdropper ensures that the state shared by Alice and the eavesdropper does not pass the privacy test with a probability greater than $\frac{1}{k}$. We generalize this statement to approximate private states in lemma 2 below.

Lemma 2. *Fix $k \in \mathbb{N}$ and $\varepsilon \in \left[0, 1 - \frac{1}{k^2}\right]$. Let $\sigma_{ABA'B'}$ be a quantum state such that*

$$F\left(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}\right) \geqslant 1 - \varepsilon, \tag{57}$$

where $\gamma^k_{ABA'B'}$ is a bipartite private state holding $\log_2 k$ secret key bits. Let $V_{ABA'B'}$ be the twisting unitary corresponding to the private state; that is, there exists a state $\tau_{A'B'}$ such that

$$\gamma^k_{ABA'B'} = V_{ABA'B'}\left(\Phi^k_{AB} \otimes \tau_{A'B'}\right) V^\dagger_{ABA'B'}. \tag{58}$$

The probability of an arbitrary state $\omega_{AEA'E'} \in \mathcal{F}(\sigma_{ABA'B'})$ passing the γ^k-privacy test is bounded from above by the following quantity:

$$\operatorname{Tr}[\Pi^\gamma_{AEA'E'}\omega_{AEA'E'}] \leqslant \varsigma(\varepsilon, k), \tag{59}$$

where

$$\varsigma(\varepsilon, k) := \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)}}{k^2}, \tag{60}$$

$\Pi^\gamma_{ABA'B'}$ is the privacy test, system B is isomorphic to E, and system B' is isomorphic to E'. The set $\mathcal{F}(\sigma_{ABA'B'})$ was defined in (33).

Proof. Let $\phi^\sigma_{ABA'B'EE'R}$ be an arbitrary purification of $\sigma_{ABA'B'}$, such that system E is isomorphic to B and system E' is isomorphic to B'. Then the quantum state $\operatorname{Tr}_{BB'R}[\phi^\sigma]$ is in the set $\mathcal{F}(\sigma_{ABA'B'})$. Let $\psi^\gamma_{ABA'B'EE'R}$ be a purification of $\gamma^k_{ABA'B'}$. An arbitrary purification of the private state $\gamma^k_{ABA'B'}$ is of the following form:

$$\psi^\gamma_{ABA'B'X} = V_{ABA'B'}\left(\Phi^k_{AB} \otimes \psi^\tau_{A'B'X}\right) V^\dagger_{ABA'B'}, \tag{61}$$

where $\psi^\tau_{A'B'X}$ is a pure state and X is a purifying system.

As a consequence of Uhlmann's theorem, consider that

$$F\left(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}\right) = \max_{\psi^\gamma} |\langle\psi^\gamma|\phi^\sigma\rangle|^2 \tag{62}$$

$$= \max_{\psi^\gamma} F\left(\psi^\gamma_{ABA'B'EE'R}, \phi^\sigma_{ABA'B'EE'R}\right) \tag{63}$$

$$= \max_{\psi^\tau_{A'B'EE'R}} F\left(V_{ABA'B'}\left(\Phi^k \otimes \psi^\tau\right) V^\dagger_{ABA'B'}, \phi^\sigma\right). \tag{64}$$

The maximizations in the first and second equalities are over every purification ψ^γ of $\gamma^k_{ABA'B'}$ on the systems $ABA'B'EE'R$. Since every purification of the state $\gamma^k_{ABA'B'}$ can be written in the form mentioned in (61), the maximization over every purification $\psi^\gamma_{ABA'B'EE'R}$ is equivalent to a maximization over every purification $\psi^\tau_{A'B'EE'R}$ of the state $\tau_{A'B'}$. Therefore, there exists a pure state $\psi^\tau_{A'B'EE'R}$ and a corresponding purification $\psi^\gamma_{ABA'B'EE'R}$ such that the following equality holds:

$$F\left(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}\right) = |\langle\psi^\gamma|\phi^\sigma\rangle|^2 = F(\psi^\gamma, \phi^\sigma). \tag{65}$$

Using the data-processing inequality for fidelity of states, consider that

$$\begin{aligned} F(\psi^\gamma, \phi^\sigma) &\leqslant F\Big(\operatorname{Tr}_{A'BB'E'R}\left[V^\dagger_{AEA'E'}\psi^\gamma V_{AEA'E'}\right], \\ &\qquad \operatorname{Tr}_{A'BB'E'R}\left[V^\dagger_{AEA'E'}\phi^\sigma V_{AEA'E'}\right]\Big) \qquad (66) \\ &= F\left(\pi_A \otimes \tau_E, \operatorname{Tr}_{A'E'}\left[V^\dagger_{AEA'E'}\omega_{AEA'E'}V_{AEA'E'}\right]\right), \qquad (67) \end{aligned}$$

where we have used lemma 1 to arrive at the final equality and $\omega_{AEA'E'}$ is defined in the statement of the lemma.

Now consider the twirling channel, defined as follows:

$$\mathcal{T}_{AB}(\cdot) = \int \mathrm{d}U \left(U_A \otimes \overline{U}_B\right)(\cdot)\left(U_A \otimes \overline{U}_B\right)^\dagger, \tag{68}$$

where the integral is with respect to the Haar measure. The action of this channel on an arbitrary quantum state ρ_{AB}, with $\dim(A) = \dim(B) = d$, results in the following isotropic state [HH99, Wat18]:

$$\mathcal{T}_{AB}(\rho_{AB}) = \operatorname{Tr}\left[\Phi^d_{AB}\rho_{AB}\right]\Phi^d_{AB} + \left(1 - \operatorname{Tr}\left[\Phi^d_{AB}\rho_{AB}\right]\right)\frac{I_{AB} - \Phi^d_{AB}}{d^2 - 1}. \tag{69}$$

Consider that

$$\begin{aligned} \operatorname{Tr}\left[\Phi^k_{AE}\left(\pi_A \otimes \tau_E\right)\right] &= \frac{1}{k}\operatorname{Tr}\left[\Phi^k_{AE}\left(I_A \otimes \tau_E\right)\right] \qquad (70) \\ &= \frac{1}{k^2}\operatorname{Tr}[\tau_E] \qquad (71) \\ &= \frac{1}{k^2}. \qquad (72) \end{aligned}$$

Therefore,

$$\mathcal{T}_{AE}(\pi_A \otimes \tau_E) = \frac{1}{k^2}\Phi^k_{AE} + \left(1 - \frac{1}{k^2}\right)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1} = \frac{I_{AE}}{k^2}. \tag{73}$$

The action of the twirling channel $\mathcal{T}_{AE}$ on the state $\operatorname{Tr}_{A'E'}\left[V^\dagger\omega_{AEA'E'}V\right]$ is given by the following expression:

$$\mathcal{T}_{AE}\left(\operatorname{Tr}_{A'E'}\left[V^\dagger\omega_{AEA'E'}V\right]\right) = q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}, \tag{74}$$

where

$$q := \operatorname{Tr}\left[\Phi^k_{AE}\left(\operatorname{Tr}_{A'E'}\left[V^\dagger\omega_{AEA'E'}V\right]\right)\right]. \tag{75}$$

The above expression can be rewritten as follows:

$$\begin{aligned} q &= \operatorname{Tr}\left[V_{AEA'E'}\left(\Phi^k_{AE} \otimes I_{A'E'}\right)V^\dagger_{AEA'E'}\omega_{AEA'E'}\right] \\ &= \operatorname{Tr}[\Pi^\gamma_{AEA'E'}\omega_{AEA'E'}], \qquad (76) \end{aligned}$$

where $\Pi^{\gamma}_{AEA'E'}$ is the γ-privacy test defined in (13). Therefore, q can be interpreted as the probability of the state $\omega_{AEA'E'}$ passing the γ-privacy test.

Going back to (67) and using the data-processing inequality for fidelity, we arrive at the following inequality:

$$F(\psi^{\gamma},\phi^{\sigma}) \leqslant F\left(\mathcal{T}_{AE}(\pi_A\otimes\tau_E),\mathcal{T}_{AE}\left(\mathrm{Tr}_{A'E'}\left[V^{\dagger}\omega V\right]\right)\right) \tag{77}$$

$$= F\left(\pi_{AE},\mathcal{T}_{AE}\left(\mathrm{Tr}_{A'E'}\left[V^{\dagger}\omega V\right]\right)\right). \tag{78}$$

Since the above inequality holds for all $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}) \geqslant 1-\varepsilon$ for some private state $\gamma^{k}_{ABA'B'}$ and every $\omega_{AEA'E'}$ that is in the set $\mathcal{F}(\sigma_{ABA'B'})$, we can combine (65), (67), and (78) to arrive at the following inequality:

$$1-\varepsilon \leqslant F\left(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}\right) \tag{79}$$

$$\leqslant F\left(\pi_{AE},\mathcal{T}_{AE}\left(\mathrm{Tr}_{A'E'}\left[V^{\dagger}\omega V\right]\right)\right) \tag{80}$$

$$= F\left(\pi_{AE}, q\,\Phi^{k}_{AE} + (1-q)\,\frac{I_{AE}-\Phi^{k}_{AE}}{k^2-1}\right) \tag{81}$$

$$= \left(\sqrt{\frac{q}{k^2}} + \sqrt{(1-q)\left(1-\frac{1}{k^2}\right)}\right)^{2}, \tag{82}$$

where the first equality follows from (74) and the last equality follows by evaluating the fidelity between the two isotropic states.

The inequality in (82) is satisfied for all $q\in[0,1]$ if $\varepsilon \geqslant 1-\frac{1}{k^2}$. If $\varepsilon \in \left[0,1-\frac{1}{k^2}\right]$ then q must lie in the following range for (82) to hold:

$$0 \leqslant q \leqslant \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)}}{k^2}. \tag{83}$$

See appendix C for a detailed proof of the aforementioned statement. Since we have identified q to be the probability of the state $\omega_{AEA'E'}$ passing the γ-privacy test, we conclude the statement of the lemma. □

Lemma 2 plays a central role in obtaining lower bounds on the unextendible entanglement of an approximate private state $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}) \geqslant 1-\varepsilon$ for some private state $\gamma^{k}_{ABA'B'}$.

Remark 2. Note that $F\left(\pi_{AB},\Phi^{k}_{AB}\right) = \frac{1}{k^2}$, where π_{AB} is the maximally mixed state. Therefore, if $\varepsilon \geqslant 1-\frac{1}{k^2}$ for some $k\in\mathbb{N}$, then the following inequality holds for the one-shot, one-way distillable key of an arbitrary bipartite state ρ_{AB}:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \geqslant \log_2 k. \tag{84}$$

As such, choosing $\varepsilon \geqslant 1-\frac{1}{k^2}$ allows the one-shot, one-way distillable key of a separable state to be non-zero, which makes this regime uninteresting from a practical perspective.

5.1. Smooth-min unextendible entanglement upper bound on one-shot distillable secret key of bipartite states

The γ-privacy test is a special POVM that can be used to distinguish a bipartite state $\sigma_{ABA'B'}$ from any state $\omega_{AEA'E'} \in \mathcal{F}(\sigma_{ABA'B'})$. Recall that the smooth-min unextendible entanglement quantifies the ability to distinguish between a state ρ_{AB} from an arbitrary state $\sigma_{AB}\in\mathcal{F}(\rho_{AB})$. Therefore, lemma 2 allows us to obtain a bound on the unextendible entanglement of a state $\sigma_{ABA'B'}$ satisfying $F(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}) \geqslant 1-\varepsilon$. This is stated as proposition 3 below.

Proposition 3. *Fix $k\in\mathbb{N}$ and $\varepsilon\in\left[0,1-\frac{1}{k^2}\right]$. Consider a quantum state $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}) \geqslant 1-\varepsilon$, where $\gamma^{k}_{ABA'B}$ is a bipartite private state. The smooth-min unextendible entanglement of the state $\sigma_{ABA'B'}$ is bounded from below by the following quantity:*

$$E^{u,\varepsilon}_{\min}(\sigma_{ABA'B'}) \geqslant -\frac{1}{2}\log_2(\varsigma(\varepsilon,k)), \tag{85}$$

where $\varsigma(\varepsilon,k)$ is defined in (60).

Proof. Let $\sigma_{ABA'B'}$ be a quantum state such that $F(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}) \geqslant 1-\varepsilon$ for some bipartite private state $\gamma^{k}_{ABA'B'}$ and some $\varepsilon\in\left[0,1-\frac{1}{k^2}\right]$. The following inequality holds for every such state $\sigma_{ABA'B'}$ [WTB17, lemma 9]:

$$\mathrm{Tr}[\Pi^{\gamma}_{ABA'B'}\sigma_{ABA'B'}] \geqslant 1-\varepsilon, \tag{86}$$

where the projector $\Pi^{\gamma}_{ABA'B'}$ is the γ^{k}-privacy test defined in (13).

Now consider the hypothesis testing relative entropy between the state $\sigma_{ABA'B'}$, for which $F(\sigma_{ABA'B'},\gamma^{k}_{ABA'B'}) \geqslant 1-\varepsilon$ for some private state $\gamma^{k}_{ABA'B'}$, and an arbitrary state $\omega_{AEA'E'}$ which lies in the set $\mathcal{F}(\sigma_{ABA'B'})$:

$$D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) = \sup_{0\leqslant\Lambda\leqslant I} -\log_2\{\mathrm{Tr}[\Lambda\omega] : \mathrm{Tr}[\Lambda\sigma] \geqslant 1-\varepsilon\}. \tag{87}$$

It is understood here that system E is isomorphic to B and system E' is isomorphic to B'.

Since $\Pi^{\gamma}_{ABA'B'}$ is a specific measurement operator that satisfies the constraints in (87), the following inequality holds:

$$D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) \geqslant -\log_2\mathrm{Tr}[\Pi^{\gamma}_{AEA'E'}\omega_{AEA'E'}], \tag{88}$$

which leads to the following inequality after applying lemma 2:

$$D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) \geqslant -\log_2(\varsigma(\varepsilon,k)). \tag{89}$$

Since (89) holds for all $\omega_{AEA'E'}$ in the set $\mathcal{F}(\sigma_{ABA'B'})$, we conclude that the smooth-min unextendible entanglement of the state $\sigma_{ABA'B'}$ is bounded from below by the following quantity:

$$E^{u,\varepsilon}_{\min}(\sigma_{ABA'B'}) = \frac{1}{2}\inf_{\omega\in\mathcal{F}(\sigma)} D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) \tag{90}$$

$$\geqslant -\frac{1}{2}\log_2(\varsigma(\varepsilon,k)), \tag{91}$$

thus completing the proof. □

Remark 3. For a fixed $\varepsilon \in \left[0, \frac{3}{4}\right]$, if $E_{\min}^{u,\varepsilon}(\sigma_{ABA'B'}) < -\frac{1}{2}\log_2(\varsigma(\varepsilon,2))$, then there does not exist a private state $\gamma_{ABA'B'}^{k}$ such that $F\left(\sigma_{ABA'B'}, \gamma_{ABA'B'}^{k}\right) \geqslant 1-\varepsilon$.

The unextendible entanglement of a state does not increase under the action of a one-way LOCC channel. Therefore, for any one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ that is used to distill an ε-approximate private state $\sigma_{A'B'A''B''}$ from a bipartite resource state ρ_{AB}, the unextendible entanglement of ρ_{AB} must be larger than the unextendible entanglement of $\sigma_{A'B'A''B''}$, which in turn is bounded from below by $-\frac{1}{2}\log_2(\varsigma(\varepsilon,k))$ as stated in proposition 3. That is,

$$E_{\min}^{u,\varepsilon}(\rho_{AB}) \geqslant E_{\min}^{u,\varepsilon}(\sigma_{A'B'A''B''}) \geqslant -\frac{1}{2}\log_2\left(\varsigma\left(\varepsilon,k\right)\right). \tag{92}$$

Rewriting the above inequality as an upper bound on $\log_2 k$, which is the maximum number of secret bits that can be distilled from ρ_{AB} using a two-extendible channel, yields an upper bound on the one-shot, one-way distillable key of the state ρ_{AB}.

Theorem 2 (unextendibility bound on one-shot distillable key). *Fix $\varepsilon \in (0,1)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\varepsilon < J_{\min}^{\varepsilon}(\rho_{AB}) \leqslant \frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon\left(1-\varepsilon\right)}}{2}, \tag{93}$$

where $J_{\min}^{\varepsilon}(\rho_{AB})$ is defined in (40). Then the one-shot, one-way distillable key of a bipartite state ρ_{AB} is bounded from above by the following quantity:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J_{\min}^{\varepsilon}(\rho_{AB})(1-J_{\min}^{\varepsilon}(\rho_{AB}))}+\sqrt{\varepsilon\left(1-\varepsilon\right)}}{J_{\min}^{\varepsilon}(\rho_{AB})-\varepsilon}\right)^2+1\right]. \tag{94}$$

If $J_{\min}^{\varepsilon}(\rho_{AB}) > \frac{1}{4}+\frac{\varepsilon}{2}+\frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}$, then the one-shot, one-way distillable key of the state is equal to zero.

Proof. See appendix D. □

When $\varepsilon = 0$, the upper bound from theorem 2 simplifies to the min-unextendible entanglement bound on the exact one-way distillable key of a state obtained in [WWW24, theorem 24].

The one-shot, one-way distillable key of a state does not increase under the action of one-way LOCC channels, and we expect the same from any reasonable bound on the quantity. Similarly, we expect that the bound does not increase with decreasing ε because demanding a higher fidelity between the distilled state and the target state should only lead to a lower yield from the distillation process. To examine if the upper bound on the one-shot, one-way distillable key of a state given in theorem 2 satisfies the aforementioned criteria, we invoke lemma 3 stated below.

Lemma 3. *For all $J \in (\varepsilon, 1-\varepsilon]$ and $\varepsilon \in [0,1]$, the following function*

$$f(J,\varepsilon) := \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon\left(1-\varepsilon\right)}}{J-\varepsilon}\right)^2+1\right] \tag{95}$$

decreases monotonically with J and increases monotonically with ε.

Proof. See appendix E. □

Recall that the quantity $J_{\min}^{\varepsilon}(\rho_{AB})$ increases under the action of one-way LOCC channels. Therefore, lemma 3 implies that the upper bound on the one-shot, one-way distillable key of a state given in theorem 2 decreases monotonically under the action of one-way LOCC channels, and it increases monotonically with ε.

The smooth-min unextendible entanglement of a state can be written as a semidefinite program (see appendix H), which allows us to compute the upper bound on the one-shot, one-way distillable key given in theorem 2 using a semidefinite program. In figure 3, we demonstrate some numerical results for the smooth-min unextendible entanglement upper bound on the one-shot, one-way distillable key of an isotropic state [HH99], which is parameterized as follows:

$$\zeta_{AB}^{F,d} = F\Phi_{AB}^{d} + (1-F)\frac{I_{AB}-\Phi_{AB}^{d}}{d^2-1}, \tag{96}$$

where F is a parameter in the interval $[0,1]$ and $d = d_A = d_B$.

In figure 3(c), we compare the upper bounds on $K_D^{\varepsilon,\rightarrow}\left(\zeta_{AB}^{F,d}\right)$ and $K_D^{\varepsilon,\rightarrow}\left(\left(\zeta_{AB}^{F,d}\right)^{\otimes 2}\right)$ for $\varepsilon = 0.01$ obtained using theorem 2. The time complexity of computing the upper bound on the one-shot, one-way distillable key of n copies of a state using the SDP bound in theorem 2 is exponential in n. We address this problem later in section 5.2 by obtaining an efficiently computable upper bound on the n-shot, one-way distillable key of a state.

5.1.1. Comparison with smooth-min relative entropy of entanglement bound. The one-shot distillable key of a state, roughly defined as the number of approximate secret bits that can be distilled from the state using an LOCC channel, is known to be bounded from above by the smooth-min relative entropy of entanglement of the state [WTB17], which is defined as follows:

$$E_R^{\varepsilon}(\rho_{AB}) := \inf_{\sigma_{AB}\in \mathrm{SEP}(A:B)} D_{\min}^{\varepsilon}(\rho_{AB}\|\sigma_{AB}), \tag{97}$$

where $\mathrm{SEP}(A:B)$ denotes the set of all separable states in $\mathcal{S}(AB)$. Naturally, the smooth-min relative entropy of entanglement is also an upper bound on the one-shot, one-way distillable key of a state since every one-way LOCC channel lies in the set of LOCC channels. As such,

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leqslant E_R^{\varepsilon}(\rho_{AB}). \tag{98}$$

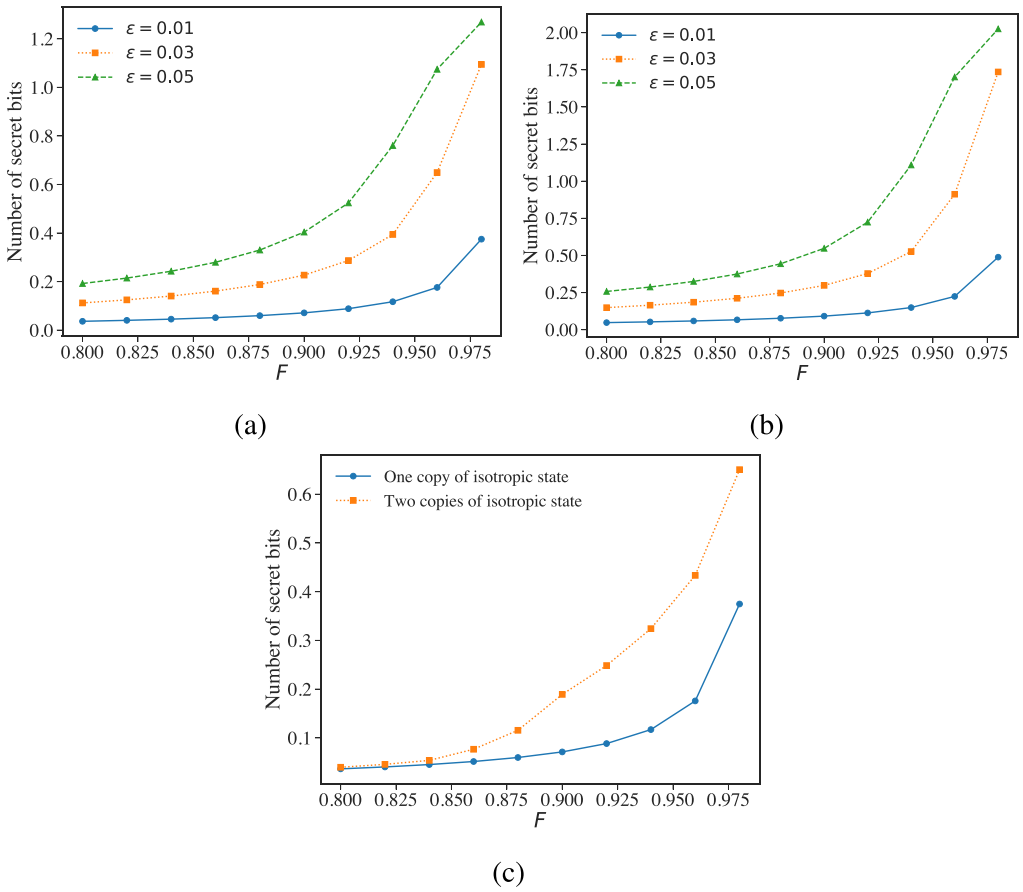


Figure 3. Upper bounds on the one-shot one-way distillable key of an isotropic state, described in (96), using (94). (a) Upper bounds for a two-dimensional isotropic state for different values of ε plotted against the parameter F. (b) Upper bounds for a three-dimensional isotropic state for different values of ε plotted against the parameter F. (c) For $\varepsilon = 0.01$, comparison between the upper bounds obtained for a single copy of a two-dimensional isotropic state with the upper bound obtained for two copies of a two-dimensional isotropic state, plotted against the parameter F.

In general, it is not practical to compute the smooth-min relative entropy of entanglement as it involves an optimization over the set of separable states, which is known to be an NP-hard problem [Gur03, Gha10]. However, one can evaluate this quantity for some highly symmetric states, such as the isotropic state defined in (96). It is known from [HH99] that a d-dimensional isotropic state $\zeta_{AB}^{F,d}$ is separable if and only if $F \leqslant \frac{1}{d}$. As such,

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F,d}\right) = 0 \qquad \forall F \in \left[0, \frac{1}{d}\right]. \tag{99}$$

In proposition 4, we state the smooth-min relative entropy of entanglement of a d-dimensional entangled isotropic state.

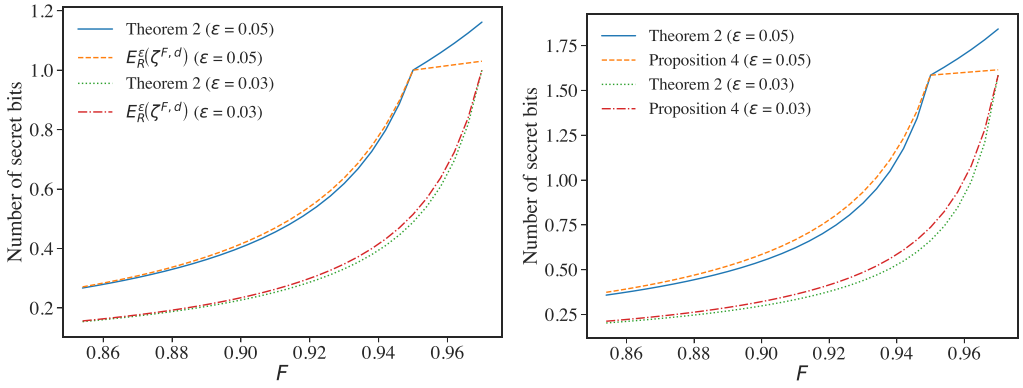
Proposition 4. *The smooth-min relative entropy of entanglement of an isotropic state $\zeta_{AB}^{F,d}$, with $F > \frac{1}{d}$, is equal to the following:*

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F}\right) = \begin{cases} -\log_2\left(1 - \frac{\varepsilon}{1-F}\left(1 - \frac{1}{d}\right)\right) & \text{if} \quad 1 - \varepsilon \geqslant F \\ \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) & \text{otherwise} \end{cases}. \tag{100}$$

Proof. See appendix I. □

The analytical expression for the smooth-min relative entropy of entanglement of isotropic states allows us to compare our bound from theorem 2 with the bound from [WTB17] for isotropic states. We must note that this is not a direct comparison of results since the smooth-min relative entropy of entanglement is an upper bound on the one-shot distillable key of a state, which is expected to be strictly larger than the one-shot, one-way distillable key of the state in general.

