No-go theorem for heralded exact one-way key distillation

Vishal Singh[1] and Mark M. Wilde[2]

[1]School of Applied and Engineering Physics, Cornell University, Ithaca, New York 14850, USA
[2]School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA

arXiv:2404.01392v2 [quant-ph] 6 Feb 2026

The heralded exact one-way distillable secret key is equal to the largest expected rate at which perfect secret key bits can be probabilistically distilled from a bipartite state by means of local operations and one-way classical communication. Here we define the set of super two-extendible states and prove that an arbitrary state in this set cannot be used for heralded exact one-way secret-key distillation. This broad class of states includes both erased states and all full-rank states. Comparing the heralded exact one-way distillable secret key with the more commonly studied approximate one-way distillable secret key, our results demonstrate an extreme gap between them for many states of interest, with the approximate one-way distillable secret key being much larger. Our findings naturally extend to heralded exact one-way entanglement distillation, with similar conclusions.

1 Introduction

Quantum key distribution has emerged as one of the most promising applications of a quantum network, as it facilitates unconditionally secure communication between distant parties [1, 2, 3]. It allows the transmission of private data between multiple parties, such that the security is ensured by the laws of quantum mechanics [4, 5, 6], instead of relying on computational assumptions about the eavesdropper [7]. The rapid development of quantum network technologies demands a strong understanding of our ability to distribute a secret key over a quantum network equipped with some available resources.

Entanglement is a major ingredient that ensures quantum mechanically secure communication [6], and it is in fact necessary as well, in the sense argued in [8]. However, the ability of a quantum state to establish a secret key is not a trivial consequence of its entanglement content. Indeed, the seminal work of [9, 10] established the existence of bound entangled states [11] that furnish a secret key upon local measurements. This motivates a separate discussion of the privacy content in a quantum state that is clearly distinct from its entanglement content.

The distillation of secret key from a quantum state under a restricted set of operations has garnered interest [12, 9, 13, 14, 15, 10, 16], due to its practical and foundational significance in quantum information science and, particularly, quantum privacy [17, 18]. Despite the differences, the theory of entanglement is intimately linked with quantum privacy, and a deeper understanding of one can reveal insights into the other. A specific task of interest is the distillation of secret key under local operations and one-way classical communication, abbreviated as one-way LOCC, due to its physically motivated setting and relation with the private capacity of quantum channels [19, 20].

In this paper, we analyze the heralded exact one-way secret-key distillation approach in which a perfect secret key is distilled from an initial bipartite state, albeit probabilistically. We also refer to this setting as probabilistic secret-key distillation with zero error, and we adopt the latter terminology henceforth. In particular, we study the one-way distillable secret key of a bipartite state in the probabilistic setting, which is roughly defined as the maximum achievable expected rate of distilling secret key bits from an arbitrarily large number of copies of the state using one-way LOCC channels.

Sometimes the term *probabilistic resource distillation* is used for probabilistic approximate distillation of a resource in the asymptotic setting, for example in [21, 22]. In that setting, a sequence of probabilistic protocols is considered a valid probabilistic resource distillation protocol if the sequence of distilled states, when the protocol is successful, converges to the maximal-resource state asymptotically. We emphasize that we use the term *probabilistic key distillation* in a more strict sense, where the distillation protocol must yield a perfect secret key whenever the protocol is successful, even if it requires an arbitrarily large number of resource states.

The particular contributions of our paper are as follows. We first establish the definition of probabilistic one-way distillable secret key, which is fundamentally different from approximate one-way distillable secret key [12]. We find a set of states, called the set of *super two-extendible* states, which have no probabilistic one-way distillable secret key and can also be described via

semidefinite constraints. Using the examples of erased states and full-rank states, we show that there exists an extreme gap between the probabilistic one-way distillable secret key and the approximate one-way distillable secret key for several states, with the former being equal to zero while the latter is strictly non-zero for these examples.

Our results establish fundamental limitations on probabilistic secret-key distillation, and consequently on probabilistic entanglement distillation, under one-way LOCC channels. The class of super two-extendible states provides a computationally-friendly framework for analyzing secret-key distillation in a resource-theoretic setting, due to its semidefinite characterization. Furthermore, our results emphasize the importance of allowing some error in secret-key distillation, as doing so can facilitate key distillation from otherwise undistillable states.

One of the main tools that we use to establish our results is the resource theory of unextendibility [23, 24] and its state-dependent variation [25]. This resource theory was developed in [23, 24] as a relaxation of the resource theory of entanglement, in which one-way LOCC channels are allowed for free. An important quantity that we employ is the min-unextendible entanglement of a bipartite state [25]. Our work also provides significant improvements on existing bounds [25, Sec. V.D] regarding the overhead of probabilistic one-way secret key distillation.

2 One-way secret-key distillation

Let us begin by considering the task of secret-key distillation. The objective of such a protocol $\mathcal{L}_{AB\to A'B'}$ is to transform a bipartite state ρ_{AB}, purified by ψ_{ABE}, into a tripartite key state as follows:

$$\mathcal{L}_{AB\to A'B'}(\psi_{ABE}) = \frac{1}{k}\sum_{i=0}^{k-1} |i\rangle\langle i|_{A'} \otimes |i\rangle\langle i|_{B'} \otimes \sigma_E, \quad (1)$$

where σ_E is an arbitrary quantum state. Alice and Bob, holding systems A' and B' respectively, can use the classically correlated state shared between them