In figure 4, we plot the upper bound on the one-shot, one-way distillable key of an isotropic state given in theorem 2 and the smooth-min relative entropy of entanglement of the isotropic state against the parameter F for different values of ε and dimension d. For a range of parameters F, the bound in theorem 2 performs better than the smooth-min relative entropy of entanglement bound, demonstrating the advantage of the bound in theorem 2 over previously known bounds numerically. Moreover, the smooth-min relative entropy of entanglement is not efficiently computable for arbitrary states while



(a) Two-dimensional isotropic state (b) Three-dimensional isotropic state

Figure 4. Comparison between the upper bounds on the one-shot, one-way distillable key of two-dimensional and three-dimensional isotropic states, parameterized as given in (96), obtained using theorem 2 and proposition 4.

the bound in theorem 2 is efficiently computable for arbitrary quantum states.

5.1.2. Simplified upper bounds. The upper bound on the one-shot, one-way distillable key of a bipartite state obtained in theorem 2 is difficult to analyze, due to its complicated form. Weaker but simpler bounds can be obtained by using the smooth-min unextendible entanglement of states.

Relaxation 1: We first consider a relaxation of the upper bound in (94) by finding an algebraic inequality for the function $\varsigma(\varepsilon,k)$ defined in (60):

$$\begin{aligned}\varsigma(\varepsilon,k) &= \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)}}{k^2} && (101)\\ &\leqslant \frac{1}{k^2} + \varepsilon\left(1-\frac{2}{k^2}\right) + 2\frac{\sqrt{k^2\varepsilon}}{k^2} && (102)\\ &\leqslant \frac{1}{k^2} + \varepsilon + 2\frac{\sqrt{\varepsilon}}{k} && (103)\\ &= \left(\frac{1}{k} + \sqrt{\varepsilon}\right)^2, && (104)\end{aligned}$$

where the first inequality follows from the fact that $(k^2-1)(1-\varepsilon) \leqslant k^2$ for all $k \in \mathbb{N}$ and $\varepsilon \in [0,1]$ and the second inequality follows from the fact that $1-\frac{2}{k^2} < 1$ for all $k \in \mathbb{N}$.

We can now use this upper bound on $\varsigma(\varepsilon,k)$ along with the statement of proposition 3 to obtain a lower bound on the smooth-min unextendible entanglement of a state $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geqslant 1-\varepsilon$ for some private state $\gamma^k_{ABA'B'}$. In particular,

$$E^{u,\varepsilon}_{\min}(\sigma_{ABA'B'}) \geqslant -\frac{1}{2}\log_2\left(\frac{1}{k}+\sqrt{\varepsilon}\right)^2 = -\log_2\left(\frac{1}{k}+\sqrt{\varepsilon}\right). \quad (105)$$

This leads to the following simplified but weaker upper bound on the one-shot, one-way distillable key of a bipartite state:

Corollary 1. *Fix $\varepsilon \in (0,1)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon\,(1-\varepsilon)}}{2} \geqslant J^{\varepsilon}_{\min}(\rho_{AB}) > \varepsilon, \quad (106)$$

where $J^{\varepsilon}_{\min}$ is defined in (40). Then the one-shot, one-way distillable key of a bipartite state ρ_{AB} is bounded from above as follows:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leqslant -\log_2\left(\sqrt{J^{\varepsilon}_{\min}(\rho_{AB})} - \sqrt{\varepsilon}\right). \quad (107)$$

Proof. The proof is similar to the proof of theorem 2 and follows directly from (105). □

Relaxation 2: Another way to obtain a simpler bound on the one-shot, one-way distillable key of a state is by considering the trace norm. First we will find a simpler but weaker statement of lemma 2. Consider a state $\sigma_{ABA'B'}$ such that $F(\gamma^k_{ABA'B'}, \sigma_{ABA'B'}) \geqslant 1-\varepsilon$ for some private state $\gamma^k_{ABA'B'}$. Combining (74) and (80), we find that the following inequality holds for any state $\omega_{AEA'E'} \in \mathcal{F}(\sigma_{ABA'B'})$:

$$1-\varepsilon \leqslant F\left(\pi_{AE}, q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right), \quad (108)$$

where $q = \mathrm{Tr}[\Pi^{\gamma}_{AEA'E'}\omega_{AEA'E'}]$ as stated in (76). Using the Fuchs-van de Graaf inequality [FvdG99] (specifically, $F(\rho,\sigma) \leqslant 1-\frac{1}{4}\|\rho-\sigma\|_1^2$), we arrive at the following inequality:

$$\begin{aligned}1-\varepsilon &\leqslant F\left(\pi_{AE}, q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right)\\ &\leqslant 1 - \frac{1}{4}\left\|\pi_{AE} - q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right\|_1^2. \quad (109)\end{aligned}$$

The above inequality can be rewritten as follows:

$$\sqrt{\varepsilon} \geqslant \frac{1}{2}\left\| \pi_{AE} - q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right\|_1 \tag{110}$$

$$= \frac{1}{2}\left\| \frac{1}{k^2}\Phi^k_{AE} - \left(1-\frac{1}{k^2}\right)\frac{I_{AE}-\Phi^k_{AE}}{k^2-1} - q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right\|_1 \tag{111}$$

$$= \frac{1}{2}\left\| \left(\frac{1}{k^2}-q\right)\Phi^k_{AE} + \left(\frac{1}{k^2}-q\right)\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right\|_1 \tag{112}$$

$$= \left|\frac{1}{k^2}-q\right|\left\| \frac{1}{2}\Phi^k_{AE} + \frac{1}{2}\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}\right\|_1 \tag{113}$$

$$= \left|\frac{1}{k^2}-q\right|, \tag{114}$$

where the first equality follows by writing the maximally mixed state as an isotropic state and the last equality follows by realizing that $\frac{1}{2}\Phi^k_{AE} + \frac{1}{2}\frac{I_{AE}-\Phi^k_{AE}}{k^2-1}$ is a quantum state for which the trace norm is equal to 1. The inequality in (114) is satisfied if and only if q lies in the following range:

$$\frac{1}{k^2} - \sqrt{\varepsilon} \leqslant q \leqslant \frac{1}{k^2} + \sqrt{\varepsilon}. \tag{115}$$

Since $q = \mathrm{Tr}[\Pi^{\gamma}_{ABA'B'}\omega_{ABA'B'}]$, we have the following inequality:

$$\mathrm{Tr}[\Pi^{\gamma}_{ABA'B'}\omega_{ABA'B'}] \leqslant \frac{1}{k^2} + \sqrt{\varepsilon}. \tag{116}$$

Using the inequality in (116) and the arguments used in the proof of proposition 3, we can bound the smooth-min unextendible entanglement of the state $\sigma_{ABA'B'}$ as follows:

$$E^{u,\varepsilon}_{\min}(\sigma_{ABA'B'}) \geqslant -\frac{1}{2}\log_2\left(\frac{1}{k^2} + \sqrt{\varepsilon}\right). \tag{117}$$

A relaxed upper bound on the one-shot, one-way distillable key of a bipartite state can be found by using the inequality mentioned above, which we state as corollary 2.

Corollary 2. *Fix $\varepsilon \in (0,1)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2} \geqslant J^{\varepsilon}_{\min}(\rho_{AB}) > \sqrt{\varepsilon}, \tag{118}$$

where $J^{\varepsilon}_{\min}$ is defined in (40). Then the one-shot, one-way distillable key of a bipartite state ρ_{AB} is bounded from above by the following quantity:

$$K^{\varepsilon,\rightarrow}_D(\rho_{AB}) \leqslant -\frac{1}{2}\log_2\left(J^{\varepsilon}_{\min}(\rho_{AB}) - \sqrt{\varepsilon}\right). \tag{119}$$

Proof. The proof is similar to the proof of theorem 2 and follows directly from (117). □

Remark 4. The upper bound on the one-shot, one-way distillable key given in corollary 1 is tighter than the upper bound given in corollary 2 for highly entangled states, but the order is reversed for weakly entangled states. To be precise,

$$K^{\varepsilon,\rightarrow}_D(\rho_{AB}) \leqslant -\log_2\left(\sqrt{J^{\varepsilon}_{\min}} - \sqrt{\varepsilon}\right) \leqslant -\frac{1}{2}\log_2\left(J^{\varepsilon}_{\min} - \sqrt{\varepsilon}\right), \tag{120}$$

for all $J^{\varepsilon}_{\min} \in \left[\sqrt{\varepsilon}, \frac{1}{4}(1+\varepsilon+2\sqrt{\varepsilon})\right]$, and

$$K^{\varepsilon,\rightarrow}_D(\rho_{AB}) \leqslant -\frac{1}{2}\log_2\left(J^{\varepsilon}_{\min} - \sqrt{\varepsilon}\right) \leqslant -\log_2\left(\sqrt{J^{\varepsilon}_{\min}} - \sqrt{\varepsilon}\right), \tag{121}$$

for all $J^{\varepsilon}_{\min} \in \left[\frac{1}{4}(1+\varepsilon+2\sqrt{\varepsilon}), 1-\varepsilon\right]$.

The bounds obtained in corollaries 1 and 2 can be computed using a semidefinite program. In figure 5 we plot the three different upper bounds on the one-shot, one-way distillable key of isotropic states, defined in (96), obtained from theorem 2, corollaries 1 and 2. Notice that the bound from corollary 1 is tighter than the bound from corollary 2 when the resource state is highly entangled.

5.2. One-way secret-key distillation from i.i.d. copies of a state

Resource distillation from independent and identically distributed (i.i.d.) copies of a state is often considered a physically relevant setting. As such, the rate at which secret bits can be distilled from n i.i.d. copies of a state, which is equal to $\frac{1}{n}K^{\varepsilon,\rightarrow}_D\left(\rho^{\otimes n}_{AB}\right)$, is an important quantity from both information-theoretic and practical perspectives.

In principle, the bounds obtained for the one-shot, one-way distillable key of a state can be used to obtain an upper bound on the one-way distillable key rate from n copies of ρ_{AB}, with ε error tolerance, by simply calculating the upper bounds for the state $\rho^{\otimes n}_{AB}$. However, the complexity of computing these bounds scales exponentially with the number of copies n, rendering the computation of these bounds intractable for large enough n. The smooth-min relative entropy is not subadditive; that is, there exists a choice of states ρ^1, ρ^2, σ^2, and σ^2, such that the following inequality does not hold:

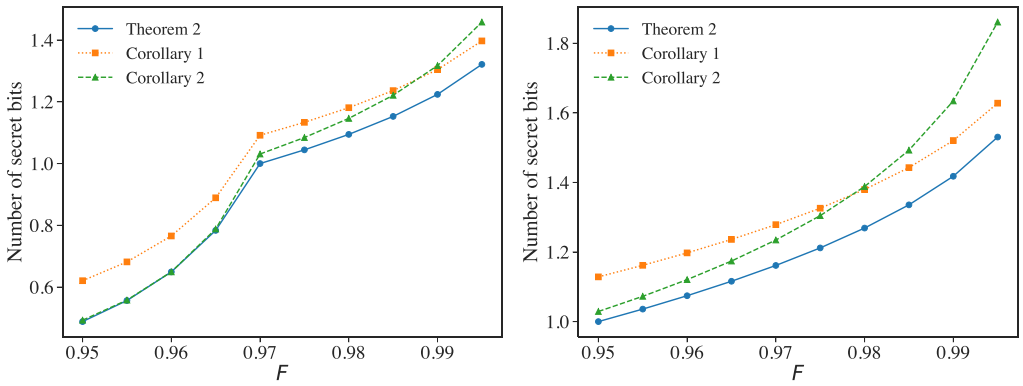
$$D^{\varepsilon}_{\min}\left(\rho^2\otimes\rho^2\|\sigma^1\otimes\sigma^2\right) \leqslant D^{\varepsilon}_{\min}\left(\rho^1\|\sigma^1\right) + D^{\varepsilon}_{\min}\left(\rho^2\|\sigma^2\right), \tag{122}$$

which makes it difficult to obtain a single-letter bound on the one-way distillable key rate with our approach. We turn to the α-sandwiched unextendible entanglement of bipartite states to address this problem.

The smooth-min relative entropy is related to the α-sandwiched Rényi relative entropy by the following inequality [CMW16, lemma 5]:

$$D^{\varepsilon}_{\min}(\rho\|\sigma) \leqslant \widetilde{D}_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right) \tag{123}$$

for all $\varepsilon \in [0,1)$ and $\alpha \in (1,\infty)$. By taking an infimum over all states $\sigma \in \mathcal{F}(\rho)$, we arrive at an inequality relating the smooth-min unextendible entanglement of a state and the α-sandwiched unextendible entanglement of the state, which we state in proposition 5 below.



(a) $\varepsilon = 0.03$ (b) $\varepsilon = 0.05$

Figure 5. Comparison between the upper bounds on the one-shot, one-way distillable key of two-dimensional isotropic states, parameterized as given in (96), obtained using theorem 2, corollaries 1 and 2.

Proposition 5. *Let $\alpha \in (1,\infty)$ and $\varepsilon \in [0,1)$. Then the following inequality holds between the smooth-min unextendible entanglement of a state and the α-sandwiched unextendible entanglement of the state:*

$$E^{u,\varepsilon}_{\min}(\rho) \leqslant \widetilde{E}^{u}_{\alpha}(\rho) + \frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{124}$$

As a counterpart of $J^{\varepsilon}_{\min}(\rho_{AB})$, we define the following quantity for mathematical simplicity:

$$\widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB}) := 2^{-2\widetilde{E}^{u}_{\alpha}(\rho_{AB})}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}} \qquad \forall \alpha \in (1,\infty). \tag{125}$$

It is straightforward to verify from proposition 5 that

$$J^{\varepsilon}_{\min}(\rho_{AB}) \geqslant \widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB}) \qquad \forall \alpha \in (1,\infty). \tag{126}$$

One can simply use theorem 2 and lemma 3 to obtain an upper bound on the one-shot, one-way distillable key of a state in terms of the α-sandwiched unextendible entanglement, as follows:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leqslant f(J^{\varepsilon}_{\min}(\rho_{AB}),\varepsilon) \leqslant f\left(\widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB}),\varepsilon\right) \quad \forall \alpha \in (1,\infty), \tag{127}$$

where the function f is defined in lemma 3. The first inequality follows from theorem 2, and the second inequality follows from (126) and lemma 3.

While the α-sandwiched unextendible entanglement bound is clearly worse than the smooth-min unextendible entanglement bound, it gives a single-letter upper bound on the one-shot, one-way distillable key from n i.i.d. copies of a state ρ_{AB}. The subadditivity of the α-sandwiched unextendible entanglement implies the following for all $\alpha \in (1,\infty)$:

$$\widetilde{J}^{\varepsilon}_{\alpha}\left(\rho^{\otimes n}_{AB}\right) = 2^{-2\widetilde{E}^{u}_{\alpha}\left(\rho^{\otimes n}_{AB}\right)}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}} \geqslant 2^{-2n\widetilde{E}^{u}_{\alpha}(\rho_{AB})}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}}. \tag{128}$$

Let us define the following quantity:

$$\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB}) := 2^{-2n\widetilde{E}^{u}_{\alpha}(\rho_{AB})}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}}. \tag{129}$$

Then the fact that $\widetilde{J}^{\varepsilon}_{\alpha}\left(\rho^{\otimes n}_{AB}\right) \geqslant \widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB})$, combined with lemma 3 and (127), leads to a single-letter upper bound on the one-shot, one-way distillable key of n i.i.d. copies of a state, which we state formally in corollary 3.

Corollary 3. *Fix $\varepsilon \in (0,1)$ and $\alpha \in (1,\infty)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\varepsilon < \widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB}) \leqslant \frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}, \tag{130}$$

where $\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB})$ is defined in (129). Then the n-shot, one-way distillable key of a state ρ_{AB} is bounded from above by the following quantity:

$$K_D^{\varepsilon,\rightarrow}\left(\rho^{\otimes n}_{AB}\right) \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB})\left(1-\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB})\right)} + \sqrt{\varepsilon(1-\varepsilon)}}{\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB}) - \varepsilon}\right)^2 + 1\right]. \tag{131}$$

If $\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB}) > \frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}$, then the n-shot, one-way distillable key of the state is equal to zero.

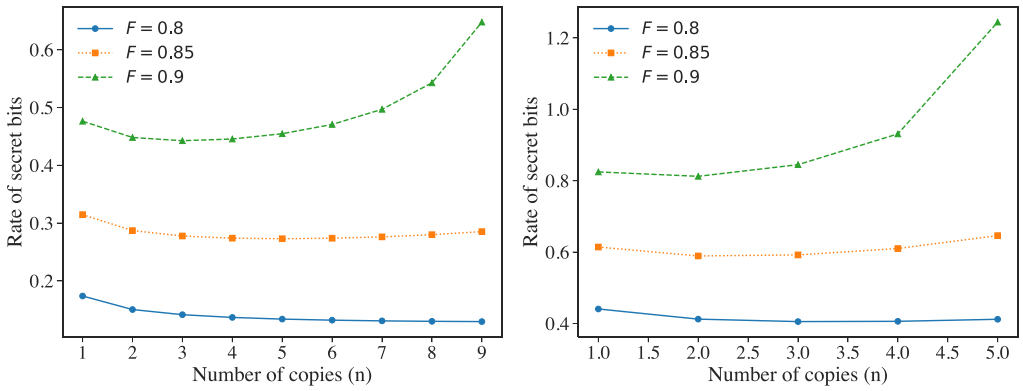
A special case of the bound stated above arises when $\alpha \to \infty$. Let us define the following quantity:

$$J^{\varepsilon}_{\max}(\rho_{AB}) := \lim_{\alpha\to\infty}\widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB}) \tag{132}$$

$$= \left(\lim_{\alpha\to\infty} 2^{-2\widetilde{E}^{u}_{\alpha}(\rho_{AB})}\right)\left(\lim_{\alpha\to\infty}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}}\right) \tag{133}$$

$$= 2^{-2E^{u}_{\max}(\rho_{AB})}(1-\varepsilon), \tag{134}$$

where the second equality follows from the definition of $\widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB})$ and the last equality follows from (55). The max-unextendible entanglement of a state can be computed using an SDP, which implies that $J^{\varepsilon}_{\max}(\rho_{AB})$ can be computed using an SDP. Thus, setting $\alpha \to \infty$ in corollary 3 leads to a single-letter, computable bound on the n-shot, one-way distillable key of a state.



(a) Two-dimensional isotropic state (b) Three-dimensional isotropic state

Figure 6. Upper bounds on the n-shot, one-way distillable-key rate of isotropic states using corollary 3 and setting $\alpha \to \infty$. The upper bounds are plotted for different values of the parameter F of the isotropic state, with respect to the parameterization given in (96), against the number of copies of the isotropic state, and ε is set equal to 0.01.

In figure 6, we plot the upper bounds on the n-shot, one-way distillable key of isotropic states calculated using corollary 3 with $\alpha \to \infty$. In figure 6(a), we plot the upper bounds for two-dimensional isotropic states, and in figure 6(b), we plot the upper bounds for three-dimensional isotropic states, with $\varepsilon = 0.01$ in all the cases.

Remark 5. The techniques used to arrive at corollaries 1 and 2 can be used to find simpler bounds on the one-shot, one-way distillable key of n i.i.d. copies of a state ρ_{AB} by using the α-sandwiched unextendible entanglement. As such, for all $\varepsilon \in (0,1)$, $\alpha \in (1,\infty)$, $n \in \mathbb{N}$, and a state ρ_{AB}, if $\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) > \varepsilon$, then

$$K_D^{\varepsilon,\to}\left(\rho_{AB}^{\otimes n}\right) \leqslant -\log_2\left(\sqrt{\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB})} - \sqrt{\varepsilon}\right), \tag{135}$$

and if $\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) > \sqrt{\varepsilon}$, then

$$K_D^{\varepsilon,\to}\left(\rho_{AB}^{\otimes n}\right) \leqslant -\frac{1}{2}\log_2\left(\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) - \sqrt{\varepsilon}\right). \tag{136}$$

5.3. One-way secret-key distillation in the asymptotic setting

Now let us study the asymptotic setting of one-way secret-key distillation by using the framework of unextendibility.

In the asymptotic setting, we are interested in the maximum rate at which an arbitrarily large number of i.i.d. copies of a state ρ_{AB} can be transformed into a state that is arbitrarily close to an ideal secret key. In this setting, a one-way secret-key distillation protocol is given by a sequence of one-way LOCC channels $\{\mathcal{L}^{n,\to}_{A^nB^n\to A'B'A''B''}\}_{n\in\mathbb{N}}$, a sequence of bipartite private states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$, and a sequence of real numbers $\{\varepsilon_n\}_{n\in\mathbb{N}}$ corresponding to the error in distillation. The joint system A^n refers to n systems, each of which are identical to the system A. The nth element of this sequence acts on n copies of the resource state ρ_{AB} such that the infidelity between the output state and $\gamma^{k_n}_{A'B'A''B''}$ is less than or equal to ε_n. That is,

$$F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{n,\to}_{A^nB^n\to A'B'A''B''}\left(\rho_{AB}^{\otimes n}\right)\right) \geqslant 1-\varepsilon_n \quad \forall n \in \mathbb{N}. \tag{137}$$

To achieve arbitrary precision in distilling secret keys, we demand that $\varepsilon_n \to 0$ as $n \to \infty$. The maximum achievable rate of distilling secret keys is then given by the one-way distillable key of the state, which can be mathematically defined in terms of the one-shot, one-way distillable key as follows [KW24, chapter 15]:

$$K_D^{\to}(\rho_{AB}) := \inf_{\varepsilon\in(0,1]} \liminf_{n\to\infty} \frac{1}{n} K_D^{\varepsilon,\to}\left(\rho_{AB}^{\otimes n}\right). \tag{138}$$

The upper bounds on the one-shot, one-way distillable key, obtained in sections 5.1 and 5.2, do not provide any new insight into the one-way distillable key of the state. This is because, for most states of interest, there exists an $n \in \mathbb{N}$ such that $J^{\varepsilon}_{\min}\left(\rho_{AB}^{\otimes n}\right) \leqslant \varepsilon$ for any $\varepsilon \in (0,1]$, rendering the bound useless.

However, consider a further restricted setting where the sequence $\{\varepsilon_n\}_{n\in\mathbb{N}}$ is required to decrease exponentially fast. The maximum rate of key distillation from an arbitrarily large number of copies of a resource state, for a fixed error exponent a, which we call the a-exponential one-way distillable key of a state, can be mathematically defined in the following manner.

Definition 6. Fix $a > 0$. We define the a-exponential one-way distillable key of a state ρ_{AB} as follows:

$$K^{\to}_{D,a}(\rho_{AB}) := \sup_{\substack{\{k_n\}_{n\in\mathbb{N}}, \left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\mathcal{L}^{n,\to}_{A^nB^n\to A'B'A''B''}\right\}_{n\in\mathbb{N}}}} \liminf_{n\to\infty} \left\{ \frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{\to}\left(\rho_{AB}^{\otimes n}\right)\right) \geqslant 1 - 2^{-an} \right\}, \tag{139}$$

where the supremum is over all sequences of bipartite states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ and all sequences of one-way LOCC channels $\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\}_{n\in\mathbb{N}}$. The bipartite state $\gamma^{k_n}_{A'B'A''B''}$ holds $\log_2 k_n$ secret bits.

We define the converse of a-exponential one-way distillable key of ρ_{AB} as follows:

$$\widetilde{K}^{\rightarrow}_{D,a}(\rho_{AB}) := \sup_{\substack{\{k_n\}_{n\in\mathbb{N}},\{\gamma^{k_n}_{A'B'A''B''}\}_{n\in\mathbb{N}}\\ \{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\}_{n\in\mathbb{N}}}} \limsup_{n\to\infty}\left\{\frac{\log_2 k_n}{n}:\right.$$
$$\left. F\left(\gamma^{k_n}_{A'B'A''B''},\mathcal{L}^{\rightarrow}\left(\rho^{\otimes n}_{AB}\right)\right)\geqslant 1-2^{-an}\right\}. \quad (140)$$

Theorem 3. *Consider an arbitrary bipartite state ρ_{AB}. Let $d := \min\{\dim(A),\dim(B)\}$ with $\dim(A)$ and $\dim(B)$ being the dimensions of systems A and B, respectively. Fix $a\in(2\log_2 d,\infty)$. Then the following bound holds:*

$$\widetilde{K}^{\rightarrow}_{D,a}(\rho_{AB})\leqslant E^u(\rho_{AB}), \quad (141)$$

where $E^u(\rho_{AB})$ is the relative-entropy-induced unextendible entanglement of the state ρ_{AB} (i.e. defined as in (29) with **D** *replaced by the quantum relative entropy D).*

Proof. Let ρ_{AB} be an arbitrary bipartite state from which we wish to distill secret keys, and let $\dim(A)$ and $\dim(B)$ be the dimensions of systems A and B, respectively. Let $\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\}_{n\in\mathbb{N}}$ be a sequence of one-way LOCC channels, and let $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ be a sequence of bipartite private states such that the following condition holds for all $a>2\log_2 d$ and $n\in\mathbb{N}$:

$$F\left(\gamma^{k_n}_{A'B'A''B''},\mathcal{L}^{n,\rightarrow}\left(\rho^{\otimes n}_{AB}\right)\right)\geqslant 1-2^{-an}, \quad (142)$$

where $d := \min\{\dim(A),\dim(B)\}$.

Let us define $\varepsilon_n := 2^{-an}$ for convenience. Let us also define $J^{\varepsilon_n,n}(\rho_{AB}) := 2^{-E^{u,\varepsilon_n}_{\min}(\rho^{\otimes n}_{AB})}$. From proposition 2 we know that $J^{\varepsilon,n}$ is bounded from below as follows:

$$J^{\varepsilon_n,n}(\rho)\geqslant\frac{1-\varepsilon_n}{d^{2n}}. \quad (143)$$

Corollary 1 implies that the following inequality holds for all one-way LOCC channels $\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}$ and all private states $\gamma^{k_n}_{A'B'A''B''}$:

$$\log_2 k_n \leqslant -\log_2\left(\sqrt{J^{\varepsilon_n,n}(\rho)}-\sqrt{\varepsilon_n}\right) \quad (144)$$
$$= -\log_2\left(\sqrt{J^{\varepsilon_n,n}(\rho)}\left(1-\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right)\right) \quad (145)$$
$$= -\frac{1}{2}\log_2(J^{\varepsilon_n,n}(\rho))-\log_2\left(1-\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right). \quad (146)$$

Dividing both sides by n and taking the limit superior as $n\to\infty$ leads to the following inequality:

$$\limsup_{n\to\infty}\frac{\log_2 k_n}{n}$$
$$\leqslant \limsup_{n\to\infty}\left\{-\frac{1}{2n}\log_2 J^{\varepsilon_n,n}(\rho)-\frac{1}{n}\log_2\left(1-\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right)\right\}. \quad (147)$$

Using the lower bound on $J^{\varepsilon_n,n}(\rho)$ from (143), we arrive at the following inequality:

$$\frac{\varepsilon_n}{J^{\varepsilon,n}}\leqslant\varepsilon_n\cdot\frac{d^{2n}}{1-\varepsilon_n} \quad (148)$$
$$\leqslant\frac{2^{-an}d^{2n}}{1-2^{-an}} \quad (149)$$
$$=\frac{d^{2n}}{2^{an}-1} \quad (150)$$
$$=\frac{2^{2n\log_2 d}}{2^{an}-1} \quad (151)$$
$$=\frac{2^{-n(a-2\log_2 d)}}{1-2^{-an}}, \quad (152)$$

where the second inequality follows from the fact that the function $\varepsilon_n/(1-\varepsilon_n)$ increases monotonically with $\varepsilon_n\in[0,1)$ and the fact that $\varepsilon_n\leqslant 2^{-an}$. Thus, for sufficiently large n, since $a>2\log_2 d$ by assumption, it follows that $\frac{2^{-n(a-2\log_2 d)}}{1-2^{-an}}\leqslant 1$ and thus that $\frac{\varepsilon_n}{J^{\varepsilon,n}}\leqslant 1$.

Then we find that

$$\limsup_{n\to\infty}-\log_2\left(1-\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right)$$
$$=-\log_2\left(1-\limsup_{n\to\infty}\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right) \quad (153)$$
$$\leqslant-\log_2\left(1-\limsup_{n\to\infty}\sqrt{\frac{2^{-n(a-2\log_2 d)}}{1-2^{-an}}}\right) \quad (154)$$
$$=-\log_2(1-0)=0. \quad (155)$$

Now let us go back to (147). Substituting (155) in (147) leads to the following inequality:

$$\limsup_{n\to\infty}\frac{\log_2 k_n}{n}\leqslant\limsup_{n\to\infty}-\frac{1}{2n}\log_2 J^{\varepsilon_n,n}(\rho) \quad (156)$$
$$=\limsup_{n\to\infty}\frac{1}{n}E^{u,\varepsilon_n}_{\min}\left(\rho^{\otimes n}_{AB}\right) \quad (157)$$
$$=\limsup_{n\to\infty}\frac{1}{2n}\inf_{\sigma_{A^nB^n}\in\mathcal{F}\left(\rho^{\otimes n}_{AB}\right)}D^{\varepsilon_n}_{\min}\left(\rho^{\otimes n}_{AB}\|\sigma_{A^nB^n}\right), \quad (158)$$

where we have used the definition of $J^{\varepsilon_n,n}(\rho)$ to arrive at the first equality and the definition of $E^{u,\varepsilon}_{\min}$ to arrive at the second

equality. Note that if $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ then $\sigma_{AB}^{\otimes n} \in \mathcal{F}\left(\rho_{AB}^{\otimes n}\right)$. Therefore,

$$\inf_{\sigma_{A^nB^n} \in \mathcal{F}\left(\rho_{AB}^{\otimes n}\right)} D_{\min}^{\varepsilon_n}\left(\rho_{AB}^{\otimes n} \| \sigma_{A^nB^n}\right) \leqslant \inf_{\sigma_{AB} \in \mathcal{F}(\rho_{AB})} D_{\min}^{\varepsilon_n}\left(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}\right). \tag{159}$$

Substituting the above inequality in (158), we arrive at the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leqslant \limsup_{n\to\infty} \frac{1}{2n} \inf_{\sigma_{AB} \in \mathcal{F}(\rho_{AB})} D_{\min}^{\varepsilon_n}\left(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}\right) \tag{160}$$

$$\leqslant \inf_{\sigma_{AB} \in \mathcal{F}(\rho_{AB})} \limsup_{n\to\infty} \frac{1}{2n} D_{\min}^{\varepsilon_n}\left(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}\right), \tag{161}$$

where the second inequality follows from an asymptotic version of the max-min inequality.

Note that $D_{\min}^{\varepsilon}(\rho\|\sigma)$ increases monotonically with increasing ε. Since $\varepsilon_n \leqslant 2^{-an}$, for every $\varepsilon^* \in (0,1)$, there exists an $N \in \mathbb{N}$ such that $\varepsilon_n \leqslant \varepsilon^*$ for all $n \geqslant N$. Consequently,

$$\frac{1}{n} D_{\min}^{\varepsilon_n}\left(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}\right) \leqslant \frac{1}{n} D_{\min}^{\varepsilon^*}\left(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}\right) \qquad \forall n \geqslant N. \tag{162}$$

Substituting the above inequality in (161), we arrive at the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leqslant \inf_{\sigma_{AB} \in \mathcal{F}(\rho_{AB})} \frac{1}{2} \limsup_{n\to\infty} \frac{1}{n} D_{\min}^{\varepsilon^*}\left(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}\right). \tag{163}$$

For all $\varepsilon \in (0,1)$, the following inequality holds [NO00]:

$$\limsup_{n\to\infty} \frac{1}{n} D_{\min}^{\varepsilon}\left(\rho^{\otimes n} \| \sigma^{\otimes n}\right) \leqslant D(\rho\|\sigma), \tag{164}$$

where $D(\cdot\|\cdot)$ is the Umegaki relative entropy [Ume62]. Therefore, we conclude the following:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leqslant \inf_{\sigma_{AB} \in \mathcal{F}(\rho_{AB})} \frac{1}{2} D\left(\rho_{AB} \| \sigma_{AB}\right) = E^u(\rho_{AB}). \tag{165}$$

Since the above inequality holds for all sequences of one-way LOCC channels $\{\mathcal{L}^{n,\to}_{A^nB^n \to A'B'A''B''}\}_{n\in\mathbb{N}}$ and all sequences of private states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ such that $F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{\to}(\rho_{AB}^{\otimes n})\right) \geqslant 1 - 2^{-an}$ for all $a > 2\log_2 d$, we conclude the statement of the theorem. □

Remark 6. The relative-entropy-induced unextendible entanglement of a state can be computed using a semidefinite program. See [KS24] for a semidefinite representation of the relative entropy between two states that can be used directly to estimate the relative-entropy-induced unextendible entanglement of a state to arbitrary precision.

6. Forward-assisted private communication from channels

In this section we extend the results obtained in section 5 to understand the limitations of private communication over channels. We begin with a brief discussion on secret-key distillation from a channel with local operations and forward classical communication in the one-shot setting. In this setting, where forward classical communication can be performed with no cost, the task of secret-key distillation from a channel is equivalent to the task of private communication from the channel.

6.1. One-shot, one-way distillable key of a channel

To distill a secret key from a channel using one-way LOCC, Alice locally prepares a state $\psi_{A'A''\hat{A}}$, and encodes one share of this state using a quantum instrument $\left\{\mathcal{E}^x_{\hat{A}\to A}\right\}_{x\in\mathcal{X}}$. She then sends the system A to Bob through the quantum channel $\mathcal{N}_{A\to B}$ along with the classical label x. Bob then decodes the received state by applying a quantum channel $\mathcal{D}^x_{B\to B'B''}$, which he can choose based on the classical label x that he received from Alice. The state established at the end of the protocol can be mathematically described as follows:

$$\sigma_{A'B'A''B''} := \sum_{x\in\mathcal{X}} \left(\mathcal{D}^x_{B\to B'B''} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}^x_{\hat{A}\to A}\right)\left(\psi_{A'A''\hat{A}}\right). \tag{166}$$

For the secret-key distillation task to be successful in distilling $\log_2 k$ secret bits with an error tolerance ε, we require the following inequality to hold:

$$F\left(\sigma_{A'B'A''B''}, \gamma^k_{A'B'A''B''}\right) \geqslant 1 - \varepsilon \tag{167}$$

for some private state $\gamma^k_{A'B'A''B''}$ holding $\log_2 k$ secret bits. Figure 7 depicts a schematic diagram of the task of one-way secret-key distillation from a channel.

The task of secret-key distillation from a quantum channel can be expressed more concisely using the language of superchannels [CDP08, Gou19]. To distill $\log_2 k$ secret bits from a channel $\mathcal{N}_{A\to B}$ with an error tolerance ε and only using one-way LOCC, Alice and Bob apply a one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{A}\to B'B'')}$ on the channel $\mathcal{N}_{A\to B}$ such that the following inequality holds:

$$F\left(\left(\Theta(\mathcal{N})\right)\left(\psi_{A'A''\hat{A}}\right), \gamma^k_{A'B'A''B''}\right) \geqslant 1 - \varepsilon, \tag{168}$$

for some locally prepared state $\psi_{A'A''\hat{A}}$ and some private state $\gamma^k_{A'B'A''B''}$ holding $\log_2 k$ secret bits. The ability to distill secret keys from a channel in the one-shot setting can then be quantified by the one-shot, one-way distillable key of the channel, which we define below.

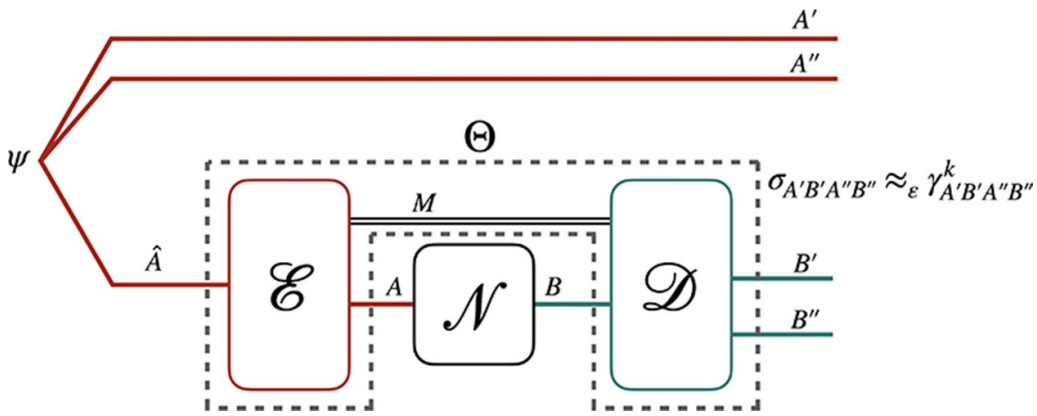


Figure 7. Schematic diagram of secret-key distillation from a channel $\mathcal{N}_{A\to B}$ using a one-way LOCC superchannel Θ. The error in the distillation process, denoted by ε, is given by the infidelity between the state $\sigma_{A'B'A''B''}$ established at the end of the protocol and a private state $\gamma^k_{A'B'A''B''}$ that holds $\log_2 k$ secret bits.

Definition 7. The one-shot, one-way distillable key of a channel $\mathcal{N}_{A\to B}$ is defined as follows:

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) := \sup_{\substack{k\in\mathbb{N},\gamma^k_{A'B'A''B''},\\ \psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A}),\\ \Theta\in 1\text{WL}}} \left\{\log_2 k : F\big((\Theta(\mathcal{N}))(\psi), \gamma^k\big) \geqslant 1-\varepsilon\right\}, \tag{169}$$

where the supremum is over every natural number k, every quantum state $\psi_{A'A''\hat{A}}$, every private state $\gamma^k_{A'B'A''B''}$, and every one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{A}\to B'B'')}$.

The one-shot, one-way distillable key of a channel can be written in terms of the one-shot, one-way distillable key of a state as follows:

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) = \sup_{\substack{\psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A}),\\ \Theta\in 1\text{WL}}} K_D^{\varepsilon,\to}\left(\left(\Theta_{(A\to B)\to(\hat{A}\to B'B'')}(\mathcal{N}_{A\to B})\right)(\psi)\right). \tag{170}$$

Establishing a secret key and using the one-time-pad scheme for private communication is not the only way to transmit private bits over a channel, and there may exist alternate protocols to realize private communication over a quantum channel [DLL03]. The notion of one-shot private capacity of channels is used to quantify the ability of a quantum channel to communicate data privately using local operations without making assumptions on the protocol.

Suppose that Alice wants to send private data to Bob by using a channel $\mathcal{N}_{A\to B}$. To do this, Alice and Bob apply a superchannel $\Theta_{(A\to B)\to(X\to\hat{X})}$ on the channel $\mathcal{N}_{A\to B}$, where X and $\hat{X}$ are classical systems. Let $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ be an isometric extension of the channel $\mathcal{N}_{A\to B}$, where the eavesdropper has access to the system E. The error in private communication through this protocol is defined as follows:

$$p_{\text{err}}(\Theta,\mathcal{N}) := \inf_{\sigma_E}\max_{x\in\mathcal{X}} \left(1 - F\big(|x\rangle\langle x|_{\hat{X}}\otimes\sigma_E, \big(\Theta\big(\mathcal{U}^{\mathcal{N}}_{A\to BE}\big)\big)(|x\rangle\langle x|_X)\big)\right), \tag{171}$$

where the infimum is over all quantum states σ_E and the maximum is over all messages x in the set $\mathcal{X}$. In figure 8, we show a schematic diagram of a protocol for private communication over a channel $\mathcal{N}_{A\to B}$. The one-shot private capacity of a channel $\mathcal{N}_{A\to B}$ is then defined as follows:

$$P^{\varepsilon}(\mathcal{N}_{A\to B}) := \sup_{\mathcal{X},\Theta\in\text{LO}} \{\log_2|\mathcal{X}| : p_{\text{err}}(\Theta,\mathcal{N}) \leqslant \varepsilon\}, \tag{172}$$

where LO refers to the set of all superchannels that can be realized by local operations only and $|\mathcal{X}|$ refers to the number of elements in the set $\mathcal{X}$. As such, the supremum is over all sets of messages $\mathcal{X}$ and all superchannels $\Theta_{(A\to B)\to(X\to\hat{X})}$ that can be realized by only local operations.

In the one-way LOCC setting considered throughout this work, Alice is allowed to send arbitrary amounts of classical data to Bob, which is publicly available to any eavesdropper as well. In this setting, the quantity of interest is the one-shot forward-assisted private capacity of a channel, which is defined as follows:

$$P^{\varepsilon,\to}(\mathcal{N}_{A\to B}) := \sup_{\mathcal{X},\Theta\in 1\text{WL}} \{\log_2|\mathcal{X}| : p_{\text{err}}(\Theta,\mathcal{N}) \leqslant \varepsilon\}, \tag{173}$$

where 1WL refers to the set of all one-way LOCC superchannels. Since LO $\subseteq$ 1WL, the following inequality holds for all quantum channels $\mathcal{N}_{A\to B}$:

$$P^{\varepsilon,\to}(\mathcal{N}_{A\to B}) \geqslant P^{\varepsilon}(\mathcal{N}_{A\to B}). \tag{174}$$

In the remainder of this paper, we will derive several upper bounds on the one-shot forward-assisted private capacity of channels, which, as a consequence of (174), also serve as upper bounds on the one-shot private capacity of the channel due to the inequality mentioned above.

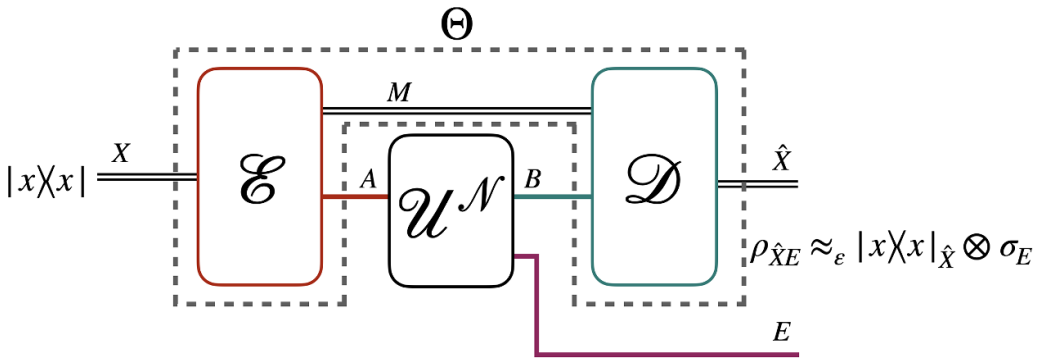


Figure 8. Schematic diagram of private communication over a channel $\mathcal{N}_{A\to B}$, with an isometric extension $\mathcal{U}^{\mathcal{N}}_{A\to BE}$, using a one-way LOCC superchannel Θ. The objective of this protocol is to send an arbitrary classical label x from Alice to Bob such that the state of an eavesdropper, who holds the system E, is independent of the state Bob receives. The error in private communication, denoted by ε, is defined in (171).

In the presence of forward-classical assistance, the task of secret-key distillation is equivalent to the task of private communication. Suppose that a forward-assisted protocol allows Alice to send n private bits to Bob through a channel $\mathcal{N}_{A\to B}$ with some error ε. Alice can send a secret key itself through this channel, hence, transforming the one-shot private communication protocol to a one-shot secret-key distillation protocol. Moreover, in the forward-classical assistance setting, a secret-key distillation protocol can be transformed into a private communication protocol by using the one-time-pad scheme, thus demonstrating the equivalence between the two tasks.

Due to the equivalence between the tasks of private communication and secret-key distillation in the presence of forward-classical assistance, the one-shot forward-assisted private capacity of a channel $P^{\varepsilon,\to}(\mathcal{N}_{A\to B})$ is equal to the one-shot, one-way distillable key of the channel. That is,

$$P^{\varepsilon,\to}(\mathcal{N}_{A\to B}) = K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}). \tag{175}$$

The techniques used in section 5 for obtaining upper bounds on the one-shot, one-way distillable key of a state can be extended to obtain upper bounds on the one-shot, one-way distillable key of a channel, using the unextendible entanglement of channels. Furthermore, the equality in (175) allows us to obtain upper bounds on the one-shot forward-assisted private capacity, which are also upper bounds on the one-shot private capacity by definition.

6.2. Unextendible entanglement of channels

The generalized unextendible entanglement of channels was defined in [SW24b]. We briefly present the relevant properties of the quantity here.

Let us define the following set of channels with respect to a given channel $\mathcal{N}_{A\to B}$:

$$\mathcal{F}(\mathcal{N}_{A\to B}) := \{\mathrm{Tr}_B \circ \mathcal{P}_{A\to BE} : \mathrm{Tr}_E \circ \mathcal{P}_{A\to BE} = \mathcal{N}_{A\to B}\}, \tag{176}$$

where systems B and E are isomorphic. The generalized unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ is defined with respect to a generalized channel divergence $\mathbf{D}$ [CMW16, LKDW18] as follows:

$$\mathbf{E}^u(\mathcal{N}_{A\to B}) := \frac{1}{2} \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \mathbf{D}(\mathcal{N}_{A\to B} \| \mathcal{M}_{A\to E}), \tag{177}$$

where the generalized divergence between channels is defined as

$$\mathbf{D}(\mathcal{N}_{A\to B} \| \mathcal{M}_{A\to B}) = \sup_{\rho_{RA}\in\mathcal{S}(RA)} \mathbf{D}(\mathcal{N}_{A\to B}(\rho_{RA}) \| \mathcal{M}_{A\to B}(\rho_{RA})). \tag{178}$$

The generalized unextendible entanglement of a channel does not increase under the action of one-way LOCC superchannels, the latter defined in section 2.2.

Lemma 4 ([SW24b]). *The generalized unextendible entanglement of a channel does not increase under the action of one-way LOCC superchannels. That is,*

$$\mathbf{E}^u(\Theta(\mathcal{N}_{A\to B})) \leqslant \mathbf{E}^u(\mathcal{N}_{A\to B}) \qquad \forall \Theta \in \mathrm{1WL}, \tag{179}$$

where 1WL *represents the set of all one-way LOCC superchannels.*

A more general statement of lemma 4 was presented in [SW24b], where it was shown that the generalized unextendible entanglement of a channel does not increase under the action of two-extendible superchannels, which is a semidefinite relaxation of the set of one-way LOCC superchannels, and hence, contains the set of one-way LOCC superchannels. In this work we will only consider one-way LOCC superchannels and not two-extendible superchannels. We point the interested reader to [SW24b] for a more detailed discussion.

A direct consequence of lemma 4 is that the maximum value of the generalized unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ is not larger than the generalized unextendible entanglement of the identity channel $\mathrm{id}_{A'\to B'}$, where $\dim(A') = \dim(B') = \min\{\dim(A), \dim(B)\}$. This can be seen from the following argument: Consider an arbitrary channel $\mathcal{N}_{A\to B}$. If $\dim(A) \geqslant \dim(B)$, then construct a superchannel $\Theta_{(B\to C)\to(A\to D)}$ that acts on an arbitrary channel $\mathcal{M}_{B\to C}$ as follows:

$$\Theta_{(B\to C)\to(A\to D)}(\mathcal{M}_{B\to C}) = \mathrm{id}_{C\to D} \circ \mathcal{M}_{B\to C} \circ \mathcal{N}_{A\to B}. \tag{180}$$

Lemma 4 implies the following inequality:

$$\begin{aligned}\mathbf{E}^u(\mathrm{id}_{B\to C}) &\geqslant \mathbf{E}^u(\Theta(\mathrm{id}_{B\to C})) && (181)\\ &= \mathbf{E}^u(\mathrm{id}_{C\to D}\circ \mathrm{id}_{B\to C}\circ \mathcal{N}_{A\to B}) && (182)\\ &= \mathbf{E}^u(\mathcal{N}_{A\to B})\,. && (183)\end{aligned}$$

Similarly, if $\dim(B)\geqslant\dim(A)$, then we can construct a superchannel $\Upsilon_{(D\to A)\to(C\to B)}$ that acts on an arbitrary channel $\mathcal{M}_{D\to A}$ as follows:

$$\Upsilon_{(D\to A)\to(C\to B)}(\mathcal{M}_{D\to A}) = \mathcal{N}_{A\to B}\circ\mathcal{M}_{D\to A}\circ\mathrm{id}_{C\to D}\,. \tag{184}$$

Once again, applying lemma 4 leads to the following inequality:

$$\mathbf{E}^u(\mathrm{id}_{D\to A}) \geqslant \mathbf{E}^u(\Upsilon(\mathrm{id}_{D\to A})) = \mathbf{E}^u(\mathcal{N}_{A\to B})\,. \tag{185}$$

The inequalities in (183) and (185) can be written together as the following inequality:

$$\mathbf{E}^u(\mathcal{N}_{A\to B}) \leqslant \min\{\mathbf{E}^u(\mathrm{id}_{A\to C}), \mathbf{E}^u(\mathrm{id}_{B\to D})\}\,, \tag{186}$$

where $\dim(A)=\dim(C)$ and $\dim(B)=\dim(D)$.

Another important property of generalized unextendible entanglement of channels, which is relevant to our discussion, is its relation with the generalized unextendible entanglement of states. In particular, the generalized unextendible entanglement of a bipartite state that can be established between two distant parties using a quantum channel $\mathcal{N}_{A\to B}$ and one-way LOCC superchannels cannot be larger than the generalized unextendible entanglement of the channel $\mathcal{N}_{A\to B}$. We state this formally in lemma 5 below.

Lemma 5 ([SW24b]). *The unextendible entanglement of a quantum state $\sigma_{RC'D}$, with respect to the partition $RC':D$, that can be established between two parties using a point-to-point quantum channel $\mathcal{N}_{A\to B}$ and a one-way LOCC superchannel $\Theta_{(A\to B)\to(C\to C'D)}$ is no greater than the unextendible entanglement of the quantum channel $\mathcal{N}_{A\to B}$; i.e.*

$$\sup_{\rho_{RC}} \mathbf{E}^u(\sigma_{RC':D}) \leqslant \mathbf{E}^u(\mathcal{N}_{A\to B})\,, \tag{187}$$

where

$$\sigma_{RC'D} := \left(\Theta_{(A\to B)\to(C\to C'D)}(\mathcal{N}_{A\to B})\right)(\rho_{RC})\,, \tag{188}$$

and ρ_{RC} is a quantum state. The symbol $\mathbf{E}^u(\sigma_{RC':D})$ denotes that the unextendible entanglement of the state $\sigma_{RC'D}$ is calculated with respect to the bipartition $RC':D$.

Lemmas 5, 3, and (170) provide us with all the necessary tools to obtain an upper bound on the one-shot, one-way distillable key of a channel using unextendible entanglement of channels.

The two important quantities that we will use in this section are the smooth-min unextendible entanglement of a channel and the α-geometric unextendible entanglement of the channel.

The smooth-min unextendible entanglement of a channel is defined in terms of the smooth-min relative entropy of channels as follows:

$$\begin{aligned}&E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B})\\ &:= \frac{1}{2}\inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} D^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to E}) && (189)\\ &= \frac{1}{2}\inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})}\sup_{\rho_{RA}\in\mathcal{S}(RA)} D^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}(\rho_{RA})\,\|\mathcal{M}_{A\to E}(\rho_{RA}))\,, && (190)\end{aligned}$$

where the smooth-min relative entropy of states was defined in (39). The smooth-min relative entropy of channels can be written as a semidefinite program [WW19b, appendix B-3], and the set $\mathcal{F}(\mathcal{N})$ can also be described by semidefinite constraints. This allows us to write the smooth-min unextendible entanglement of a channel as a semidefinite program (see appendix H).

Proposition 6. *The smooth-min unextendible entanglement of a channel is bounded as follows:*

$$-\frac{1}{2}\log_2(1-\varepsilon) \leqslant E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \leqslant \log_2 d - \frac{1}{2}\log_2(1-\varepsilon)\,, \tag{191}$$

where $d := \min\{\dim(A),\dim(B)\}$.

Proof. See appendix F. □

The α-geometric unextendible entanglement of channels was explored in [SW24b] in the context of zero-error private communication. It is defined for a parameter $\alpha\in(0,1)\cup(1,2]$ as follows:

$$\widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) := \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})}\frac{1}{2}\widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) \tag{192}$$

$$= \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})}\sup_{\rho_{RA}\in\mathcal{S}(RA)}\frac{1}{2}\widehat{D}_\alpha(\mathcal{N}_{A\to B}(\rho_{RA})\,\|\mathcal{M}_{A\to B}(\rho_{RA}))\,, \tag{193}$$

where the α-geometric Rényi relative entropy of states is defined for all $\alpha\in(0,1)\cup(1,\infty)$ as follows [Mat13]:

$$\widehat{D}_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log_2\mathrm{Tr}\left[\sigma\left(\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}\right)^\alpha\right]. \tag{194}$$

We list some properties of the α-geometric unextendible entanglement of channels that are relevant to this work. We refer the interested reader to [SW24b] for a more detailed discussion of these properties:

1. **Monotonicity in α:** The α-geometric unextendible entanglement of channels increases monotonically with increasing α. That is,
$$\widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \geqslant \widehat{E}^u_\beta(\mathcal{N}_{A\to B}) \quad \forall\alpha,\beta\in(0,1)\cup(1,2], \quad \alpha\geqslant\beta. \tag{195}$$

2. **Subadditivity:** The α-geometric unextendible entanglement of channels is subadditive under tensor products of

channels. That is, the following inequality holds for all $\alpha \in (0,1)\cup(1,2]$:

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}\otimes\mathcal{M}_{A\to B}) \leqslant \widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) + \widehat{E}^{u}_{\alpha}(\mathcal{M}_{A\to B}), \tag{196}$$

where $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A\to B}$ are quantum channels.

3. **Limiting case when $\alpha\to 1$:** The α-geometric unextendible entanglement converges to the unextendible entanglement induced by the Belavkin–Staszewski relative entropy as $\alpha\to 1$. That is,

$$\widehat{E}^{u}(\mathcal{N}_{A\to B}) := \lim_{\alpha\to 1}\widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) = \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})}\frac{1}{2}\widehat{D}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}), \tag{197}$$

where the Belavkin–Staszewski relative entropy of states is defined as follows [BS82]:

$$\widehat{D}(\rho\|\sigma) := \begin{cases} \operatorname{Tr}\left[\rho\log_2\left(\sqrt{\rho}\sigma^{-1}\sqrt{\rho}\right)\right] & \text{if } \operatorname{supp}(\rho)\subseteq\operatorname{supp}(\sigma) \\ +\infty & \text{otherwise,}\end{cases} \tag{198}$$

and where σ^{-1} is taken on the support of σ and the logarithm is evaluated on the support of ρ. The rightmost equality in (197) follows directly from [DKQ+23, proposition 36].

4. **Semidefinite program:** The α-geometric unextendible entanglement of a channel can be computed using a semidefinite program for rational values of $\alpha\in(1,2]$ (see appendix H).

The α-geometric unextendible entanglement of a channel can be related with the smooth-min unextendible entanglement using the inequality in (123). The α-geometric Rényi relative entropy of states is known to be larger than or equal to the α-sandwiched Rényi relative entropy of states for all $\alpha\in(0,1)\cup(1,\infty)$ [Tom15, WWW24]. The inequality in (123) then implies the following inequality, which holds for all $\alpha\in(1,\infty)$ and $\varepsilon\in[0,1)$:

$$D^{\varepsilon}_{\min}(\rho\|\sigma) \leqslant \widetilde{D}_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right) \tag{199}$$

$$\leqslant \widehat{D}_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{200}$$

We will restrict our discussion to $\alpha\in(1,2]$, as this is the interval for which the α-geometric Rényi relative entropy obeys the data-processing inequality. Setting $\rho\to(\mathrm{id}_R\otimes\mathcal{N})(\rho_{RA})$ and $\sigma\to(\mathrm{id}_R\otimes\mathcal{M})(\rho_{RA})$, where $\mathcal{N}$ and $\mathcal{M}$ are quantum channels, leads to the following inequality:

$$\begin{aligned} &D^{\varepsilon}_{\min}\left(\left(\mathrm{id}_R\otimes\mathcal{N}\right)(\rho_{RA})\,\|\,\left(\mathrm{id}_R\otimes\mathcal{M}\right)(\rho_{RA})\right) \\ &\leqslant \widehat{D}_{\alpha}\left(\left(\mathrm{id}_R\otimes\mathcal{N}\right)(\rho_{RA})\,\|\,\left(\mathrm{id}_R\otimes\mathcal{M}\right)(\rho_{RA})\right) \\ &\quad + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \end{aligned} \tag{201}$$

Since the above inequality holds for every state ρ, we can take a supremum over all states and conclude the following inequality:

$$D^{\varepsilon}_{\min}(\mathcal{N}\|\mathcal{M}) \leqslant \widehat{D}_{\alpha}(\mathcal{N}\|\mathcal{M}) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{202}$$

Now taking an infimum over all $\mathcal{M}\in\mathcal{F}(\mathcal{N})$, we arrive at the following inequality, which holds for all $\alpha\in(1,2]$ and $\varepsilon\in[0,1)$:

$$\begin{aligned} &E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \\ &= \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})}\frac{1}{2}D^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) && (203)\\ &\leqslant \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})}\frac{1}{2}\widehat{D}_{\alpha}(\mathcal{N}\|\mathcal{M}) + \frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right) && (204)\\ &= \widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) + \frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). && (205) \end{aligned}$$

6.3. Upper bounds on the one-shot private capacity of a channel

In this section, we discuss the application of the smooth-min unextendible entanglement and the max-unextendible entanglement of channels to obtaining upper bounds on the one-shot, one-way distillable key of a channel.

6.3.1. Smooth-min unextendible entanglement upper bound.

Consider the following quantity:

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) := 2^{-2E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B})}. \tag{206}$$

Lemma 5 implies the following inequality:

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \leqslant \sup_{\substack{\rho_{A'A''\hat{A}}\in\mathcal{S}\left(A'A''\hat{A}\right),\\ \Theta\in\mathrm{1WL}}} J^{\varepsilon}_{\min}((\Theta(\mathcal{N}_{A\to B}))(\rho)), \tag{207}$$

where $J^{\varepsilon}_{\min}(\cdot)$ for states was defined in (40). The supremum in the above inequality is over every state $\rho_{A'A''\hat{A}}$ and one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{A}\to B'B'')}$. The inequality in (207), along with theorem 2 and lemma 3, yields an upper bound on the one-shot forward-assisted private capacity of a channel, which we state in theorem 4 below.

Theorem 4 (unextendibility bound on one-shot private capacity). *Consider a quantum channel $\mathcal{N}_{A\to B}$ and a parameter $\varepsilon\in[0,1]$ such that*

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) > \varepsilon, \tag{208}$$

where $J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})$ is defined in (206). Then the one-shot, one-way distillable key of the channel, which is equal to the one-shot private capacity of the channel according to (175), is

bounded from above by the following quantity:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) = K_D^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(\mathcal{N})\left(1-J^{\varepsilon}_{\min}(\mathcal{N})\right)}+\sqrt{\varepsilon\left(1-\varepsilon\right)}}{J^{\varepsilon}_{\min}(\mathcal{N})-\varepsilon}\right)^2+1\right]. \tag{209}$$

Proof. Let $\mathcal{N}_{A\to B}$ be a quantum channel, and let $\varepsilon \in [0,1]$ be a parameter such that

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) > \varepsilon. \tag{210}$$

Using the equality relating the one-shot, one-way distillable key of a channel and the one-shot, one-way distillable key of a state from (170), we arrive at the following:

$$K_D^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) = \sup_{\Theta\in 1\text{WL},\,\psi_{A'A''\hat{A}}\in\mathcal{S}\left(A'A''\hat{A}\right)} K_D^{\varepsilon,\rightarrow}\left(\Theta(\mathcal{N}_{A\to B})\left(\psi_{A'A''\hat{A}}\right)\right) \tag{211}$$

$$\leqslant \sup_{\substack{\psi_{A'A''\hat{A}}\in\mathcal{S}\left(A'A''\hat{A}\right),\\ \Theta\in 1\text{WL}}} \left\{ \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}\left(1-J^{\varepsilon}_{\min}\right)}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2+1\right] : J^{\varepsilon}_{\min} = J^{\varepsilon}_{\min}\left(\left(\Theta(\mathcal{N})\right)\left(\psi_{A'A''\hat{A}}\right)\right) \right\}, \tag{212}$$

where $J^{\varepsilon}_{\min}(\cdot)$ for states is defined in (40). The inequality in (212) follows from theorem 2. Note that the above inequality holds only if $J^{\varepsilon}_{\min} > \varepsilon$, but since we have assumed that $J^{\varepsilon}_{\min}(\mathcal{N}) > \varepsilon$, the quantity $J^{\varepsilon}_{\min}$ is guaranteed to be strictly greater than ε due to (207).

Let us define

$$J^{\varepsilon,s}_{\min}(\mathcal{N}_{A\to B}) := \sup_{\substack{\psi_{A'A''\hat{A}}\in\mathcal{S}\left(A'A''\hat{A}\right),\\ \Theta\in 1\text{WL}}} J^{\varepsilon}_{\min}\left(\left(\Theta(\mathcal{N})\right)\left(\psi_{A'A''\hat{A}}\right)\right). \tag{213}$$

Then the inequality in (212) can be written as follows:

$$K_D^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon,s}_{\min}(\mathcal{N})\left(1-J^{\varepsilon,s}_{\min}(\mathcal{N})\right)}+\sqrt{\varepsilon\left(1-\varepsilon\right)}}{J^{\varepsilon,s}_{\min}(\mathcal{N})-\varepsilon}\right)^2+1\right]. \tag{214}$$

The inequality in (207) states that $J^{\varepsilon}_{\min}(\mathcal{N}) \leqslant J^{\varepsilon,s}_{\min}(\mathcal{N})$. Therefore, by applying lemma 3, we arrive at the following inequality:

$$K_D^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(\mathcal{N})\left(1-J^{\varepsilon}_{\min}(\mathcal{N})\right)}+\sqrt{\varepsilon\left(1-\varepsilon\right)}}{J^{\varepsilon}_{\min}(\mathcal{N})-\varepsilon}\right)^2+1\right]. \tag{215}$$

Finally, using the fact that the one-shot forward-assisted private capacity of a channel is equal to the one-shot one-way distillable key of the channel, we conclude the statement of the theorem. □

In figure 9, we plot the upper bounds on the one-shot forward-assisted private capacity of a two-dimensional and a three-dimensional erasure channel for different erasure probabilities and different values of ε. The erasure channel is mathematically defined as follows:

$$\mathcal{E}^{p}_{A\to B}(\rho_{RA}) = (1-p)\,\rho_{RB} + p\,\mathrm{Tr}_A[\rho_{RA}]\otimes|e\rangle\langle e|_B, \tag{216}$$

where $|e\rangle_B$ is the erasure symbol, which is orthogonal to every state in the span of $\{|i\rangle\langle j|\}_{i,j=0}^{d-1}$, and d is the dimension of the system A. The parameter $p \in [0,1]$ is the erasure probability of the channel.

The simplified upper bounds obtained in corollaries 1 and 2 can be used to obtain simplified upper bounds on the one-shot forward-assisted private capacity of a channel. The inequality in (207), the equality in (170), and the application of lemma 3 together lead to simplified upper bounds on the one-shot forward-assisted private capacity of a channel, stated in the corollary below.

Corollary 4. *Fix $\varepsilon \in [0,1]$. Let $\mathcal{N}_{A\to B}$ be a channel such that the following inequality holds:*

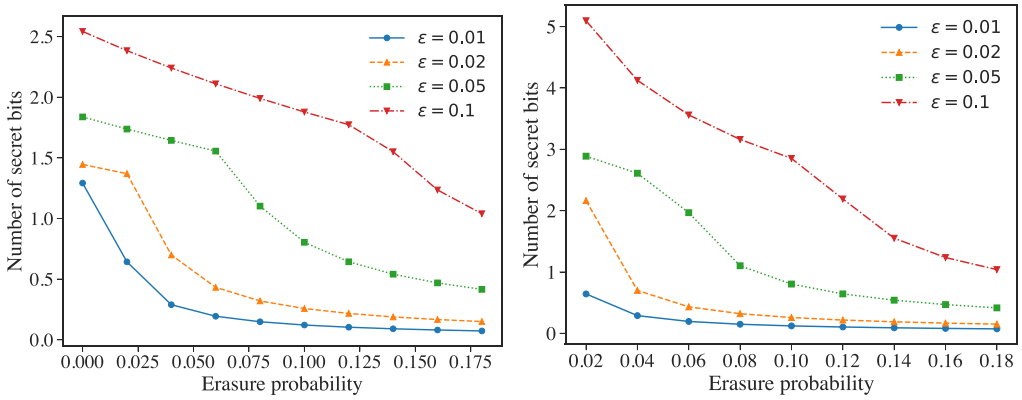
$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) > \varepsilon, \tag{217}$$

where $J^{\varepsilon}_{\min}(\mathcal{N})$ is defined in (206). Then the one-shot forward-assisted private capacity of a channel is bounded from above as follows:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leqslant -\log_2\left(\sqrt{J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})}-\sqrt{\varepsilon}\right). \tag{218}$$

If $J^{\varepsilon}_{\min}(\mathcal{N}) > \sqrt{\varepsilon}$ then the following inequality also holds:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leqslant -\frac{1}{2}\log_2\left(J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})-\sqrt{\varepsilon}\right). \tag{219}$$



(a) Two-dimensional erasure channel (b) Three-dimensional erasure channel

Figure 9. Upper bound on the number of private bits that can be transmitted over a single use of an erasure channel assisted by local operations and forward-classical communication. The upper bound given in theorem 4 is plotted against the erasure probability of an erasure channel for different values of ε.

6.3.2. α-geometric unextendible entanglement upper bound. The subadditivity of the α-geometric unextendible entanglement of channels, as given in (196), can be used to obtain an upper bound on the n-shot, forward-assisted private capacity of a channel.

Consider an arbitrary quantum channel $\mathcal{N}_{A\to B}$. Recall the definition of $J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})$ from (206). The inequality in (205) implies that the following inequality holds for all $\alpha \in (1,2]$ and $\varepsilon \in [0,1)$:

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \geqslant 2^{-2\widehat{E}^{u}_{\alpha}(\mathcal{N}) - \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right)} \tag{220}$$

$$= (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2\widehat{E}^{u}_{\alpha}(\mathcal{N})}. \tag{221}$$

Now consider the following quantity:

$$J^{\varepsilon}_{\min}\left(\mathcal{N}^{\otimes n}_{A\to B}\right) \geqslant (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2\widehat{E}^{u}_{\alpha}\left(\mathcal{N}^{\otimes n}\right)} \tag{222}$$

$$\geqslant (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2n\widehat{E}^{u}_{\alpha}(\mathcal{N})}, \tag{223}$$

where the second inequality follows from the subadditivity of the α-geometric unextendible entanglement of channels (see (196)).

Let us define the following quantity:

$$\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B}) := (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2n\widehat{E}^{u}_{\alpha}(\mathcal{N})}, \tag{224}$$

which, according to (223), is a lower bound on $J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})$. If α is a rational number in the interval $(1,2]$, then $\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B})$ can be computed using a semidefinite program, by employing the algorithms given in [FS17] (see appendix H for a special case). The application of lemma 3 to theorem 4, along with the inequality in (223), directly leads to a single-letter, semidefinite computable upper bound on the n-shot forward-assisted private capacity of a channel, which we state formally in corollary 5 below.

Corollary 5. *Fix $\varepsilon \in (0,1)$. Let $\mathcal{N}_{A\to B}$ be a quantum channel such that the following inequality holds for some $\alpha \in (1,2]$:*

$$\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B}) > \varepsilon \tag{225}$$

where $\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B})$ is defined in (224). Then the n-shot forward-assisted private capacity of a channel $\mathcal{N}_{A\to B}$ is bounded from above by the following quantity:

$$P^{\varepsilon,\to}\left(\mathcal{N}^{\otimes n}_{A\to B}\right) \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B})\left(1-\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B})\right)} + \sqrt{\varepsilon(1-\varepsilon)}}{\widehat{J}^{\varepsilon,n}_{\alpha}(\mathcal{N}_{A\to B}) - \varepsilon}\right)^2 + 1\right]. \tag{226}$$

We turn to the erasure channel once again to demonstrate our results stated in corollary 5. An erasure channel with erasure probability greater than or equal to $\frac{1}{2}$ (see (216)) is a two-extendible channel, and hence, its α-geometric unextendible entanglement is equal to zero for all $\alpha \in (0,1)\cup(1,2]$. If the erasure probability is less than $\frac{1}{2}$, then the explicit form of the α-geometric unextendible entanglement can be derived, which we state in proposition 7 below.

Proposition 7. *For all $\alpha \in (0,1)\cup(1,2]$, the α-geometric unextendible entanglement of a d-dimensional erasure channel, with erasure probability p, evaluates to the following:*

$$\widehat{E}^{u}_{\alpha}(\mathcal{E}^{p}_{A\to B}) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(\left(p+\frac{b_{\text{opt}}}{d^2}\right)^{1-\alpha}(1-p)^{\alpha} + (1-p-b_{\text{opt}})^{1-\alpha}p^{\alpha}\right) \tag{227}$$

for all $p \in \left(0, \frac{1}{d^{1/\alpha}+1}\right]$, where

$$b_{\text{opt}} := \frac{d^2\left((1-p)^2 - p^2 d^{2/\alpha}\right)}{pd^{2/\alpha} + (1-p)d^2}. \tag{228}$$

For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}^{u}_{\alpha}(\mathcal{E}^{p}_{A\to B}) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(p^{1-\alpha}(1-p)^{\alpha} + (1-p)^{1-\alpha}p^{\alpha}\right). \tag{229}$$

Proof. See appendix G. □

In figure 10, we plot the upper bound on the n-shot, forward-assisted private capacity of erasure channels computed using corollary 5. The α-geometric unextendible entanglement of the erasure channel is computed using proposition 7. The n-shot, forward-assisted private capacity of a channel is expected to increase with the number of channel uses. In figure 10, however, the computed value of the upper bound on the n-shot forward-assisted private capacity decreases with the number of channel uses, which indicates that the upper bound improves with an increasing number of channel uses.

6.3.3. Private communication over a channel in the asymptotic setting. In this section we study private communication over quantum channels using one-way LOCC superchannels in the asymptotic setting.

First, let us consider the task of secret-key distillation from quantum channels in a setting similar to the one discussed in section 5.3. In the asymptotic setting, a one-way LOCC protocol to distill secret keys from a channel $\mathcal{N}_{A\to B}$ is described by a sequence of positive integers $\{k_n\}_{n\in\mathbb{N}}$, a sequence of bipartite private states $\left\{\gamma^{k_n}_{A'A''B'B''}\right\}_{n\in\mathbb{N}}$, a sequence of one-way LOCC superchannels $\left\{\Theta^{n,1\text{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}\right\}_{n\in\mathbb{N}}$, a sequence of states $\left\{\rho^{n}_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}$, and a sequence of error parameters $\{\varepsilon_n\}_{n\in\mathbb{N}}$. A sequence of tuples, $\left\{\left(k_n, \gamma^{k_n}_{A'A''B'B''}, \Theta^{n,1\text{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}, \rho^{n}_{A'A''\hat{A}}, \varepsilon_n\right)\right\}_{n\in\mathbb{N}}$, describes a one-way LOCC secret-key distillation protocol for a channel $\mathcal{N}_{A\to B}$ if the following inequality holds for all $n\in\mathbb{N}$:

$$F\left(\gamma^{k_n}, \left(\Theta^{n,1\text{WL}}\left(\mathcal{N}^{\otimes n}\right)\right)(\rho^n)\right) \geqslant 1-\varepsilon_n, \tag{230}$$

and $\varepsilon_n \to 0$ as $n\to\infty$. We are interested in the maximum rate at which secret bits can be distilled from a channel $\mathcal{N}_{A\to B}$ using any such one-way LOCC secret-key distillation protocol.

Similar to the discussion in section 5.3, we impose an additional constraint on the sequence of error parameters ε_n, that $\varepsilon_n \leqslant 2^{-an}$ for some fixed error exponent $a>0$. We define the quantity 'a-exponential one-way distillable key of a channel' as the maximum rate at which secret bits can be distilled from a channel using a one-way LOCC secret-key distillation protocol, with a being the error exponent.

Definition 8. Fix $a>0$. The a-exponential one-way distillable key of a channel $\mathcal{N}_{A\to B}$ is defined as follows:

$$K^{\rightarrow}_{D,a}(\mathcal{N}_{A\to B}) := \sup_{\substack{\{k_n\}_{n\in\mathbb{N}}, \left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\Theta^{n,1\text{WL}}\right\}_{n\in\mathbb{N}}, \left\{\rho^{n}_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}}} \liminf_{n\to\infty}\left\{\frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}, \Theta^{n,1\text{WL}}\left(\mathcal{N}^{\otimes n}\right)(\rho^n)\right) \geqslant 1-2^{-an}\right\}, \tag{231}$$

where the supremum is over all sequences of integers $\{k_n\}_{n\in\mathbb{N}}$, all sequences of bipartite states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$, all sequences of one-way LOCC superchannels $\left\{\Theta^{n,1\text{WL}}_{(A^n\to B^n)\to A'B'A''B''}\right\}_{n\in\mathbb{N}}$, and all sequences of states $\left\{\rho_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}$. The bipartite state $\gamma^{k_n}_{A'B'A''B''}$ holds $\log_2 k_n$ secret bits.

We define the converse of a-exponential one-way distillable key of the channel $\mathcal{N}_{A\to B}$ as follows:

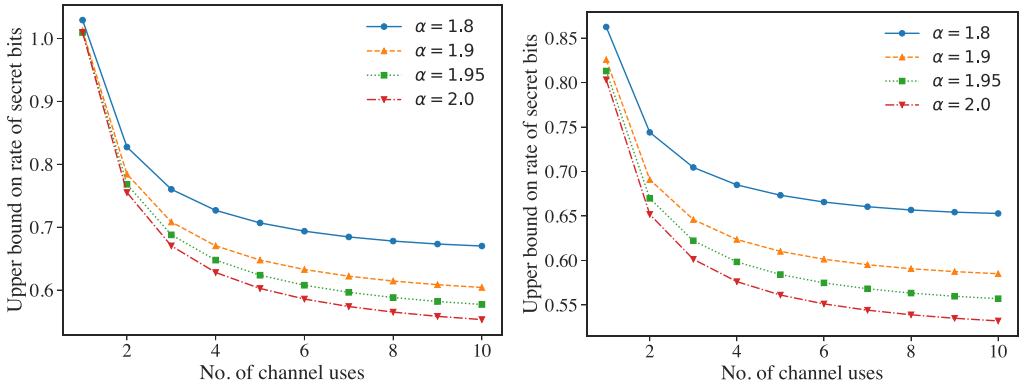
$$\widetilde{K}^{\rightarrow}_{D,a}(\mathcal{N}_{A\to B}) := \sup_{\substack{\{k_n\}_{n\in\mathbb{N}}, \left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\Theta^{n,1\text{WL}}\right\}_{n\in\mathbb{N}}, \left\{\rho^{n}_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}}} \limsup_{n\to\infty}\left\{\frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}, \Theta^{n,1\text{WL}}\left(\mathcal{N}^{\otimes n}\right)(\rho^n)\right) \geqslant 1-2^{-an}\right\}. \tag{232}$$

We can also consider the task of private communication over channels in this setting. We define the a-exponential forward-assisted private capacity of a channel as follows:

Definition 9. Fix $a>0$. The a-exponential forward-assisted private capacity of a channel $\mathcal{N}_{A\to B}$ is defined as follows:

$$P^{\rightarrow}_{a}(\mathcal{N}_{A\to B}) := \sup_{\{\mathcal{X}_n\}_{n\in\mathbb{N}}, \left\{\Theta^{n,1\text{WL}}\right\}_{n\in\mathbb{N}}} \liminf_{n\to\infty}\left\{\frac{\log_2|\mathcal{X}_n|}{n} : p_{\text{err}}\left(\mathcal{N}^{\otimes n}, \Theta^{n,1\text{WL}}\right) \leqslant 2^{-an}\right\}, \tag{233}$$

where the supremum is over all sequences of message sets $\{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and all sequences of one-way LOCC superchannels $\left\{\Theta^{n,1\text{WL}}_{(A^n\to B^n)\to(X\to\hat{X})}\right\}_{n\in\mathbb{N}}$.



(a) Erasure probability = 0.2 (b) Erasure probability = 0.3

Figure 10. Upper bound on the n-shot private capacity of an erasure channel with the error parameter $\varepsilon = 10^{-7}$. The bounds are computed for different values of α using corollary 5, where the α-geometric unextendible entanglement of the erasure channel is computed using proposition 7.

We define the converse of a-exponential forward-assisted private capacity of the channel $\mathcal{N}_{A\to B}$ as follows:

$$\widetilde{P}_a^{\rightarrow}(\mathcal{N}_{A\to B}) := \sup_{\{\mathcal{X}_n\}_{n\in\mathbb{N}},\left\{\Theta^{n,1\mathrm{WL}}\right\}_{n\in\mathbb{N}}} \limsup_{n\to\infty} \left\{ \frac{\log_2|\mathcal{X}_n|}{n} : p_{\mathrm{err}}\left(\mathcal{N}^{\otimes n}, \Theta^{n,1\mathrm{WL}}\right) \leqslant 2^{-an} \right\}. \quad (234)$$

Using the arguments mentioned before (175), we can see that the following equalities hold:

$$K_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B}) = P_a^{\rightarrow}(\mathcal{N}_{A\to B}) \quad (235)$$

$$\widetilde{K}_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B}) = \widetilde{P}_a^{\rightarrow}(\mathcal{N}_{A\to B}). \quad (236)$$

Therefore, any bounds obtained on the a-exponential distillable key of a channel hold for the a-exponential private capacity of the channel as well.

Theorem 5. *Consider an arbitrary quantum channel $\mathcal{N}_{A\to B}$. Let $d := \min\{\dim(A), \dim(B)\}$ with $\dim(A)$ and $\dim(B)$ being the dimensions of systems A and B, respectively. Fix $a \in (2\log_2 d, \infty)$. Then the following bound holds:*

$$\widetilde{P}_a^{\rightarrow}(\mathcal{N}_{A\to B}) = \widetilde{K}_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B}) \leqslant \widehat{E}^{u}(\mathcal{N}_{A\to B}), \quad (237)$$

where $\widehat{E}^{u}(\mathcal{N}_{A\to B})$ is the unextendible entanglement of the channel $\mathcal{N}_{A\to B}$ induced by the Belavkin–Staszewski relative entropy defined in (197).

Proof. The proof is similar to the proof of theorem 3. We sketch out the main arguments here.

Let $\mathcal{N}_{A\to B}$ be an arbitrary quantum channel, with input and output dimensions $\dim(A)$ and $\dim(B)$ respectively, from which we wish to distill secret keys. Let $\left\{\Theta^{n,1\mathrm{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}\right\}_{n\in\mathbb{N}}$ be a sequence of one-way LOCC superchannels, let $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ be a sequence of bipartite private states, and let $\left\{\rho^{n}_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}$ be a sequence of quantum states such that the following condition holds for all $a > 2\log_2 d$ and $n \in \mathbb{N}$:

$$F\left(\gamma^{k_n}_{A'B'A''B''}, \left(\Theta^{n,1\mathrm{WL}}\left(\mathcal{N}^{\otimes n}_{A\to B}\right)\right)\left(\rho^{n}_{A'A''\hat{A}}\right)\right) \geqslant 1 - 2^{-an}, \quad (238)$$

where $d := \min\{\dim(A), \dim(B)\}$.

Let us set $\varepsilon_n := 2^{-an}$ for convenience. Corollary 4 implies that the following inequality holds for all one-way LOCC secret-key distillation protocols such that (238) is satisfied:

$$\log_2 k_n \leqslant -\log_2\left(\sqrt{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})} - \sqrt{\varepsilon_n}\right) \quad (239)$$

$$= -\frac{1}{2}\log_2\left(J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})\right) - \log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})}}\right). \quad (240)$$

The quantity $J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})$ is bounded from below by the following quantity:

$$J^{\varepsilon_n}_{\min}\left(\mathcal{N}^{\otimes n}_{A\to B}\right) \geqslant \frac{1-\varepsilon_n}{d^{2n}}, \quad (241)$$

which is evident from proposition 6. The inequalities in (240) and (241) allow us to use the mathematical arguments presented in (148)–(155) in order to conclude the following:

$$\limsup_{n\to\infty} -\frac{1}{n}\log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})}}\right) = 0. \quad (242)$$

Therefore, taking $\limsup_{n\to\infty}$ in (240) leads to the following inequality:

$$\begin{aligned}
&\limsup_{n\to\infty}\frac{\log_2 k_n}{n}\\
&\leqslant \limsup_{n\to\infty}\left\{-\frac{1}{2n}\log_2\left(J_{\min}^{\varepsilon_n}\left(\mathcal{N}^{\otimes n}\right)\right)\right.\\
&\qquad\left.-\frac{1}{n}\log_2\left(1-\sqrt{\frac{\varepsilon_n}{J_{\min}^{\varepsilon_n}\left(\mathcal{N}^{\otimes n}\right)}}\right)\right\} \qquad (243)\\
&= \limsup_{n\to\infty}-\frac{1}{2n}\log_2\left(J_{\min}^{\varepsilon_n}\left(\mathcal{N}^{\otimes n}\right)\right)\\
&\quad+\limsup_{n\to\infty}-\frac{1}{n}\log_2\left(1-\sqrt{\frac{\varepsilon_n}{J_{\min}^{\varepsilon_n}\left(\mathcal{N}^{\otimes n}\right)}}\right) \qquad (244)\\
&= \limsup_{n\to\infty}-\frac{1}{2n}\log_2\left(J_{\min}^{\varepsilon_n}\left(\mathcal{N}^{\otimes n}\right)\right) \qquad (245)\\
&= \limsup_{n\to\infty}\frac{1}{n}E_{\min}^{u,\varepsilon_n}\left(\mathcal{N}^{\otimes n}\right), \qquad (246)
\end{aligned}$$

where the second equality follows from (242).

Recall the relation between the smooth-min unextendible entanglement of a channel and the α-geometric unextendible entanglement of the channel from (205). The inequality in (205) combined with (246) leads to the following inequality:

$$\limsup_{n\to\infty}\frac{\log_2 k_n}{n}\leqslant\limsup_{n\to\infty}\frac{1}{n}\left(\widehat{E}_\alpha^u\left(\mathcal{N}^{\otimes n}\right)-\frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2(1-\varepsilon_n)\right) \qquad (247)$$

$$=\limsup_{n\to\infty}\frac{1}{n}\widehat{E}_\alpha^u\left(\mathcal{N}^{\otimes n}\right)+\limsup_{n\to\infty}-\frac{1}{2n}\cdot\frac{\alpha}{\alpha-1}\log_2(1-\varepsilon_n), \qquad (248)$$

which holds for all $\alpha\in(1,2]$. Since $\varepsilon_n\to 0$ as $n\to\infty$,

$$\limsup_{n\to\infty}-\frac{1}{2n}\cdot\frac{\alpha}{\alpha-1}\log_2(1-\varepsilon_n)=0. \qquad (249)$$

Now using the subadditivity of the α-geometric unextendible entanglement of channels, we arrive at the following inequality:

$$\limsup_{n\to\infty}\frac{\log_2 k_n}{n}\leqslant\limsup_{n\to\infty}\frac{1}{n}\widehat{E}_\alpha^u\left(\mathcal{N}^{\otimes n}\right)\leqslant\widehat{E}_\alpha^u(\mathcal{N}). \qquad (250)$$

The above inequality holds for every sequence $\{k_n\}_{n\in\mathbb{N}}$ for which there exists a sequence of private states $\left\{\gamma_{A'B'A''B''}^{k_n}\right\}_{n\in\mathbb{N}}$, a sequence of one-way LOCC superchannels $\left\{\Theta_{(A^n\to B^n)\to(\hat{A}\to B'B'')}^{n,1\text{WL}}\right\}_{n\in\mathbb{N}}$, and a sequence of states $\left\{\rho_{A'A''\hat{A}}^n\right\}_{n\in\mathbb{N}}$ such that (238) holds for all $a>2\log_2 d$ and $n\in\mathbb{N}$. Therefore,

$$\widetilde{K}_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B})\leqslant\widehat{E}_\alpha^u(\mathcal{N}_{A\to B})\qquad\forall\alpha\in(1,2], \qquad (251)$$

which follows from the definition of $\widetilde{K}_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B})$. Since the α-geometric unextendible entanglement of a channel increases monotonically with α, we can take $\lim_{\alpha\to 1^+}$ to obtain the tightest upper bound, which is the unextendible entanglement of the channel $\mathcal{N}_{A\to B}$ induced by the Belavkin–Staszewski relative entropy. Finally, using (236) leads to the statement of the theorem. □

7. Conclusion

In this paper we studied the task of secret-key distillation from bipartite states and point-to-point quantum channels using local operations and one-way classical communication. Using the resource theory of unextendible entanglement, which is a semidefinite relaxation of the resource theory of entanglement, we obtained efficiently computable upper bounds on several quantities of interest in the theory of private communication over a quantum network.

We derived efficiently computable upper bounds on the one-shot, one-way distillable key of a bipartite state using the resource theory of unextendible entanglement. We also derived upper bounds on the one-shot forward-assisted private capacity of a channel that can be computed using a semidefinite program. In both cases, these are the first instances of efficiently computable upper bounds on these quantities, to the best of our knowledge.

We extended our results to the i.i.d. setting and obtained single-letter efficiently computable upper bounds on the n-shot one-way distillable key of bipartite states and n-shot forward-assisted private capacity of point-to-point channels. Finally, we obtained efficiently computable upper bounds on the rate at which secret keys can be distilled from a bipartite state or a quantum channel using one-way LOCC when the error is required to decay exponentially with an error exponent larger than a fixed threshold.

The majority of bounds obtained in this work can be computed using semidefinite programs. We numerically computed the upper bounds on the one-shot, one-way distillable key and the n-shot, one-way distillable key for isotropic states to demonstrate our results. We also found analytical expressions for the upper bounds on the n-shot, forward-assisted private capacity of erasure channels.

We obtained a family of upper bounds on the n-shot, one-way distillable key of a bipartite state in this work using the α-sandwiched Rényi relative entropy. However, a semidefinite representation of the α-sandwiched Rényi relative entropy is only known when $\alpha\to\infty$. As such, only one member from the family of upper bounds on the n-shot, one-way distillable key of a state is known to be efficiently computable.

Going forward from here, there are some open problems left for future investigation. The bounds obtained in this work are based on the resource theory of unextendible entanglement. It may be possible to obtain stronger bounds by studying entanglement measures that combine the concepts of unextendibility and the positive partial transpose criterion. Furthermore, it can give insights into the asymptotic setting of private communication where there are no assumptions

on the rate at which error decays. As another open problem of interest, finding semidefinite representations of the α-sandwiched Rényi relative entropies would improve our numerical findings here, as they can lead to tighter efficiently computable bounds on the n-shot, one-way distillable key of a state.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

V S and M M W acknowledge support from the National Science Foundation under Grant No. 2329662. M M W acknowledges Nilanjana Datta for many insightful discussions about this project, starting from a visit to her group at University of Cambridge in October 2022, and V S and M M W are also grateful to her for feedback on the manuscript. We also thank Kaiyuan Ji, Theshani Nuradha, Dhrumil Patel, and Aby Philip for helpful discussions.

Author contributions

The following describes the different contributions of the authors of this work, using roles defined by the CRediT (Contributor Roles Taxonomy) project [NIS]:

V S: Formal Analysis, Investigation, Methodology, Software, Writing—Original draft, Validation, Writing—Review & Editing.

M M W: Conceptualization, Formal Analysis, Funding acquisition, Investigation, Methodology, Supervision, Validation, Writing—Review & Editing.

Appendix A. Proof of proposition 1

In this section, we calculate the smooth-min unextendible entanglement of the maximally entangled state Φ_{AB}^d.

We first note that all extensions of the state Φ_{AB}^d are of the form $\Phi_{AB}^d \otimes \tau_E$ since Φ_{AB}^d is a pure state. Therefore, all states in the set $\mathcal{F}(\Phi_{AB}^d)$ are of the form $\pi_A \otimes \tau_E$, where π_A is the maximally mixed state and $E \cong B$. The unextendible entanglement of Φ_{AB}^d induced by the hypothesis testing relative entropy can be calculated as follows:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) = \inf_{\tau_B \in \mathcal{S}(B)} \frac{1}{2} D_{\min}^{\varepsilon}\left(\Phi_{AB}^d \| \pi_A \otimes \tau_B\right) \tag{A.1}$$

$$= \inf_{\tau_B} -\frac{1}{2}\log_2 \inf_{0 \leqslant \Lambda \leqslant I} \left\{ \operatorname{Tr}[\Lambda_{AB}\left(\pi_A \otimes \tau_B\right)] : \operatorname{Tr}\left[\Lambda_{AB}\Phi_{AB}^d\right] \geqslant 1-\varepsilon \right\}. \tag{A.2}$$

Choosing $\Lambda_{AB} = (1-\varepsilon)\Phi_{AB}^d$, we find that

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) \geqslant \inf_{\tau_B} -\frac{1}{2}\log_2\left(\left(1-\varepsilon\right)\operatorname{Tr}\left[\Phi_{AB}^d\left(\pi_A \otimes \tau_B\right)\right]\right) \tag{A.3}$$

$$= \inf_{\tau_B} -\frac{1}{2}\log_2\left(\frac{1-\varepsilon}{d}\operatorname{Tr}\left[\Phi_{AB}^d\left(I_A \otimes \tau_B\right)\right]\right) \tag{A.4}$$

$$= \inf_{\tau_B} -\frac{1}{2}\log_2\left(\frac{1-\varepsilon}{d}\operatorname{Tr}[\pi_B\tau_B]\right) \tag{A.5}$$

$$= \inf_{\tau_B} -\frac{1}{2}\log_2\left(\frac{1-\varepsilon}{d^2}\operatorname{Tr}[\tau_B]\right) \tag{A.6}$$

$$= -\frac{1}{2}\log_2\left(\frac{1-\varepsilon}{d^2}\right). \tag{A.7}$$

The hypothesis testing relative entropy can also be computed using the following SDP:

$$D_{\min}^{\varepsilon}(\rho_{AB}) = -\log_2 \sup_{\mu \geqslant 0, Z \geqslant 0} \left\{ \mu\left(1-\varepsilon\right) - \operatorname{Tr}[Z] : \mu\rho \leqslant \sigma + Z \right\}. \tag{A.8}$$

The unextendible entanglement of the maximally entangled state induced by the hypothesis testing relative entropy can then be computed as follows:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) = \inf_{\tau_B \in \mathcal{S}(B)} -\frac{1}{2}\log_2 \sup_{\mu \geqslant 0, Z \geqslant 0} \left\{ \mu\left(1-\varepsilon\right) - \operatorname{Tr}[Z] : \mu\Phi_{AB}^d \leqslant \pi_A \otimes \tau_B + Z_{AB} \right\}. \tag{A.9}$$

Choosing τ_B to be the maximally mixed state, we arrive at the following inequality:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) \leqslant -\frac{1}{2}\log_2 \sup_{\mu \geqslant 0, Z \geqslant 0} \left\{ \mu\left(1-\varepsilon\right) - \operatorname{Tr}[Z] : \mu\Phi_{AB}^d \leqslant \pi_{AB} + Z_{AB} \right\} \tag{A.10}$$

$$= \inf_{\mu \geqslant 0, Z \geqslant 0} -\frac{1}{2}\log_2 \left\{ \mu\left(1-\varepsilon\right) - \operatorname{Tr}[Z] : \mu\Phi_{AB}^d \leqslant \pi_{AB} + Z_{AB} \right\}. \tag{A.11}$$

Note that the pair $\left(\mu = 1/d^2, Z = 0\right)$ lies in the feasible set of the aforementioned SDP. Therefore, setting $\mu = 1/d^2$ and $Z = 0$ leads to the following inequality:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) \leqslant -\frac{1}{2}\log_2\left(\frac{1-\varepsilon}{d^2}\right) = \log_2 d - \frac{1}{2}\log_2\left(1-\varepsilon\right). \tag{A.12}$$

Combining (A.7) and (A.12) concludes the proof.

Appendix B. Proof of proposition 2

In this section we find the range of values that the smooth-min unextendible entanglement of a state can take.

The smooth-min relative entropy between two states is never smaller than $-\log_2(1-\varepsilon)$, which can be seen from the data-processing inequality of the smooth-min relative entropy as follows:

$$D^{\varepsilon}_{\min}(\rho\|\sigma) \geqslant D^{\varepsilon}_{\min}(\mathcal{R}^{\pi}(\rho)\,\|\mathcal{R}^{\pi}(\sigma)) \tag{B.1}$$

$$= D^{\varepsilon}_{\min}(\pi\|\pi) \tag{B.2}$$

$$= -\log_2 \inf_{0\leqslant\Lambda\leqslant I}\{\mathrm{Tr}[\Lambda\pi] : \mathrm{Tr}[\Lambda\pi] \geqslant 1-\varepsilon\} \tag{B.3}$$

$$= -\log_2(1-\varepsilon), \tag{B.4}$$

where $\mathcal{R}^{\pi}$ is a channel that traces out the state it acts on and replaces it with the maximally mixed state π. This leads to the following bound on the smooth-min unextendible entanglement of a bipartite state ρ_{AB}:

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) = \inf_{\sigma\in\mathcal{F}(\rho)} \frac{1}{2} D^{\varepsilon}_{\min}(\rho_{AB}\|\sigma_{AB}) \geqslant -\frac{1}{2}\log_2(1-\varepsilon). \tag{B.5}$$

To find an upper bound on $E^{u,\varepsilon}_{\min}(\rho_{AB})$, we invoke (37). Since the hypothesis testing relative entropy is an example of generalized divergence, (37) implies the following inequality:

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) \leqslant E^{u,\varepsilon}_{\min}\left(\Phi^{d}_{A_0B_0}\right) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), \tag{B.6}$$

where $d := \min\{\dim(A), \dim(B)\}$. The equality in (B.6) follows from proposition 1.

Appendix C. Proof of equation (83)

In this appendix, we show that (82) implies (83).

Let us analyze the expression on the right-hand side of (82) in the interval $q \in [0,1]$ and for $k \in \mathbb{N}$. In what follows, we find the inflection points of the expression by setting the derivative equal to zero:

$$0 = \frac{\partial}{\partial q}\left(\sqrt{\frac{q}{k^2}} + \sqrt{(1-q)\left(1-\frac{1}{k^2}\right)}\right)^2 \tag{C.1}$$

$$= 2\left(\sqrt{\frac{q}{k^2}} + \sqrt{(1-q)\left(1-\frac{1}{k^2}\right)}\right)\left(\frac{1}{2k\sqrt{q}} - \frac{1}{2\sqrt{1-q}}\sqrt{1-\frac{1}{k^2}}\right). \tag{C.2}$$

Solving the above equation for q, we find that

$$\frac{1}{2k\sqrt{q}} = \frac{1}{2\sqrt{1-q}}\sqrt{1-\frac{1}{k^2}} \tag{C.3}$$

$$\implies \sqrt{1-q} = \sqrt{q(k^2-1)} \tag{C.4}$$

$$\implies 1-q = q(k^2-1) \tag{C.5}$$

$$\implies q = \frac{1}{k^2}. \tag{C.6}$$

It is easy to verify that the function of q given on the right-hand side of (82) achieves its maximum value at this inflection point. Therefore, the function is monotonically increasing for $q \in [0, \frac{1}{k^2}]$, and it is monotonically decreasing for $q \in [\frac{1}{k^2}, 1]$. Equivalently, the derivative in (C.2) is non-negative for $q \in [0, \frac{1}{k^2}]$, and it is non-positive for $q \in [\frac{1}{k^2}, 1]$.

Now let us find the values of q that satisfy (82). We can rewrite the inequality in (82) as follows:

$$1-\varepsilon \leqslant \frac{q}{k^2} + (1-q)\left(1-\frac{1}{k^2}\right) + 2\sqrt{q(1-q)}\sqrt{\frac{1}{k^2}\left(1-\frac{1}{k^2}\right)}. \tag{C.7}$$

Rearranging the terms, we arrive at the following inequality:

$$q\left(1-\frac{2}{k^2}\right) - \varepsilon + \frac{1}{k^2} \leqslant 2\sqrt{q(1-q)}\sqrt{\frac{1}{k^2}\left(1-\frac{1}{k^2}\right)}. \tag{C.8}$$

The right-hand side of the above equation is always non-negative for all $q \in [0,1]$ and $k \in \mathbb{N}$. If the left-hand side of the above inequality is negative, then the above inequality is satisfied. As such, the above inequality is satisfied if the following condition holds:

$$q\left(1-\frac{2}{k^2}\right)-\varepsilon+\frac{1}{k^2} \leqslant 0 \implies q \leqslant \frac{\varepsilon-\frac{1}{k^2}}{1-\frac{2}{k^2}} \quad \forall k \geqslant 2. \tag{C.9}$$

If $\varepsilon-\frac{1}{k^2} \geqslant 0$ then the inequality in (C.8) is satisfied for all $q \in \left[0, \frac{\varepsilon-k^{-2}}{1-2k^{-2}}\right]$ and $k \geqslant 2$.

Now let us consider the case where the left-hand side of (C.8) is non-negative, which is true for $k \geqslant 2$ if $\varepsilon \leqslant \frac{1}{k^2}$ or $q \geqslant \left(\varepsilon-\frac{1}{k^2}\right)/\left(1-\frac{2}{k^2}\right)$. We can square both sides to get the following inequality:

$$\left(q\left(1-\frac{2}{k^2}\right)-\varepsilon+\frac{1}{k^2}\right)^2 \leqslant \left(2\sqrt{q(1-q)}\sqrt{\frac{1}{k^2}\left(1-\frac{1}{k^2}\right)}\right)^2 \tag{C.10}$$

$$= \frac{4}{k^2}\left(1-\frac{1}{k^2}\right)q(1-q). \tag{C.11}$$

Setting

$$d := 1-\frac{2}{k^2}, \tag{C.12}$$

$$e := \varepsilon-\frac{1}{k^2}, \tag{C.13}$$

$$f := \frac{4}{k^2}\left(1-\frac{1}{k^2}\right), \tag{C.14}$$

we can rewrite the above inequality as follows:

$$(d\cdot q-e)^2 \leqslant f\cdot q(1-q) \tag{C.15}$$

$$\implies d^2q^2+e^2-2deq \leqslant fq-fq^2 \tag{C.16}$$

$$\implies \left(d^2+f\right)q^2-(2de+f)q+e^2 \leqslant 0. \tag{C.17}$$

The above inequality is in the standard form of a quadratic inequality. Let us first find each of the coefficients. The coefficient of q^2 evaluates to the following:

$$d^2+f = \left(1-\frac{2}{k^2}\right)^2+\frac{4}{k^2}\left(1-\frac{1}{k^2}\right) \tag{C.18}$$

$$= 1+\frac{4}{k^4}-\frac{4}{k^2}+\frac{4}{k^2}-\frac{4}{k^4} \tag{C.19}$$

$$= 1. \tag{C.20}$$

The coefficient of q evaluates to the following:

$$-2de-f = -2\left(1-\frac{2}{k^2}\right)\left(\varepsilon-\frac{1}{k^2}\right)-\frac{4}{k^2}\left(1-\frac{1}{k^2}\right) \tag{C.21}$$

$$= -2\left(\varepsilon-\frac{1}{k^2}-\frac{2\varepsilon}{k^2}+\frac{2}{k^4}\right)-\frac{4}{k^2}+\frac{4}{k^4} \tag{C.22}$$

$$= -2\left(\varepsilon+\frac{1-2\varepsilon}{k^2}\right). \tag{C.23}$$

Finally, the term independent of q is equal to the following:

$$e^2 = \left(\varepsilon-\frac{1}{k^2}\right)^2 \tag{C.24}$$

$$= \varepsilon^2+\frac{1}{k^4}-\frac{2\varepsilon}{k^2}. \tag{C.25}$$

The quadratic inequality in (C.11) can now be written as follows:

$$q^2 - 2q\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right) + \varepsilon^2 + \frac{1}{k^4} - \frac{2\varepsilon}{k^2} \leqslant 0. \tag{C.26}$$

The discriminant of the above quadratic expression can be evaluated as follows:

$$\begin{aligned}
&(-2de - f)^2 - 4\left(d^2 + f\right)e^2 \\
&= 4\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right)^2 - 4\left(\varepsilon^2 + \frac{1}{k^4} - \frac{2\varepsilon}{k^2}\right) && \text{(C.27)}\\
&= 4\left(\varepsilon^2 + \left(\frac{1-2\varepsilon}{k^2}\right)^2 + 2\varepsilon\left(\frac{1-2\varepsilon}{k^2}\right) - \varepsilon^2 - \frac{1}{k^4} + \frac{2\varepsilon}{k^2}\right) && \text{(C.28)}\\
&= 4\left(\frac{1+4\varepsilon^2-4\varepsilon}{k^4} - \frac{1}{k^4} + \frac{2\varepsilon}{k^2}(2-2\varepsilon)\right) && \text{(C.29)}\\
&= 4\left(\frac{4\varepsilon(\varepsilon-1)}{k^4} + \frac{4\varepsilon(1-\varepsilon)}{k^2}\right) && \text{(C.30)}\\
&= 16\frac{\left(k^2-1\right)\varepsilon(1-\varepsilon)}{k^4}. && \text{(C.31)}
\end{aligned}$$

We can now factor the quadratic expression in (C.26) as follows:

$$(q - \alpha_{q+})(q - \alpha_{q-}) \leqslant 0, \tag{C.32}$$

where

$$\begin{aligned}
\alpha_{q\pm} &= \frac{1}{2}\left(2\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right) \pm \frac{\sqrt{16\left(k^2-1\right)\varepsilon(1-\varepsilon)}}{k^2}\right) && \text{(C.33)}\\
&= \varepsilon + \frac{1-2\varepsilon}{k^2} \pm \frac{2\sqrt{\left(k^2-1\right)\varepsilon(1-\varepsilon)}}{k^2}. && \text{(C.34)}
\end{aligned}$$

Now we are in a position to identify the range of values that q can take for all $\varepsilon \in [0,1]$ and $k \geqslant 2$.

- If $\varepsilon \in \left[0, \frac{1}{k^2}\right]$, then

$$\alpha_{q-} \leqslant q \leqslant \alpha_{q+}, \tag{C.35}$$

  where α_{q-} and α_{q+} are defined in (C.34).
- If $\varepsilon \in \left[\frac{1}{k^2}, 1\right]$, then

$$q \in \left[0, \min\left\{\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}}, 1\right\}\right] \cup \left[\alpha_{q-}, \alpha_{q+}\right]. \tag{C.36}$$

We can identify the values of ε such that the two intervals in (C.36) overlap. Let us first find the values of ε that satisfy the following inequality:

$$\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}} \leqslant \alpha_{q+} = \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{\left(k^2-1\right)\varepsilon(1-\varepsilon)}}{k^2}. \tag{C.37}$$

We can rearrange the terms of the above inequality to get the following inequality:

$$\begin{aligned}
&\frac{k^2\varepsilon - 1}{k^2 - 2} - \frac{\left(k^2-2\right)\varepsilon + 1}{k^2} \leqslant \frac{2\sqrt{\left(k^2-1\right)\varepsilon(1-\varepsilon)}}{k^2} && \text{(C.38)}\\
\implies &\frac{k^4\varepsilon - k^2 - \left(k^2-2\right)^2\varepsilon - k^2 + 2}{k^2\left(k^2-2\right)} \leqslant \frac{2\sqrt{\left(k^2-1\right)\varepsilon(1-\varepsilon)}}{k^2} && \text{(C.39)}
\end{aligned}$$

$$\implies \frac{4\left(k^2-1\right)\varepsilon+2\left(1-k^2\right)}{k^2-2} \leqslant 2\sqrt{\left(k^2-1\right)\varepsilon\left(1-\varepsilon\right)} \tag{C.40}$$

$$\implies \frac{\left(k^2-1\right)\left(2\varepsilon-1\right)}{k^2-2} \leqslant \sqrt{\left(k^2-1\right)\varepsilon\left(1-\varepsilon\right)}. \tag{C.41}$$

The above inequality is satisfied for all $\varepsilon \in [0,1/2]$ and $k \geqslant 2$. Now assuming that $\varepsilon \geqslant 1/2$ and $k \geqslant 2$, we can square both sides of the above inequality to get the following inequality:

$$\frac{\left(k^2-1\right)\left(2\varepsilon-1\right)^2}{\left(k^2-2\right)^2} \leqslant \varepsilon\left(1-\varepsilon\right). \tag{C.42}$$

Setting $a := (k^2-1)/(k^2-2)^2$, we can rewrite the above inequality as follows:

$$a\left(2\varepsilon-1\right)^2 \leqslant \varepsilon\left(1-\varepsilon\right) \tag{C.43}$$

$$\implies (4a+1)\varepsilon^2-(4a+1)\varepsilon+a \leqslant 0. \tag{C.44}$$

Note that a is a positive number, which implies that $4a+1$ is also a positive number. Therefore, the above quadratic inequality can be factored as follows:

$$\left(\varepsilon-\frac{1}{2}\left(1+\frac{1}{\sqrt{4a+1}}\right)\right)\left(\varepsilon-\frac{1}{2}\left(1-\frac{1}{\sqrt{4a+1}}\right)\right) \leqslant 0. \tag{C.45}$$

Substituting the value of a, the quantity $\sqrt{4a+1}$ evaluates to the following:

$$\sqrt{4a+1} = \frac{k^2}{k^2-2}. \tag{C.46}$$

Therefore, the inequality in (C.45) can be written as follows:

$$\left(\varepsilon-\frac{1}{2}\left(1+\frac{k^2-2}{k^2}\right)\right)\left(\varepsilon-\frac{1}{2}\left(1-\frac{k^2-2}{k^2}\right)\right) \leqslant 0 \tag{C.47}$$

$$\implies \left(\varepsilon-\left(1-\frac{1}{k^2}\right)\right)\left(\varepsilon-\frac{1}{k^2}\right) \leqslant 0. \tag{C.48}$$

The above inequality is satisfied only when $\varepsilon \in \left[1/k^2, 1-1/k^2\right]$. To get the above inequality we assumed that $\alpha \geqslant 1/2$. Since $1-\frac{1}{k^2} \geqslant \frac{1}{2}$ for all $k \geqslant 2$ and every $\varepsilon \in [0,1/2]$ satisfies the inequality in (C.37), we conclude that the inequality in (C.37) is satisfied if and only if $\varepsilon \in \left[0, 1-\frac{1}{k^2}\right]$.

Now let us find the values of ε for which the following inequality is satisfied:

$$\frac{\varepsilon-\frac{1}{k^2}}{1-\frac{2}{k^2}} \leqslant \alpha_{q-} = \varepsilon + \frac{1-2\varepsilon}{k^2} - \frac{2\sqrt{\left(k^2-1\right)\varepsilon\left(1-\varepsilon\right)}}{k^2}. \tag{C.49}$$

Following the same steps as above, we arrive at the following inequality:

$$\frac{\left(k^2-1\right)\left(2\varepsilon-1\right)}{k^2-2} \leqslant -\sqrt{\left(k^2-1\right)\varepsilon\left(1-\varepsilon\right)}, \tag{C.50}$$

which is similar to (C.41). This inequality is not satisfied by any value of $\varepsilon \geqslant 1/2$. Under the assumption that $\varepsilon \leqslant 1/2$, we can square both sides of the above inequality to get the following inequality:

$$\frac{\left(k^2-1\right)\left(2\varepsilon-1\right)^2}{\left(k^2-2\right)^2} \geqslant \varepsilon\left(1-\varepsilon\right). \tag{C.51}$$

From the solution of (C.42), we know that the opposite of this quadratic inequality is satisfied when $\varepsilon \in \left[\frac{1}{k^2}, 1-\frac{1}{k^2}\right]$. Therefore, the inequality in (C.51) is satisfied when $\varepsilon \in \left[0, \frac{1}{k^2}\right] \cup \left[1-\frac{1}{k^2}, 1\right]$. Recall that we assumed $\varepsilon \in [0,1/2]$ to arrive at (C.51) from (C.50). Therefore, for every $k \geqslant 2$, we conclude that (C.49) is satisfied for all $\varepsilon \in \left[0, \frac{1}{k^2}\right]$.

Now we know the values of q that satisfy (82) for some fixed value of $\varepsilon \in [0,1]$ and integer $k \geqslant 2$, which are given as follows:

$$q \in \begin{cases} [\alpha_{q-}, \alpha_{q+}] & \text{if } \varepsilon \in \left[0, \frac{1}{k^2}\right] \\ [0, \alpha_{q+}] & \text{if } \varepsilon \in \left[\frac{1}{k^2}, 1-\frac{1}{k^2}\right] \\ \left[0, \min\left\{\frac{\varepsilon-\frac{1}{k^2}}{1-\frac{2}{k^2}}, 1\right\}\right] & \text{if } \varepsilon \in \left[1-\frac{1}{k^2}, 1\right] \end{cases}, \tag{C.52}$$

where α_{q+} and α_{q-} are defined in (C.34). Observe that $\frac{\varepsilon-\frac{1}{k^2}}{1-\frac{2}{k^2}} \geqslant 1$ for all $\varepsilon \in \left[1-\frac{1}{k^2}, 1\right]$. Therefore, we can rewrite the above condition as follows:

$$q \in \begin{cases} [\alpha_{q-}, \alpha_{q+}] & \text{if } \varepsilon \in \left[0, \frac{1}{k^2}\right] \\ [0, \alpha_{q+}] & \text{if } \varepsilon \in \left[\frac{1}{k^2}, 1-\frac{1}{k^2}\right] \\ [0,1] & \text{if } \varepsilon \in \left[1-\frac{1}{k^2}, 1\right] \end{cases}. \tag{C.53}$$

As such, if $\varepsilon \leqslant 1-\frac{1}{k^2}$, then q is bounded from above by the following quantity:

$$q \leqslant \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)}}{k^2}, \tag{C.54}$$

and otherwise, when $\varepsilon > 1-\frac{1}{k^2}$, we only have the trivial bound $q \leqslant 1$.

Appendix D. Proof of theorem 2

First let us note that the condition $\varepsilon < J^{\varepsilon}_{\min}(\rho_{AB})$ is only satisfied if $\varepsilon < \frac{1}{2}$. This is because $J^{\varepsilon}_{\min}(\rho_{AB}) \leqslant 1-\varepsilon$, as stated in proposition 2. So we restrict to $\varepsilon < \frac{1}{2}$ for the remainder of the proof.

Let $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ be a one-way LOCC channel that acts on ρ_{AB} to give a state $\sigma_{A'B'A''B''}$ such that $F(\sigma_{A'B'A''B''}, \gamma^k_{A'B'A''B''}) \geqslant 1-\varepsilon$ for some bipartite private state $\gamma^k_{A'B'A''B''}$. That is,

$$\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}(\rho_{AB}) = \sigma_{A'B'A''B''}. \tag{D.1}$$

The smooth-min unextendible entanglement of a bipartite state does not increase under the action of a one-way LOCC channel [WWW24, theorem 2]. Therefore,

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) \geqslant E^{u,\varepsilon}_{\min}(\mathcal{L}^{\rightarrow}(\rho_{AB})) \tag{D.2}$$

$$= E^{u,\varepsilon}_{\min}(\sigma_{A'B'A''B''}). \tag{D.3}$$

Consequently,

$$J^{\varepsilon}_{\min}(\rho_{AB}) \leqslant J^{\varepsilon}_{\min}(\sigma_{A'B'A''B''}). \tag{D.4}$$

Since $\varepsilon < \frac{1}{2}$, we can use remark 3 to state that one cannot distill any secret bits from a state ρ_{AB} with an error tolerance of ε if $J^{\varepsilon}_{\min}(\rho_{AB}) > \varsigma(\varepsilon, 2)$, where ς is defined in (60).

Let us now consider the case when one-shot, one-way secret-key distillation is possible. Proposition 3 implies that the following inequality holds for all $\varepsilon \in \left[0, \frac{1}{2}\right)$:

$$J^{\varepsilon}_{\min}(\rho_{AB}) \leqslant \varsigma(\varepsilon, k) = \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)}}{k^2} \tag{D.5}$$

if $F\left(\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}(\rho_{AB}), \gamma^k_{A'B'A''B''}\right) \geqslant 1-\varepsilon$ for some one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ and some private state $\gamma^k_{A'B'A''B''}$ with $k \geqslant 2$. We will use $J^{\varepsilon}_{\min}$ as a shorthand for $J^{\varepsilon}_{\min}(\rho_{AB})$ in the remainder of the proof for convenience. Rearranging the terms in (D.5), we arrive at the following inequality:

$$k^2\,(J^{\varepsilon}_{\min} - \varepsilon) \leqslant 1 - 2\varepsilon + 2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)} \tag{D.6}$$

$$\implies \left(k^2-1\right)(J^{\varepsilon}_{\min} - \varepsilon) + J^{\varepsilon}_{\min} - \varepsilon \leqslant 1 - 2\varepsilon + 2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)} \tag{D.7}$$

$$\implies \left(k^2-1\right)(J^{\varepsilon}_{\min} - \varepsilon) + J^{\varepsilon}_{\min} + \varepsilon - 1 \leqslant 2\sqrt{(k^2-1)\,\varepsilon\,(1-\varepsilon)}. \tag{D.8}$$

The above inequality is always satisfied if the left-hand side is non-positive, that is, if

$$\left(k^2-1\right)\left(J^{\varepsilon}_{\min}-\varepsilon\right)+J^{\varepsilon}_{\min}+\varepsilon-1\leqslant 0. \tag{D.9}$$

Note that $J^{\varepsilon}_{\min}+\varepsilon-1$ is always non-positive due to (45). Therefore, if $J^{\varepsilon}_{\min}\leqslant\varepsilon$, then the above inequality holds for all $k\in\mathbb{N}$. If $J^{\varepsilon}_{\min}>\varepsilon$, then (D.9) is satisfied when the following condition holds:

$$k^2-1\leqslant\frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}. \tag{D.10}$$

Consequently, if the inequality in (D.10) holds, then the inequality in (D.8) also holds for all $J^{\varepsilon}_{\min}\in[0,1-\varepsilon]$.

Now let us assume that $(k^2-1)(J^{\varepsilon}_{\min}-\varepsilon)+J^{\varepsilon}_{\min}+\varepsilon-1>0$. Then we can square both sides of (D.8) to get the following inequality:

$$\left(\left(k^2-1\right)\left(J^{\varepsilon}_{\min}-\varepsilon\right)+J^{\varepsilon}_{\min}+\varepsilon-1\right)^2\leqslant 4\left(k^2-1\right)\varepsilon\left(1-\varepsilon\right). \tag{D.11}$$

We write the above inequality as follows:

$$\left(d\cdot x+e\right)^2\leqslant f\cdot x, \tag{D.12}$$

where we have made the following assignments:

$$x:=k^2-1, \tag{D.13}$$
$$d:=J^{\varepsilon}_{\min}-\varepsilon, \tag{D.14}$$
$$e:=J^{\varepsilon}_{\min}+\varepsilon-1, \tag{D.15}$$
$$f:=4\varepsilon\left(1-\varepsilon\right). \tag{D.16}$$

We can write the inequality in (D.12) as the following quadratic inequality in x:

$$d^2x^2+e^2+2de\cdot x\leqslant f\cdot x \tag{D.17}$$
$$\implies d^2x^2+\left(2de-f\right)x+e^2\leqslant 0. \tag{D.18}$$

The coefficient of x^2 evaluates to the following:

$$d^2=\left(J^{\varepsilon}_{\min}-\varepsilon\right)^2. \tag{D.19}$$

The coefficient of x evaluates to the following:

$$2de-f=2\left(J^{\varepsilon}_{\min}-\varepsilon\right)\left(J^{\varepsilon}_{\min}+\varepsilon-1\right)-4\varepsilon\left(1-\varepsilon\right) \tag{D.20}$$
$$=-2J^{\varepsilon}_{\min}\left(1-J^{\varepsilon}_{\min}\right)-2\varepsilon\left(1-\varepsilon\right). \tag{D.21}$$

In what follows, we compute the discriminant of the above quadratic expression:

$$\left(2de-f\right)^2-4d^2e^2=4d^2e^2+f^2-4def-4d^2e^2 \tag{D.22}$$
$$=f^2-4def \tag{D.23}$$
$$=16\varepsilon^2\left(1-\varepsilon\right)^2-16\left(J^{\varepsilon}_{\min}-\varepsilon\right)\left(J^{\varepsilon}_{\min}+\varepsilon-1\right)\varepsilon\left(1-\varepsilon\right) \tag{D.24}$$
$$=16\varepsilon\left(1-\varepsilon\right)\left[\varepsilon\left(1-\varepsilon\right)-\left(J^{\varepsilon}_{\min}\right)^2+J^{\varepsilon}_{\min}-\varepsilon\left(1-\varepsilon\right)\right] \tag{D.25}$$
$$=16\varepsilon\left(1-\varepsilon\right)J^{\varepsilon}_{\min}\left(1-J^{\varepsilon}_{\min}\right). \tag{D.26}$$

Note that the coefficient of x^2, that is $(J^{\varepsilon}_{\min}-\varepsilon)^2$, is always positive since we have assumed that $J^{\varepsilon}_{\min}>\varepsilon$, which allows us to factor the quadratic expression in (D.11) as follows:

$$\left(x-\beta_{x-}\right)\left(x-\beta_{x+}\right)\leqslant 0, \tag{D.27}$$

where

$$\beta_{x\pm}:=\frac{2J^{\varepsilon}_{\min}\left(1-J^{\varepsilon}_{\min}\right)+2\varepsilon\left(1-\varepsilon\right)\pm 4\sqrt{\varepsilon\left(1-\varepsilon\right)J^{\varepsilon}_{\min}\left(1-J^{\varepsilon}_{\min}\right)}}{2\left(J^{\varepsilon}_{\min}-\varepsilon\right)^2} \tag{D.28}$$

$$= \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} \pm \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon} \right)^2 . \tag{D.29}$$

The inequality in (D.27) is satisfied if and only if $\beta_{x-} \leqslant x \leqslant \beta_{x+}$. Combining (D.10) and (D.27), we conclude that (D.8) is satisfied if and only if

$$k^2 - 1 \in \left[0, \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}\right] \cup [\beta_{x-}, \beta_{x+}] . \tag{D.30}$$

Recall that we had assumed $k^2 - 1 > \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$ to arrive at (D.11), and the inequality in (D.8) holds for all $0 \leqslant k^2 - 1 \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$. In what follows, we shall show that $\beta_{x-} \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \leqslant \beta_{x+}$ for all $\varepsilon < J^{\varepsilon}_{\min} \leqslant 1-\varepsilon$.

First, let us consider the following inequality:

$$\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} \leqslant \sqrt{\varepsilon(1-\varepsilon)} \tag{D.31}$$

$$\iff J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) \leqslant \varepsilon(1-\varepsilon) \tag{D.32}$$

$$\iff (J^{\varepsilon}_{\min})^2 - J^{\varepsilon}_{\min} + \varepsilon(1-\varepsilon) \geqslant 0. \tag{D.33}$$

The above inequality can be factored as follows:

$$(J^{\varepsilon}_{\min}-\varepsilon)(J^{\varepsilon}_{\min}-(1-\varepsilon)) \geqslant 0. \tag{D.34}$$

Therefore, the inequality in (D.31) is satisfied if and only if $J^{\varepsilon}_{\min} \leqslant \varepsilon$ or $J^{\varepsilon}_{\min} \geqslant 1-\varepsilon$, with the inequality being saturated if $J^{\varepsilon}_{\min} = \varepsilon$ or $J^{\varepsilon}_{\min} = 1-\varepsilon$. Thus, we conclude that the following inequality holds for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$:

$$\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} \geqslant \sqrt{\varepsilon(1-\varepsilon)}. \tag{D.35}$$

Now we prove that $\beta_{x-} \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$, provided that $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$. Consider that

$$\beta_{x-} \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \tag{D.36}$$

$$\iff \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon} \right)^2 \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \tag{D.37}$$

$$\iff \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)} \right)^2 \leqslant (J^{\varepsilon}_{\min}-\varepsilon)(1-\varepsilon-J^{\varepsilon}_{\min}) \tag{D.38}$$

$$\iff \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)} \right)^2 \leqslant J^{\varepsilon}_{\min} - (J^{\varepsilon}_{\min})^2 - \varepsilon + \varepsilon^2 \tag{D.39}$$

$$\iff \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)} \right)^2 \leqslant J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) - \varepsilon(1-\varepsilon) \tag{D.40}$$

$$\iff \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)} \leqslant \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}. \tag{D.41}$$

$$\iff 0 \leqslant 2\sqrt{\varepsilon(1-\varepsilon)}. \tag{D.42}$$

To arrive at the penultimate inequality, we have used the fact that

$$J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) - \varepsilon(1-\varepsilon) = \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)} \right) \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)} \right) . \tag{D.43}$$

Since the last inequality $0 \leqslant 2\sqrt{\varepsilon(1-\varepsilon)}$ holds trivially for $\varepsilon \in [0,1]$, we conclude that $\beta_{x-} \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$ for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$.

To show that $\beta_{x+} \geqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$, we consider the following inequality:

$$\beta_{x+} = \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon} \right)^2 \geqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}. \tag{D.44}$$

Following the same steps as before, the above inequality can be transformed into the following inequality:

$$\left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)}\right)^2 \geqslant J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})-\varepsilon(1-\varepsilon) \tag{D.45}$$

$$\iff \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)} \geqslant \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}-\sqrt{\varepsilon(1-\varepsilon)}, \tag{D.46}$$

which holds for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$ and $\varepsilon \in [0,1]$. Hence, we conclude the following:

$$\left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}-\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2 \leqslant \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \tag{D.47}$$

$$\leqslant \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2. \tag{D.48}$$

Recall from (D.30) that (D.8) is satisfied for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$ if and only if $k^2-1 \in \left[0, \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}\right] \cup [\beta_{x-}, \beta_{x+}]$. The inequalities in (D.47) and (D.48) further reveal that the inequality in (D.8) is satisfied for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$ if and only if the following condition holds:

$$0 \leqslant k^2-1 \leqslant \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2. \tag{D.49}$$

The quantity $\log_2 k$ is interpreted as the number of secret bits that can be distilled from the state ρ_{AB} using the one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$. Therefore, we rewrite the condition in (D.49) as the following upper bound on $\log_2 k$:

$$\log_2 k \leqslant \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2+1\right]. \tag{D.50}$$

Since the inequality in (D.50) holds for every integer $k \geqslant 2$, every private state $\gamma^k_{A'B'A''B''}$, and every one-way LOCC channels $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$, we conclude (94).

Appendix E. Proof of lemma 3

In this section we show that the following function:

$$f(J,\varepsilon) := \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right)^2+1\right] \tag{E.1}$$

decreases monotonically with increasing J and increases monotonically with increasing ε for all $\varepsilon \in [0,1]$ and $J \in (\varepsilon, 1-\varepsilon]$.

First, let us analyze the monotonicity of $f(J,\varepsilon)$ in J. The logarithm function is monotonic in its argument. Therefore, we only need to check the monotonicity of the following function:

$$g(J,\varepsilon) := \left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right)^2. \tag{E.2}$$

Note that the quantity $\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}$ is non-negative for all $\varepsilon < J \leqslant 1$ and $0 \leqslant \varepsilon \leqslant 1$. Therefore, $g(J,\varepsilon)$ is monotonic in J if $\sqrt{g(J,\varepsilon)}$ is monotonic in J in the given domain.

Let us compute the derivative of $\sqrt{g(J,\varepsilon)}$ with respect to J.

$$\frac{\mathrm{d}}{\mathrm{d}J}\sqrt{g(J,\varepsilon)} = \frac{1}{(J-\varepsilon)^2}\left((J-\varepsilon)\left(\frac{1}{2}\cdot\frac{1-2J}{\sqrt{J(1-J)}}\right)-\left(\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}\right)\right). \tag{E.3}$$

Set $h := J - \varepsilon$ so that $h \in (0, 1-2\varepsilon]$. The first term of the above expression can then be expressed as follows:

$$(J-\varepsilon)\left(\frac{1}{2}\cdot\frac{1-2J}{\sqrt{J(1-J)}}\right) = \frac{h(1-2h-2\varepsilon)}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{E.4}$$

$$= \frac{h(2-2h-2\varepsilon)}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} - \frac{h}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{E.5}$$

$$= \frac{h\sqrt{1-h-\varepsilon}}{\sqrt{h+\varepsilon}} - \frac{h}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{E.6}$$

$$\leqslant \sqrt{(h+\varepsilon)(1-h-\varepsilon)} - \frac{h}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{E.7}$$

$$= \sqrt{J(1-J)} - \frac{J-\varepsilon}{2\sqrt{J(1-J)}}, \tag{E.8}$$

where we have used the fact that $h \leqslant h+\varepsilon$ to arrive at the inequality. Substituting the above inequality in (E.3),

$$\frac{\mathrm{d}}{\mathrm{d}J}\sqrt{g(J,\varepsilon)} \leqslant \frac{1}{(J-\varepsilon)^2}\left(\sqrt{J(1-J)} - \frac{J-\varepsilon}{2\sqrt{J(1-J)}} - \sqrt{J(1-J)} - \sqrt{\varepsilon(1-\varepsilon)}\right) \tag{E.9}$$

$$= -\frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{J(1-J)}} + \sqrt{\varepsilon(1-\varepsilon)}\right), \tag{E.10}$$

which is negative for all $J \in (\varepsilon, 1-\varepsilon]$ and $\varepsilon \in [0,1]$. Therefore, $\sqrt{g(J,\varepsilon)}$ decreases monotonically with J in the given domain, and consequently, $f(J,\varepsilon)$ decreases monotonically with J in the same domain.

Now let us analyze the monotonicity of $f(J,\varepsilon)$ in ε. Once again, we only need to determine the monotonicity of $\sqrt{g(J,\varepsilon)}$ in ε to determine the monotonicity of $f(J,\varepsilon)$ in ε. Taking the derivative of $\sqrt{g(J,\varepsilon)}$, we arrive at the following equality:

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\sqrt{g(J,\varepsilon)} = \frac{\mathrm{d}}{\mathrm{d}\varepsilon}\left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right) \tag{E.11}$$

$$= \frac{1}{(J-\varepsilon)^2}\left((J-\varepsilon)\left(\frac{1}{2}\cdot\frac{1-2\varepsilon}{\sqrt{\varepsilon(1-\varepsilon)}}\right) + \sqrt{J(1-J)} + \sqrt{\varepsilon(1-\varepsilon)}\right) \tag{E.12}$$

$$= \frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{\varepsilon(1-\varepsilon)}} - \frac{\varepsilon(J-\varepsilon)}{\sqrt{\varepsilon(1-\varepsilon)}} + \sqrt{J(1-J)} + \sqrt{\varepsilon(1-\varepsilon)}\right) \tag{E.13}$$

$$= \frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{\varepsilon(1-\varepsilon)}} + \frac{\varepsilon(1-\varepsilon)-\varepsilon(J-\varepsilon)}{\sqrt{\varepsilon(1-\varepsilon)}} + \sqrt{J(1-J)}\right) \tag{E.14}$$

$$= \frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{\varepsilon(1-\varepsilon)}} + \frac{\varepsilon(1-J)}{\sqrt{\varepsilon(1-\varepsilon)}} + \sqrt{J(1-J)}\right). \tag{E.15}$$

The above expression is strictly positive for all $\varepsilon \in [0,1]$ and all $J \in (\varepsilon, 1-\varepsilon]$. Therefore, $\sqrt{g(J,\varepsilon)}$ is monotonically increasing in ε in the given domain, and consequently, $f(J,\varepsilon)$ is monotonically increasing in ε in the same domain.

Appendix F. Proof of proposition 6

In this section, we show that the smooth-min unextendible entanglement of a channel lies in the following range:

$$-\frac{1}{2}(1-\varepsilon) \leqslant E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}) \leqslant \log_2 d - \frac{1}{2}(1-\varepsilon). \tag{F.1}$$

The lower bound on the smooth-min unextendible entanglement can be obtained from proposition 2 and lemma 5. For every quantum state ρ_{RA},

$$E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}) \geqslant E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}(\rho_{RA})) \tag{F.2}$$

$$\geqslant -\frac{1}{2}\log_2(1-\varepsilon), \tag{F.3}$$

where the first inequality follows from lemma 5 and the second inequality follows from proposition 2.

To obtain an upper bound on the smooth-min unextendible entanglement of a channel, consider the smooth-min unextendible entanglement of the identity channel. Recall the inequality in (123). Setting $\rho \to \mathrm{id}_{A\to B}(\rho_{RA})$, $\sigma \to \mathcal{M}_{A\to E}(\rho_{RA})$, and $\alpha \to \infty$, we arrive at the following inequality:

$$D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}(\rho_{RA})\,\|\mathcal{M}_{A\to E}(\rho_{RA})) \leqslant D_{\max}(\mathrm{id}_{A\to B}(\rho_{RA})\,\|\mathcal{M}_{A\to E}(\rho_{RA})) - \log_2(1-\varepsilon), \tag{F.4}$$

where $\mathcal{M}_{A\to E}$ is an arbitrary quantum channel and systems B and E are isomorphic. Since the above inequality holds for every state ρ_{RA}, we can take a supremum over all states and arrive at the following inequality between the smooth-min relative entropy of channels and the max-relative entropy of channels:

$$D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\,\|\mathcal{M}_{A\to E}) \leqslant D_{\max}(\mathrm{id}_{A\to B}\,\|\mathcal{M}_{A\to E}) - \log_2(1-\varepsilon). \tag{F.5}$$

In [DFW+18, WBHK20], it was shown that the following equality holds for the max-relative entropy of channels:

$$D_{\max}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) = D_{\max}\left(\mathcal{N}_{A\to B}\left(\Phi^{d}_{RA}\right)\|\mathcal{M}_{A\to B}\left(\Phi^{d}_{RA}\right)\right), \tag{F.6}$$

where d is the dimension of the input system of the channel and Φ^{d}_{RA} is the maximally entangled state with Schmidt rank d. Therefore, we can rewrite (F.5) as follows:

$$D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\,\|\mathcal{M}_{A\to E}) \leqslant D_{\max}\left(\Phi^{d}_{RB}\|\mathcal{M}_{A\to E}\left(\Phi^{d}_{RA}\right)\right) - \log_2(1-\varepsilon). \tag{F.7}$$

Any channel that lies in the set $\mathcal{F}(\mathrm{id}_{A\to B})$ is a trace and replace channel; that is, it is of the following form:

$$\mathcal{M}_{A\to E}(\cdot) = \mathrm{Tr}[\cdot]\,\sigma_E, \tag{F.8}$$

where σ_E is a quantum state. Therefore, the inequality in (F.7) leads to the following inequality:

$$\begin{aligned}\inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\,\|\mathcal{M}_{A\to E}) &\leqslant \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} D_{\max}\left(\Phi^{d}_{RB}\|\mathcal{M}_{A\to E}\left(\Phi^{d}_{RA}\right)\right) - \log_2(1-\varepsilon) &\text{(F.9)}\\ &= \inf_{\sigma_E\in\mathcal{S}(E)} D_{\max}\left(\Phi^{d}_{RB}\|\pi_R\otimes\sigma_E\right) - \log_2(1-\varepsilon), &\text{(F.10)}\end{aligned}$$

where π_R is the maximally mixed state. Moreover, an arbitrary extension of the maximally entangled state is of the following form $\Phi^{d}_{AB}\otimes\tau_E$ because the maximally entangled state is a pure state. As such, every state in the set $\mathcal{F}\left(\Phi^{d}_{RB}\right)$ can be written as $\pi_R\otimes\tau_E$ for some $\tau_E\in\mathcal{S}(E)$. Therefore, the max-unextendible entanglement of the maximally entangled state can be written as follows:

$$\begin{aligned}E^{u}_{\max}\left(\Phi^{d}_{AB}\right) &= \inf_{\tau_E\in\mathcal{S}(E)} \frac{1}{2} D_{\max}\left(\Phi^{d}_{RB}\|\pi_R\otimes\tau_E\right) &\text{(F.11)}\\ &\geqslant \frac{1}{2} D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\,\|\mathcal{M}_{A\to E}) + \frac{1}{2}\log_2(1-\varepsilon) &\text{(F.12)}\\ &= E^{u,\varepsilon}_{\min}(\mathrm{id}_{A\to B}) + \frac{1}{2}\log_2(1-\varepsilon), &\text{(F.13)}\end{aligned}$$

where the first inequality follows from (F.10) and the last equality follows from the definition of smooth-min unextendible entanglement of channels.

The max-unextendible entanglement of a maximally entangled state with Schmidt rank d is equal to $\log_2 d$ as shown in [WWW24, proposition 11]. Therefore,

$$E^{u,\varepsilon}_{\min}(\mathrm{id}_{A\to B}) \leqslant \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \tag{F.14}$$

The converse of the above inequality is also true as lemma 5 implies the following inequality:

$$\begin{aligned}E^{\varepsilon,u}_{\min}(\mathrm{id}_{A\to B}) &\geqslant E^{\varepsilon,u}_{\min}\left(\mathrm{id}_{A\to B}\left(\Phi^{d}_{AB}\right)\right) &\text{(F.15)}\\ &= E^{\varepsilon,u}_{\min}\left(\Phi^{d}_{AB}\right) &\text{(F.16)}\\ &= \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), &\text{(F.17)}\end{aligned}$$

where the final equality follows from proposition 1. Therefore,

$$E_{\min}^{u,\varepsilon}(\mathrm{id}_{A\to B}) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \tag{F.18}$$

Since

$$E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}) \leqslant \min\{E_{\min}^{u,\varepsilon}(\mathrm{id}_{A\to C}), E_{\min}^{u,\varepsilon}(\mathrm{id}_{B\to D})\}, \tag{F.19}$$

where $\dim(A) = \dim(C)$ and $\dim(B) = \dim(D)$, we conclude the second inequality in the statement of the proposition.

Appendix G. Proof of proposition 7

In this section we derive an expression for the α-geometric unextendible entanglement of the d-dimensional erasure channel, for $\alpha \in (0,1)\cup(1,2]$. An upper bound on the α-geometric unextendible entanglement of the d-dimensional erasure channel was obtained in [SW24b, appendix J]. Here we show that the inequality stated in [SW24b] is, in fact, an equality.

Lemma 5 implies the following inequality:

$$\mathbf{E}^u\left(\mathcal{E}^p_{A\to B}\left(\Phi^d_{RA}\right)\right) = \mathbf{E}^u\left((1-p)\ \Phi^d_{AB} + p\frac{I_A}{d}\otimes|e\rangle\langle e|_B\right) \leqslant \mathbf{E}^u(\mathcal{E}^p_{A\to B}), \tag{G.1}$$

where Φ^d_{RA} is the maximally entangled state of Schmidt rank $d\in\mathbb{N}$, $|e\rangle$ is the erasure symbol, and $\mathcal{E}^p_{A\to B}$ is a d-dimensional erasure channel with erasure probability $p\in[0,1]$. The bipartite state obtained after sending one share of a maximally entangled state through an erasure channel is called an erased state, which we denote as follows:

$$\eta^p_{AB} := (1-p)\ \Phi^d_{AB} + p\frac{I_A}{d}\otimes|e\rangle\langle e|_B. \tag{G.2}$$

In what follows, we will obtain an analytical expression for the α-geometric unextendible entanglement of a d-dimensional erased state η^p_{AB} and show that it matches the upper bound on the α-geometric unextendible entanglement of the erasure channel $\mathcal{E}^p_{A\to B}$ obtained in [SW24b, appendix J]. The inequality in (G.1) then simply implies that the α-geometric unextendible entanglement of the erasure channel $\mathcal{E}^p_{A\to B}$ is equal to the α-geometric unextendible entanglement of the erased state η^p_{AB}, thus establishing the equality stated in proposition 7.

Let us analyze the generalized unextendible entanglement of an erased state. We will restrict our discussion to $p<\frac{1}{2}$ since $\widehat{E}^u_\alpha(\eta^p_{AB}) = 0$ for all $p\geqslant\frac{1}{2}$.

Lemma 6. *For $p\in[0,1/2)$, let η^p_{AB} be the erased state defined in (G.2). The generalized unextendible entanglement of the erased state is equal to the following:*

$$\mathbf{E}^u(\eta^p_{AB}) = \inf_{b\in[0,1-p]}\frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\|\omega^{p,b}_{AE'}\right), \tag{G.3}$$

where

$$\omega^{p,b}_{AB} = p\ \Phi^d_{AB} + b\ \frac{I_A\otimes\Pi_B}{d^2} + (1-p-b)\frac{I_A}{d}\otimes|e\rangle\langle e|_B \tag{G.4}$$

and

$$\Pi := |0\rangle\langle 0| + \cdots + |d-1\rangle\langle d-1|. \tag{G.5}$$

Proof. Let $\eta^p_{AB} := (1-p)\ \Phi^d_{AB} + p\frac{I_A}{d}\otimes|e\rangle\langle e|_B$ be an erased state. Consider the following purification of η^p_{AB}:

$$|\psi^\eta\rangle_{ABE} := \sqrt{1-p}|\Phi^d\rangle_{AB}\otimes|e\rangle_E + \sqrt{p}|\Phi^d\rangle_{AE}\otimes|e\rangle_B, \tag{G.6}$$

where systems B and E are isomorphic to each other. For clarity, we define the following projector:

$$\Pi := |0\rangle\langle 0| + \cdots + |d-1\rangle\langle d-1|, \tag{G.7}$$

which is the projector onto the subspace orthogonal to $|e\rangle\langle e|$. The maximally mixed state of a d-dimensional system is defined as $\pi := \frac{\Pi}{d}$. Since system A does not have any component of the erasure symbol, $I_A = \Pi_A$.

Using the correspondence between a purification and an extension of a state established in [CW04], we can write an arbitrary extension of the erased state as $\mathcal{N}_{E\to E'}(\psi^{\eta}_{ABE})$. Therefore, any state $\sigma_{AE'} \in \mathcal{F}(\eta^{p}_{AB})$ can be written as follows:

$$\begin{aligned}\sigma_{AE'} &= \mathrm{Tr}_B[\mathcal{N}_{E\to E'}(\psi^{\eta}_{ABE})] && \text{(G.8)}\\ &= \mathcal{N}_{E\to E'}(\mathrm{Tr}_B[\psi^{\eta}_{ABE}]) && \text{(G.9)}\\ &= \mathcal{N}_{E\to E'}\left((1-p)\,\pi_A \otimes |e\rangle\langle e|_E + p\,\Phi^{d}_{AE}\right) && \text{(G.10)}\\ &= (1-p)\,\pi_A \otimes \mathcal{N}_{E\to E'}(|e\rangle\langle e|_E) + p\,\mathcal{N}_{E\to E'}\left(\Phi^{d}_{AE}\right), && \text{(G.11)}\end{aligned}$$

where systems B, E, and E' are all isomorphic to each other.

Let us consider the following partially dephasing channel:

$$\Delta_{E'}(\cdot) = \Pi_{E'}(\cdot)\,\Pi_{E'} + |e\rangle\langle e|_{E'}(\cdot)\,|e\rangle\langle e|_{E'}. \tag{G.12}$$

Applying this dephasing channel on $\sigma_{AE'}$ leads to a state of the following form:

$$\Delta_{E'}(\sigma_{AE'}) = (1-x)\,\rho_{AE'} + x\pi_A \otimes |e\rangle\langle e|_{E'}, \tag{G.13}$$

where $x \in [0,1]$ and $\rho_{AE'}$ is a quantum state such that $\rho_{AE'}|e\rangle_{E'} = 0$.

Let U_A be an arbitrary unitary operator acting on the Hilbert space of system A. The corresponding operator acting on the Hilbert space of system E' has the following property:

$$U^{\dagger}_{E'}U_{E'} = U_{E'}U^{\dagger}_{E'} = \Pi_{E'}. \tag{G.14}$$

We can promote $U_{E'}$ to a unitary operator on the Hilbert space of system E' as follows:

$$V^{U}_{E'} = U_{E'} + |e\rangle\langle e|_{E'}. \tag{G.15}$$

Note that

$$V^{U}_{E'}\rho_{AE'}\left(V^{U}_{E'}\right)^{\dagger} = U_{E'}\rho_{AE'}U^{\dagger}_{E'}, \tag{G.16}$$

and

$$V^{U}_{E'}|e\rangle\langle e|_{E'}\left(V^{U}_{E'}\right)^{\dagger} = |e\rangle\langle e|_{E'}. \tag{G.17}$$

Now consider the following twirling channel:

$$\mathcal{T}_{AE'} := \int \mathrm{d}U\left(\overline{U}_A \otimes V^{U}_{E'}\right)(\cdot)\left(\overline{U}_A \otimes V^{U}_{E'}\right)^{\dagger}, \tag{G.18}$$

which can be implemented by local operations and common randomness (LOCR). The action of this twirling channel on the dephased state in (G.13) results in the following state:

$$\begin{aligned}\mathcal{T}_{AE'}\circ\Delta_{E'}(\sigma_{AE'}) &= (1-x)\,\mathcal{T}_{AE'}(\rho_{AE'}) + x\int \mathrm{d}U U_A\pi_A U^{\dagger}_A \otimes |e\rangle\langle e|_{E'} && \text{(G.19)}\\ &= (1-x)\int \mathrm{d}U\left(\overline{\mathcal{U}}_A \otimes \mathcal{U}_{E'}\right)(\rho_{AE'}) + x\pi_A \otimes |e\rangle\langle e|_{E'} && \text{(G.20)}\\ &= q\Phi^{d}_{AE'} + (1-q-x)\,\frac{\Pi_A\otimes\Pi_{E'} - \Phi^{d}_{AE'}}{d^2-1} + x\pi_A\otimes|e\rangle\langle e|_{E'}, && \text{(G.21)}\end{aligned}$$

where $q := (1-x)\,\mathrm{Tr}\left[\rho_{AE'}\Phi^{d}_{AE'}\right]$. In the above, the second equality follows from (G.16), and the final equality is a consequence of the following equality [HH99]:

$$\int \mathrm{d}U\left(\overline{\mathcal{U}}_A \otimes \mathcal{U}_{E'}\right)(\tau_{AE'}) = \mathrm{Tr}\left[\tau_{AE'}\Phi^{d}_{AE'}\right]\Phi^{d}_{AE'} + \mathrm{Tr}\left[\tau_{AE'}\left(\Pi_A\otimes\Pi_{E'} - \Phi^{d}_{AE'}\right)\right]\frac{\Pi_A\otimes\Pi_{E'} - \Phi^{d}_{AE'}}{d^2-1}, \tag{G.22}$$

which holds for every quantum state $\tau_{AE'}$. We can rewrite (G.21) as follows:

$$\omega^{a,b}_{AE'} := \mathcal{T}_{AE'}\circ\Delta_{E'}(\sigma_{AE'}) = a\,\Phi^{d}_{AE'} + b\,\pi_{AE'} + (1-a-b)\,\pi_A\otimes|e\rangle\langle e|_{E'}, \tag{G.23}$$

where $a = q - \frac{1-q-x}{d^2-1}$ and $b = \frac{(1-q-x)d^2}{d^2-1}$.

The generalized unextendible entanglement of the erased state can now be written as follows:

$$\mathbf{E}^{u}(\eta^{p}_{AB}) = \inf_{\sigma\in\mathcal{F}(\eta^{p})} \frac{1}{2}\mathbf{D}(\eta^{p}_{AB}\|\sigma_{AE'}) \tag{G.24}$$

$$\geqslant \inf_{\sigma\in\mathcal{F}(\eta^{p})} \frac{1}{2}\mathbf{D}(\mathcal{T}_{AB}\circ\Delta_{B}(\eta^{p}_{AB})\,\|\mathcal{T}_{AE'}\circ\Delta_{E'}(\sigma_{AE'})) \tag{G.25}$$

$$= \inf_{\sigma\in\mathcal{F}(\eta^{p})} \frac{1}{2}\mathbf{D}(\eta^{p}_{AB}\|\mathcal{T}_{AE'}\circ\Delta_{E'}(\sigma_{AE'}))\,, \tag{G.26}$$

where the inequality follows from the data-processing inequality of the generalized divergence and the final equality follows from the fact that the erased state is invariant under the action of the dephasing channel Δ_B as well as the twirling channel $\mathcal{T}_{AB}$. The inequality in (G.26) implies that for every state $\sigma_{AE'}\in\mathcal{F}(\eta^{p}_{AB})$ there exists a state $\omega^{a,b}_{AE'}$, defined in (G.23), such that

$$\frac{1}{2}\mathbf{D}(\eta^{p}_{AB}\|\sigma_{AE'}) \geqslant \frac{1}{2}\mathbf{D}\left(\eta^{p}_{AB}\|\omega^{a,b}_{AE'}\right). \tag{G.27}$$

Therefore, it suffices to restrict the infimum in (G.24) to the following optimization:

$$\mathbf{E}^{u}(\eta^{p}_{AB}) = \inf_{a\in\mathcal{A},b\in\mathcal{B}} \frac{1}{2}\mathbf{D}\left(\eta^{p}_{AB}\|\omega^{a,b}_{AE'}\right), \tag{G.28}$$

where sets $\mathcal{A}$ and $\mathcal{B}$ correspond to the sets of parameters a and b such that $\omega^{a,b}_{AE'}\in\mathcal{F}(\eta^{p}_{AB})$.

Now let us find the range of values that a and b can take such that $\omega^{a,b}_{AE'}$, defined in (G.23), lies in the set $\mathcal{F}(\eta^{p}_{AB})$. Note that

$$\omega^{a,b}_{AE'} = \mathcal{T}_{AE'}\circ\Delta_{E'}\circ\mathcal{N}_{E\to E'}\left(p\,\Phi^{d}_{AE} + (1-p)\,\pi_{A}\otimes|e\rangle\langle e|_{E}\right). \tag{G.29}$$

For every $\mathcal{N}_{E\to E'}$, the channel $\mathcal{T}_{AE'}\circ\Delta_{E'}\circ\mathcal{N}_{E\to E'}$ acts on $\pi_A\otimes|e\rangle\langle e|_E$ and Φ^{d}_{AE} as follows:

$$\mathcal{T}_{AE'}\circ\Delta_{E'}\circ\mathcal{N}_{E\to E'}(\pi_{A}\otimes|e\rangle\langle e|_{E}) = y\pi_{AE'} + (1-y)\,\pi_{A}\otimes|e\rangle\langle e|_{E'}, \tag{G.30}$$

$$\mathcal{T}_{AE'}\circ\Delta_{E'}\circ\mathcal{N}_{E\to E'}\left(\Phi^{d}_{AE}\right) = y'\Phi^{d}_{AE'} + y''\pi_{AE'} + (1-y'-y'')\,\pi_{A}\otimes|e\rangle\langle e|_{E'}, \tag{G.31}$$

where $y\in[0,1]$, $y'\in[0,1]$ and $y''\in[0,1-y']$. The state $\omega^{a,b}_{AE'}$ can hence be written as follows:

$$\omega^{a,b}_{AE'} = py'\,\Phi^{d}_{AE} + (y(1-p)+py'')\,\pi_{AE'} + ((1-y)(1-p)+p(1-y'-y''))\,\pi_{A}\otimes|e\rangle\langle e|_{E'}, \tag{G.32}$$

for some $y\in[0,1]$, $y'\in[0,1]$ and $y''\in[0,1-y']$. Comparing with (G.23), it is clear that $a\leqslant p$. Therefore, if $\omega^{a,b}_{AE'}\in\mathcal{F}(\eta^{p}_{AB})$, then a must be less than or equal to p.

Now we will show that $\omega^{a,b}_{AE'}\in\mathcal{F}(\eta^{p}_{AB})$ for all $a\in[0,p]$ and $b\in[0,1-a]$. Consider the following extension of the state $\omega^{a,b}_{AE'}$:

$$\omega^{a,b,c,g}_{ABE'} = \left(a\,\Phi^{d}_{AE'} + c\,\pi_{AE'}\right)\otimes|e\rangle\langle e|_{B} + \left(g\,\Phi^{d}_{AB} + f\,\pi_{AB}\right)\otimes|e\rangle\langle e|_{E'} + (b-c)\,\Phi^{d}_{AB}\otimes\pi_{E'}, \tag{G.33}$$

where $g+f=1-a-b$ and $a,b\geqslant 0$ follow from (G.23) and $c,g,f\geqslant 0$ and $c\leqslant b$ ensure that $\omega^{a,b,c,g}_{ABE'}$ is positive semi-definite. It can be easily verified that $\mathrm{Tr}_{B}\left[\omega^{a,b,c,g}_{ABE'}\right] = \omega^{a,b}_{AE'}$. Moreover, if $a+c=p$ and $f=0$, then $\mathrm{Tr}_{E'}\left[\omega^{a,b,c,g}_{ABE'}\right] = \eta^{p}_{AB}$ (and also $g+b-c=1-p$ as a consequence). Therefore, for all $a\in[0,p]$, there exists $b\in[0,1-a]$ such that $\omega^{a,b}_{AE'}\in\mathcal{F}(\eta^{p}_{AB})$. As such, $\omega^{a,b}_{AE'}\in\mathcal{F}(\eta^{p}_{AB})$ if and only if $a\in[0,p]$ and $b\in[0,1-a]$. Invoking (G.28), we can write the generalized unextendible entanglement of an erased state η^{p}_{AB} as follows:

$$\mathbf{E}^{u}(\eta^{p}_{AB}) = \inf_{\substack{a\in[0,p],\\ b\in[0,1-a]}} \frac{1}{2}\mathbf{D}\left(\eta^{p}_{AB}\|\omega^{a,b}_{AE'}\right). \tag{G.34}$$

Consider the following channel:

$$\mathcal{R}^{s}_{AE'}(\cdot) = |e\rangle\langle e|_{E'}(\cdot)\,|e\rangle\langle e|_{E'} + (1-s)\,\mathrm{Tr}[\Pi_{E'}(\cdot)\,\Pi_{E'}]\,\Phi^{d}_{AE'} + s\,\mathrm{id}_{AE'}(\Pi_{E'}(\cdot)\,\Pi_{E'}), \tag{G.35}$$

where $s\in[0,1]$. The channel $\mathcal{R}^{s}_{AE'}$ can be realized by applying the POVM $\{\Pi_{E'},|e\rangle\langle e|_{E'}\}$ on the state of system E'. If the outcome corresponding to the POVM element $\Pi_{E'}$ occurs, then the state is replaced by the maximally entangled state $\Phi^{d}_{AE'}$ with

probability $1-s$ and otherwise, with probability s, the identity channel is applied. The erased state $\eta^p_{AE'}$ is invariant under the action of the channel $\mathcal{R}^s_{AE'}$ for all $s \in [0,1]$. The channel $\mathcal{R}^s_{AE'}$ acts on $\omega^{a,b}_{AE'}$ as follows:

$$\mathcal{R}^s_{AE'}\left(\omega^{a,b}_{AE'}\right) = ((1-s)\,b+a)\,\Phi^d_{AE'} + sb\,\pi_{AE'} + (1-a-b)\,\pi_A \otimes |e\rangle\langle e|_{E'} \tag{G.36}$$

$$= \omega^{a+(1-s)b,sb}_{AE'}. \tag{G.37}$$

Fix $s = (a+b-p)/b$. The data-processing inequality of the generalized divergence yields the following inequality:

$$\mathbf{D}\left(\eta^p_{AB}\|\omega^{a,b}_{AE'}\right) \geqslant \mathbf{D}\left(\mathcal{R}^s_{AB}(\eta^p_{AB})\,\|\mathcal{R}^s_{AE'}\left(\omega^{a,b}_{AE'}\right)\right) \tag{G.38}$$

$$= \mathbf{D}\left(\eta^p_{AB}\|\omega^{a+(1-s)b,sb}_{AE'}\right) \tag{G.39}$$

$$= \mathbf{D}\left(\eta^p_{AB}\|\omega^{p,a+b-p}_{AE'}\right). \tag{G.40}$$

If $\omega^{a,b}_{AE'} \in \mathcal{F}(\eta^p_{AB})$, then $\omega^{p,a+b-p}_{AE'}$ also lies in set $\mathcal{F}(\eta^p_{AB})$. Therefore, the bivariate infimum in (G.34) can be restricted to a single variable infimum as follows:

$$\mathbf{E}^u(\eta^p_{AB}) = \inf_{b\in[0,1-p]} \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\|\omega^{p,b}_{AE'}\right). \tag{G.41}$$

This concludes the proof. □

Lemma 6 allows us to obtain an analytical expression for the α-geometric unextendible entanglement of the erased state, which we present in proposition 8 stated below.

Proposition 8. *For all $\alpha \in (0,1)\cup(1,2]$, the α-geometric unextendible entanglement of a d-dimensional erased state η^p_{AB}, defined in lemma 6, evaluates to the following:*

$$\widehat{E}^u_\alpha(\eta^p_{AB}) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(\left(p+\frac{b_{\text{opt}}}{d^2}\right)^{1-\alpha}(1-p)^\alpha + (1-p-b_{\text{opt}})^{1-\alpha}p^\alpha\right) \tag{G.42}$$

for all $p \in \left(0, \frac{1}{d^{1/\alpha}+1}\right]$, where

$$b_{\text{opt}} := \frac{d^2\left((1-p)^2 - p^2d^{2/\alpha}\right)}{pd^{2/\alpha} + (1-p)\,d^2}. \tag{G.43}$$

For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}^u_\alpha(\eta^p_{AB}) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(p^{1-\alpha}(1-p)^\alpha + (1-p)^{1-\alpha}p^\alpha\right). \tag{G.44}$$

Proof. The α-geometric unextendible entanglement of the erased state can be computed using lemma 6 as follows:

$$\widehat{E}^u_\alpha(\eta^p_{AB}) = \inf_{b\in[0,1-p]} \frac{1}{2}\widehat{D}_\alpha\left(\eta^p_{AB}\|\omega^{p,b}_{AB}\right), \tag{G.45}$$

where $\omega^{p,b}_{AB}$ is defined in (G.4) and $\alpha \in (0,1)\cup(1,2]$. Recall the definition of the α-geometric Rényi relative entropy given in (194). The α-geometric Rényi relative entropy of η^p_{AB} with respect to $\omega^{p,b}_{AB}$ can be computed as follows:

$$\widehat{D}_\alpha\left(\eta^p_{AB}\|\omega^{p,b}_{AB}\right) = \frac{1}{\alpha-1}\log_2\left(\left(p+\frac{b}{d^2}\right)^{1-\alpha}(1-p)^\alpha + (1-p-b)^{1-\alpha}p^\alpha\right). \tag{G.46}$$

The above expression is minimized for

$$b = b_{\text{opt}} := \frac{d^2\left((1-p)^2 - p^2d^{2/\alpha}\right)}{pd^{2/\alpha} + (1-p)\,d^2}. \tag{G.47}$$

Let us now find the range of p such that $b_{\text{opt}} \in [0, 1-p]$. Consider the following expression:

$$1 - p - b_{\text{opt}} = \frac{pd^{2/\alpha}\left(1 - p + pd^2\right)}{pd^{2/\alpha} + (1-p)d^2}. \tag{G.48}$$

The above expression is greater than or equal to zero for all $p \in [0,1]$. Therefore, $b_{\text{opt}} \leqslant 1-p$ for all $p \in [0,1]$. Moreover, $b_{\text{opt}} \geqslant 0$ if and only if $0 \leqslant (1-p)^2 - p^2 d^{2/\alpha}$, which holds for all $p \in \left[0, \frac{1}{d^{1/\alpha}+1}\right)$. If $b_{\text{opt}} \leqslant 0$, the value of $b \in [0, 1-p]$ that minimizes the expression in (G.46) is $b = 0$. Therefore, for all $\alpha \in (0,1) \cup (1,2]$, the α-geometric unextendible entanglement of a d-dimensional erased state η^p_{AB} evaluates to the following:

$$\widehat{E}^u_\alpha(\eta^p_{AB}) = \frac{1}{2} \cdot \frac{1}{\alpha - 1} \log_2 \left(\left(p + \frac{b_{\text{opt}}}{d^2} \right)^{1-\alpha} (1-p)^\alpha + (1 - p - b_{\text{opt}})^{1-\alpha} p^\alpha \right) \tag{G.49}$$

for all $p \in \left(0, \frac{1}{d^{1/\alpha}+1}\right]$, where b_{opt} is defined in (G.47). For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}^u_\alpha(\eta^p_{AB}) = \frac{1}{2} \cdot \frac{1}{\alpha - 1} \log_2 \left(p^{1-\alpha} (1-p)^\alpha + (1-p)^{1-\alpha} p^\alpha \right). \tag{G.50}$$

This concludes the proof. □

Proof of proposition 7. The α-geometric unextendible entanglement of the erased state serves as a lower bound on the α-geometric unextendible entanglement of the erasure channel, as is evident from (G.1). The expression for the α-geometric unextendible entanglement of the erased state η^p_{AB} derived in proposition 8 was found to be an upper bound on the α-geometric unextendible entanglement of a d-dimensional erasure channel with erasure probability p. We give a brief outline of the proof here.

Consider a quantum channel $\mathcal{P}^{b^*}_{A\to BE}$ with the following Choi operator:

$$\Gamma^{\mathcal{P},b^*}_{ABE} = pd\, \Phi^d_{AE} \otimes |e\rangle\langle e|_B + (1 - p - b^*)\, d\, \Phi^d_{AB} \otimes |e\rangle\langle e|_E + b^* d\, \Phi^d_{AB} \otimes \pi_E. \tag{G.51}$$

The two relevant marginals of this Choi operator are as follows:

$$\Gamma^{\mathcal{E}}_{AB} = d\left((1-p)\, \Phi^d_{AB} + p\, \pi_A \otimes |e\rangle\langle e|_B\right), \tag{G.52}$$

which is the Choi operator of a d-dimensional erasure channel with erasure probability p, and

$$\Gamma^{\mathcal{M},b^*}_{AE} = d\left(p\, \Phi^d_{AE} + (1 - p - b^*)\, \pi_A \otimes |e\rangle\langle e|_E + b^* \pi_{AE}\right). \tag{G.53}$$

The Choi operator $\Gamma^{\mathcal{M},b^*}_{AE}$ corresponds to a channel $\mathcal{M}^{b^*}_{A\to E}$ that lies in the set $\mathcal{F}(\mathcal{E}^p_{A\to B})$ if $b^* \in [0, 1-p]$, where $\mathcal{E}^p_{A\to B}$ is a d-dimensional erasure channel with erasure probability p. By definition,

$$\widehat{E}^u_\alpha(\mathcal{E}^p_{A\to B}) \leqslant \frac{1}{2} \widehat{D}_\alpha \left(\mathcal{E}^p_{A\to B} \| \mathcal{M}^{b^*}_{A\to E} \right) \tag{G.54}$$

for all $b^* \in [0, 1-p]$. Choosing $b^* = \min\{0, b_{\text{opt}}\}$, where b_{opt} is defined in (G.47), the α-geometric Rényi relative entropy of $\mathcal{E}^p_{A\to B}$ with respect to $\mathcal{M}^{b^*}_{A\to E}$ evaluates to the expression which is equal to the α-geometric unextendible entanglement of the erased state η^p_{AB} derived in proposition 8. Since the α-geometric unextendible entanglement of the erasure channel $\mathcal{E}^p_{A\to B}$ cannot be less than the α-geometric unextendible entanglement of the erased state η^p_{AB}, we conclude that the two quantities are equal. □

Appendix H. Semidefinite programs

In this section we present all the semidefinite programs that were used in this work.

1. **Smooth-min unextendible entanglement of a state:**

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) = -\frac{1}{2} \log_2 \max \left\{ \begin{array}{c} \mu(1-\varepsilon) - \text{Tr}[Z_{AB}] : \\ \mu \geqslant 0, Z_{AB} \geqslant 0, \omega_{ABE} \geqslant 0, \\ \mu \rho_{AB} \leqslant \text{Tr}_B[\omega_{ABE}] + Z_{AB}, \\ \text{Tr}_E[\omega_{ABE}] = \rho_{AB} \end{array} \right\}. \tag{H.1}$$

2. **Max-unextendible entanglement of a state:** The semidefinite program for the max-unextendible entanglement of a state was given in [WWW24]. We include it here for completeness.

$$E^{u}_{\max}(\rho_{AB}) = -\frac{1}{2}\log_2 \max\left\{ \begin{array}{c} \lambda : \\ \lambda\rho_{AB} \leqslant \mathrm{Tr}_B[\omega_{ABE}], \\ \omega_{ABE} \geqslant 0, \\ \mathrm{Tr}_E[\omega_{ABE}] = \rho_{AB} \end{array} \right\}. \tag{H.2}$$

3. **Smooth-min unextendible entanglement of a channel:** The smooth-min relative entropy of a channel $\mathcal{N}$ with respect to a channel $\mathcal{M}$ has a semidefinite program, which was given in [WW19b, proposition 2]. We use it to write the semidefinite program for smooth-min unextendible entanglement of a channel as follows:

$$E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) = -\frac{1}{2}\log_2 \max\left\{ \begin{array}{c} \mu(1-\varepsilon) - \lambda : \\ \lambda \geqslant 0, \mu \geqslant 0, Y_{AB} \geqslant 0, \Gamma^{\mathcal{P}}_{ABE} \geqslant 0, \\ \mu\Gamma^{\mathcal{N}}_{AB} \leqslant \mathrm{Tr}_B\left[\Gamma^{\mathcal{P}}_{AB}\right] + Y_{AB} \\ \mathrm{Tr}_B[Y_{AB}] \leqslant \lambda I_A, \\ \mathrm{Tr}_E\left[\Gamma^{\mathcal{P}}_{ABE}\right] = \Gamma^{\mathcal{N}}_{AB} \end{array} \right\}, \tag{H.3}$$

where $\Gamma^{\mathcal{N}}_{AB}$ is the Choi operator of the channel $\mathcal{N}_{A\to B}$ defined in (3).

4. **α-geometric unextendible entanglement of a channel:** Fix $\ell \in \mathbb{N}$. The α-geometric unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ for $\alpha = 1 + 2^{-\ell}$ can be computed using the following semidefinite program:

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) = 2^{\ell} \min_{\substack{y\in\mathbb{R}, \Gamma^{\mathcal{P}}_{ABE}\geqslant 0 \\ M_{AE}, \{N^i_{AE}\}_{i=0}^{\ell}, \in \mathrm{Herm}}} \log_2 y, \tag{H.4}$$

subject to the constraints,

$$\mathrm{Tr}_E\left[\Gamma^{\mathcal{P}}_{ABE}\right] = \Gamma^{\mathcal{N}}_{AB}, \tag{H.5}$$

$$\mathrm{Tr}_E\left[M_{AE}\right] \leqslant y I_A, \tag{H.6}$$

$$\mathrm{Tr}_B\left[\Gamma^{\mathcal{P}}_{ABE}\right] = N^0_{AE}, \tag{H.7}$$

$$\begin{bmatrix} M_{AE} & \Gamma^{\mathcal{N}}_{AB} \\ \Gamma^{\mathcal{N}}_{AB} & N^{\ell}_{AE} \end{bmatrix} \geqslant 0, \tag{H.8}$$

$$\begin{bmatrix} \Gamma^{\mathcal{N}}_{AE} & N^{i}_{AE} \\ N^{i}_{AE} & N^{i-1}_{AE} \end{bmatrix} \geqslant 0 \quad \forall i \in \{1,2,\ldots,\ell\}, \tag{H.9}$$

where $\Gamma^{\mathcal{N}}_{AB}$ is the Choi operator of the channel $\mathcal{N}_{A\to B}$ and the system E is isomorphic to the system B. To compute the α-geometric unextendible entanglement of the channel for other rational values of α see [FS17, table 4].

Appendix I. Proof of proposition 4

In this section, we evaluate the smooth-min relative entropy of entanglement of isotropic states.

Consider an arbitrary d-dimensional isotropic state $\zeta^{F,d}_{AB}$. Let $\mathcal{T}_{AB}$ be the twirling channel defined in (68). Recall from (69) that this twirling channel transforms an arbitrary quantum state into an isotropic state. Also, an isotropic state is invariant under the action of $\mathcal{T}_{AB}$. Let σ_{AB} be an arbitrary quantum state. Then the following inequality holds:

$$D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB} \| \sigma_{AB}\right) \geqslant D^{\varepsilon}_{\min}\left(\mathcal{T}_{AB}\left(\zeta^{F,d}_{AB}\right) \| \mathcal{T}_{AB}(\sigma_{AB})\right) \tag{I.1}$$

$$= D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB} \| \zeta^{F',d}_{AB}\right) \tag{I.2}$$

for some $F' \in [0,1]$, where we have used the data-processing inequality for smooth-min relative entropy to arrive at the inequality in (I.1) and we have used (69) to arrive at the equality in (I.2).

The channel $\mathcal{T}_{AB}$ can be implemented using local operations and common randomness, and hence, $\mathcal{T}_{AB}$ transforms an arbitrary separable state σ_{AB} into a separable isotropic state $\zeta^{F',d}_{AB}$. It is known from [HH99, section V] that an isotropic state $\zeta^{F',d}_{AB}$ is separable if and only if $F' \leqslant \frac{1}{d}$. Therefore, for every separable state σ_{AB}, the following inequality holds:

$$D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB} \| \sigma_{AB}\right) \geqslant D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB} \| \zeta^{F',d}_{AB}\right) \tag{I.3}$$

for some $F' \in \left[0, \frac{1}{d}\right]$. Since the above inequality holds for every separable state σ_{AB}, we can evaluate the smooth-min relative entropy of entanglement of an isotropic state by optimizing over separable isotropic states only. That is,

$$E_R^\varepsilon\left(\zeta_{AB}^{F,d}\right) = \inf_{F' \in \left[0, \frac{1}{d}\right]} D_{\min}^\varepsilon\left(\zeta_{AB}^{F,d} \| \zeta_{AB}^{F',d}\right). \tag{I.4}$$

Using the definition of $D_{\min}^\varepsilon$ from (39), we can write the smooth-min relative entropy of entanglement of an isotropic state as follows:

$$E_R^\varepsilon\left(\zeta_{AB}^{F,d}\right) = \inf_{F' \in \left[0, \frac{1}{d}\right]} -\log_2 \inf_{0 \leqslant \Lambda_{AB} \leqslant I_{AB}} \left\{ \operatorname{Tr}\left[\Lambda_{AB} \zeta_{AB}^{F',d}\right] : \operatorname{Tr}\left[\Lambda_{AB} \zeta_{AB}^{F,d}\right] \geqslant 1 - \varepsilon \right\}. \tag{I.5}$$

If $1 - \varepsilon \leqslant F$, we can choose $\Lambda_{AB} = \frac{1-\varepsilon}{F} \Phi_{AB}^d$ to arrive at the following inequality:

$$\begin{aligned} E_R^\varepsilon\left(\zeta_{AB}^{F,d}\right) &\geqslant \inf_{F' \in \left[0, \frac{1}{d}\right]} -\log_2\left(\frac{1-\varepsilon}{F} F'\right) && \text{(I.6)} \\ &= -\log_2\left(\frac{1-\varepsilon}{F}\right) - \sup_{F' \in \left[0, \frac{1}{d}\right]} \log_2 F' && \text{(I.7)} \\ &= -\log_2\left(\frac{1-\varepsilon}{F}\right) + \log_2 d, && \text{(I.8)} \end{aligned}$$

where the final equality follows from the monotonicity of the logarithm function.

If $1 - \varepsilon > F$, we can choose Λ to be the following:

$$\Lambda_{AB} = \Phi_{AB}^d + \frac{1 - \varepsilon - F}{1 - F}\left(I_{AB} - \Phi_{AB}^d\right), \tag{I.9}$$

which is a valid measurement operator with $\operatorname{Tr}\left[\Lambda_{AB} \zeta_{AB}^{F,d}\right] = 1 - \varepsilon$. This choice of Λ yields the following lower bound on the smooth-min relative entropy of entanglement of an isotropic state:

$$\begin{aligned} E_R^\varepsilon\left(\zeta_{AB}^{F,d}\right) &\geqslant \inf_{F' \in \left[0, \frac{1}{d}\right]} -\log_2\left(F' + \frac{1 - \varepsilon - F}{1 - F}(1 - F')\right) && \text{(I.10)} \\ &= -\log_2 \sup_{F' \in \left[0, \frac{1}{d}\right]} \left\{ F'\left(1 - \frac{1 - \varepsilon - F}{1 - F}\right) + \frac{1 - \varepsilon - F}{1 - F} \right\} && \text{(I.11)} \\ &= -\log_2 \sup_{F' \in \left[0, \frac{1}{d}\right]} \left\{ (F' - 1)\left(\frac{\varepsilon}{1 - F}\right) + 1 \right\} && \text{(I.12)} \\ &= -\log_2\left(\left(\frac{1}{d} - 1\right)\left(\frac{\varepsilon}{1 - F}\right) + 1\right) && \text{(I.13)} \\ &= -\log_2\left(1 - \left(1 - \frac{1}{d}\right)\frac{\varepsilon}{1 - F}\right). && \text{(I.14)} \end{aligned}$$

Combining (I.8) and (I.14), we arrive at the following lower bound on the smooth-min relative entropy of entanglement of an isotropic state:

$$E_R^\varepsilon\left(\zeta_{AB}^{F,d}\right) \geqslant \begin{cases} -\log_2\left(1 - \left(1 - \frac{1}{d}\right)\frac{\varepsilon}{1-F}\right) & \text{if } 1 - \varepsilon \geqslant F \\ \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) & \text{otherwise} \end{cases}. \tag{I.15}$$

Let us now find an upper bound on the smooth-min relative entropy of entanglement of an isotropic state. Using the SDP formulation of the smooth-min relative entropy from [WW19a, equation (B2)], we can write the smooth-min relative entropy of entanglement of isotropic states as follows:

$$\begin{aligned} E_R^\varepsilon\left(\zeta_{AB}^{F,d}\right) &= \inf_{F' \in \left[0, \frac{1}{d}\right]} -\log_2 \sup_{\mu \geqslant 0, X_{AB} \geqslant 0} \left\{ \mu(1 - \varepsilon) - \operatorname{Tr}[X_{AB}] : \mu \zeta_{AB}^{F,d} \leqslant \zeta_{AB}^{F',d} + X_{AB} \right\} && \text{(I.16)} \\ &= -\log_2 \sup_{\substack{F' \in \left[0, \frac{1}{d}\right], \\ \mu \geqslant 0, X_{AB} \geqslant 0}} \left\{ \mu(1 - \varepsilon) - \operatorname{Tr}[X_{AB}] : \mu \zeta_{AB}^{F,d} \leqslant \zeta_{AB}^{F',d} + X_{AB} \right\}, && \text{(I.17)} \end{aligned}$$

where the last equality follows from the monotonicity of the logarithm function. The following choice constitutes a feasible point of the SDP in (I.17):

$$F' = \frac{1}{d}, \quad \mu = \frac{d-1}{d(1-F)}, \quad X_{AB} = \frac{Fd-1}{d(1-F)}\Phi^d_{AB}. \tag{I.18}$$

Clearly $\mu \geqslant 0$ for every $d \geqslant 1$, and $X_{AB} \geqslant 0$ since we have assumed $F > \frac{1}{d}$. Also, $\mu\zeta^{F,d}_{AB} = \zeta^{F',d}_{AB} + X_{AB}$ as we see below:

$$\begin{aligned}
\mu\zeta^{F,d}_{AB} &= \frac{d-1}{d(1-F)} F\,\Phi^d_{AB} + \frac{d-1}{d(1-F)}(1-F)\frac{I_{AB}-\Phi^d_{AB}}{d^2-1} && \text{(I.19)}\\
&= \left(\frac{d-1}{d(1-F)}F + \frac{1}{d} - \frac{1}{d}\right)\Phi^d_{AB} + \frac{d-1}{d}\frac{I_{AB}-\Phi^d_{AB}}{d^2-1} && \text{(I.20)}\\
&= \frac{1}{d}\Phi^d_{AB} + \left(1-\frac{1}{d}\right)\frac{I_{AB}-\Phi^d_{AB}}{d^2-1} + \frac{Fd-1}{d(1-F)}\Phi^d_{AB} && \text{(I.21)}\\
&= \zeta^{\frac{1}{d},d}_{AB} + \frac{Fd-1}{d(1-F)}\Phi^d_{AB}. && \text{(I.22)}
\end{aligned}$$

Therefore, we can write the following upper bound on the smooth-min relative entropy of entanglement:

$$\begin{aligned}
E^{\varepsilon}_R\left(\zeta^{F,d}_{AB}\right) &\leqslant -\log_2\left(\frac{d-1}{d(1-F)}(1-\varepsilon) - \frac{Fd-1}{d(1-F)}\right) && \text{(I.23)}\\
&= \log_2\left(\frac{\varepsilon(1-d)+d(1-F)}{d(1-F)}\right) && \text{(I.24)}\\
&= -\log_2\left(1 - \frac{\varepsilon}{1-F}\left(1-\frac{1}{d}\right)\right). && \text{(I.25)}
\end{aligned}$$

The argument of logarithm in the above function expression is always positive if $1-\varepsilon \geqslant F$, and it matches with the lower bound on the smooth-min relative entropy of entanglement of an isotropic state obtained in (I.14).

If $1-\varepsilon < F$, then we can choose the following feasible point of the SDP in (I.17):

$$F' = \frac{1}{d}, \quad \mu = \frac{1}{\mathrm{d}F}, \quad X_{AB} = 0, \tag{I.26}$$

which leads to the following inequality:

$$\begin{aligned}
E^{\varepsilon}_R\left(\zeta^{F,d}_{AB}\right) &\leqslant -\log_2\left(\frac{1-\varepsilon}{Fd}\right) \qquad \text{if } 1-\varepsilon < F && \text{(I.27)}\\
&= \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) \qquad \text{if } 1-\varepsilon < F. && \text{(I.28)}
\end{aligned}$$

We can combine the inequalities in (I.25) and (I.28) to write the following inequality:

$$E^{\varepsilon}_R\left(\zeta^{F,d}_{AB}\right) \leqslant \begin{cases} -\log_2\left(1-\left(1-\frac{1}{d}\right)\frac{\varepsilon}{1-F}\right) & \text{if } 1-\varepsilon \geqslant F \\ \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) & \text{otherwise} \end{cases}. \tag{I.29}$$

Since the upper bound on the smooth-min relative entropy of entanglement of an isotropic state matches with the lower bound in (I.15), we conclude the statement of proposition 4.

ORCID iDs

Vishal Singh https://orcid.org/0000-0003-2152-0614
Mark M Wilde https://orcid.org/0000-0002-3916-4462

References

[BB84] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (India)* p 175

[BD10] Buscemi F and Datta N 2010 The quantum capacity of channels with arbitrarily correlated noise *IEEE Trans. Inf. Theory* **56** 1447–60

[BD11] Brandao F G S L and Datta N 2011 One-shot rates for entanglement manipulation under non-entangling maps *IEEE Trans. Inf. Theory* **57** 1754–60

[BS82] Belavkin V P and Staszewski P 1982 C*-algebraic generalization of relative entropy and entropy *Ann. Inst. Henri Poincare Phys. Theor.* **37** 51–58

[CDP08] Chiribella G, D'Ariano G M and Perinotti P 2008 Transforming quantum operations: quantum supermaps *Europhys. Lett.* **83** 30004

[CEH+07] Christandl M, Ekert A, Horodecki M, Horodecki P, Oppenheim J and Renner R 2007 Unifying classical and quantum key distillation *Theory of Cryptography* ed S P Vadhan (Springer) pp 456–78

[Chr06] Christandl M 2006 The structure of bipartite quantum states—insights from group theory and cryptography (arXiv:quant-ph/0604183)

[CMW16] Cooney T, Mosonyi M and Wilde M M 2016 Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication *Commun. Math. Phys.* **344** 797–829

[CSW12] Christandl M, Schuch N and Winter A 2012 Entanglement of the antisymmetric state *Commun. Math. Phys.* **311** 397–422

[CW04] Christandl M and Winter A 2004 "Squashed entanglement": an additive entanglement measure *J. Math. Phys.* **45** 829–40

[CWY04] Cai N, Winter A and Yeung R W 2004 Quantum privacy and quantum wiretap channels *Problems Inf. Transm.* **40** 318–36

[Dat09] Datta N 2009 Min- and max-relative entropies and a new entanglement monotone *IEEE Trans. Inf. Theory* **55** 2816–26

[DFW+18] Díaz M G, Fang K, Wang X, Rosati M, Skotiniotis M, Calsamiglia J and Winter A 2018 Using and reusing coherence to realize quantum processes *Quantum* **2** 100

[DKQ+23] Ding D, Khatri S, Quek Y, Shor P W, Wang X and Wilde M M 2023 Bounding the forward classical capacity of bipartite quantum channels *IEEE Trans. Inf. Theory* **69** 3034–61

[DLL03] Deng F-G, Lu Long G and Liu X-S 2003 Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block *Phys. Rev.* A **68** 042317

[DPS04] Doherty A C, Parrilo P A and Spedalieri F M 2004 Complete family of separability criteria *Phys. Rev.* A **69** 022308

[DW05] Devetak I and Winter A 2005 Distillation of secret key and entanglement from quantum states *Proc. R. Soc.* A **461** 207–35

[Eke91] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3

[FF21] Fang K and Fawzi H 2021 Geometric Rényi divergence and its applications in quantum channel capacities *Commun. Math. Phys.* **384** 1615–77

[FS17] Fawzi H and Saunderson J 2017 Lieb's concavity theorem, matrix geometric means and semidefinite optimization *Linear Algebr. Appl.* **513** 240–63

[FvdG99] Fuchs C A and van de Graaf J 1999 Cryptographic distinguishability measures for quantum-mechanical states *IEEE Trans. Inf. Theory* **45** 1216–27

[Gha10] Gharibian S 2010 Strong NP-hardness of the quantum separability problem *Quantum Inf. Comput.* **10** 343–60

[Gou19] Gour G 2019 Comparison of quantum channels by superchannels *IEEE Trans. Inf. Theory* **65** 5880–904

[Gur03] Gurvits L 2003 Classical deterministic complexity of Edmonds' problem and quantum entanglement *Proc. 35th Annual ACM Symp. on Theory of Computing, STOC '03 (New York, NY, USA)* (Association for Computing Machinery) pp 10–19

[HH99] Horodecki M and Horodecki P 1999 Reduction criterion of separability and limits for a class of distillation protocols *Phys. Rev.* A **59** 4206–16

[HHH+08a] Horodecki K, Horodecki M, Horodecki P, Leung D and Oppenheim J 2008 Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity *IEEE Trans. Inf. Theory* **54** 2604–20

[HHH+08b] Horodecki K, Horodecki M, Horodecki P, Leung D and Oppenheim J 2008 Unconditional privacy over channels which cannot convey quantum information *Phys. Rev. Lett.* **100** 110502

[HHHO05] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Secure key from bound entanglement *Phys. Rev. Lett.* **94** 160502

[HHHO09] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2009 General paradigm for distilling classical key from quantum states *IEEE Trans. Inf. Theory* **55** 1898–929

[HMZ16] Heinosaari T, Miyadera T and Ziman M 2016 An invitation to quantum incompatibility *J. Phys. A: Math. Theor.* **49** 123001

[HSW23] Holdsworth T, Singh V and Wilde M M 2023 Quantifying the performance of approximate teleportation and quantum error correction via symmetric 2-PPT-extendible channels *Phys. Rev.* A **107** 012428

[KDWW19] Kaur E, Das S, Wilde M M and Winter A 2019 Extendibility limits the performance of quantum processors *Phys. Rev. Lett.* **123** 070502

[KDWW21] Kaur E, Das S, Wilde M M and Winter A 2021 Resource theory of unextendibility and nonasymptotic quantum capacity *Phys. Rev.* A **104** 022401

[KKGW21] Khatri S, Kaur E, Guha S and Wilde M M 2021 Second-order coding rates for key distillation in quantum key distribution (arXiv:1910.03883)

[KS24] Koßmann G and Schwonnek R 2024 Optimising the relative entropy under semi definite constraints—a new tool for estimating key rates in QKD (arXiv:2404.17016)

[KW24] Khatri S and Wilde M M 2024 Principles of quantum communication theory: a modern approach (arXiv:2011.04672v2)
[LDS18] Leditzky F, Datta N and Smith G 2018 Useful states and entanglement distillation *IEEE Trans. Inf. Theory* **64** 4689–708
[LKDW18] Leditzky F, Kaur E, Datta N and Wilde M M 2018 Approaches for approximate additivity of the Holevo information of quantum channels *Phys. Rev.* A **97** 012332
[LM15] Leung D and Matthews W 2015 On the power of PPT-preserving and non-signalling codes *IEEE Trans. Inf. Theory* **61** 4486–99
[Mat13] Matsumoto K 2013 A new quantum version of f-divergence (arXiv:1311.4722)
[MH11] Mosonyi M and Hiai F 2011 On the quantum Rényi relative entropies and related capacity formulas *IEEE Trans. Inf. Theory* **57** 2474–87
[MLDS+13] Müller-Lennert M, Dupuis F'eric, Szehr O, Fehr S and Tomamichel M 2013 On quantum Rényi entropies: a new generalization and some properties *J. Math. Phys.* **54** 122203
[MO21] Mosonyi M and Ogawa T 2021 Divergence radii and the strong converse exponent of classical-quantum channel coding with constant compositions *IEEE Trans. Inf. Theory* **67** 1668–98
[NIS] NISO 2024 Credit—contributor roles taxonomy (available at: https://credit.niso.org/) (Accessed 14 October 2024)
[NO00] Nagaoka H and Ogawa T 2000 Strong converse and Stein's lemma in quantum hypothesis testing *IEEE Trans. Inf. Theory* **46** 2428–33
[Pet86] Petz D 1986 Quasi-entropies for finite quantum systems *Rep. Math. Phys.* **23** 57–65
[PV10] Polyanskiy Y and Verdú S 2010 Arimoto channel coding converse and Rényi divergence *2010 48th Annual Allerton Conf. on Communication, Control and Computing (Allerton)* pp 1327–33
[QSW18] Qi H, Sharma K and Wilde M M 2018 Entanglement-assisted private communication over quantum broadcast channels *J. Phys. A: Math. Theor.* **51** 374001
[RBL18] Rosset D, Buscemi F and Liang Y-C 2018 Resource theory of quantum memories and their faithful verification with minimal assumptions *Phys. Rev.* X **8** 021033
[RR11] Renes J M and Renner R 2011 Noisy channel coding via privacy amplification and information reconciliation *IEEE Trans. Inf. Theory* **57** 7377–85
[RR12] Renes J M and Renner R 2012 One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys *IEEE Trans. Inf. Theory* **58** 1985–91
[RSW17] Radhakrishnan J, Sen P and Warsi N A 2017 One-shot private classical capacity of quantum wiretap channel: based on one-shot quantum covering lemma (arXiv:1703.01932)
[Sio58] Sion M 1958 On general minimax theorems *Pac. J. Math.* **8** 171–6
[SW24a] Singh V and Wilde M M 2024 No-go theorem for probabilistic one-way secret-key distillation (arXiv:2404.01392)
[SW24b] Singh V and Wilde M M 2024 Unextendible entanglement of quantum channels *IEEE Trans. Inf. Theory* (https://doi.org/10.1109/TIT.2025.3566737)
[TGW14] Takeoka M, Guha S and Wilde M M 2014 The squashed entanglement of a quantum channel *IEEE Trans. Inf. Theory* **60** 4987–98
[Tom15] Tomamichel M 2015 *Quantum Information Processing With Finite Resources* (Springer) (https://doi.org/10.1007/978-3-319-21891-5)
[Ume62] Umegaki H 1962 Conditional expectation in an operator algebra. IV. Entropy and information *Kodai Math. Semin. Rep.* **14** 59–85
[Wat18] Watrous J 2018 *The Theory of Quantum Information* (Cambridge University Press)
[WBHK20] Wilde M M, Berta M, Hirche C and Kaur E 2020 Amortized channel divergence for asymptotic quantum channel discrimination *Lett. Math. Phys.* **110** 2277–336
[Wer89] Werner R F 1989 An application of Bell's inequalities to a quantum state extension problem *Lett. Math. Phys.* **17** 359–63
[Wil16] Wilde M M 2016 Squashed entanglement and approximate private states *Quantum Inf. Process.* **15** 4563–80
[Wil17] Wilde M M 2017 Position-based coding and convex splitting for private communication over quantum channels *Quantum Inf. Process.* **16** 264
[WR12] Wang L and Renner R 2012 One-shot classical-quantum capacity and hypothesis testing *Phys. Rev. Lett.* **108** 200501
[WTB17] Wilde M M, Tomamichel M and Berta M 2017 Converse bounds for private communication over quantum channels *IEEE Trans. Inf. Theory* **63** 1792–817
[WW19a] Wang X and Wilde M M 2019 Resource theory of asymmetric distinguishability *Phys. Rev. Res.* **1** 033170
[WW19b] Wang X and Wilde M M 2019 Resource theory of asymmetric distinguishability for quantum channels *Phys. Rev. Res.* **1** 033169
[WWW24] Wang K, Wang X and Wilde M M 2024 Quantifying the unextendibility of entanglement *New J. Phys.* **26** 033013
[WWY14] Wilde M M, Winter A and Yang D 2014 Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy *Commun. Math. Phys.* **331** 593–622
[Yan06] Yang D 2006 A simple proof of monogamy of entanglement *Phys. Lett.* A **360** 249–50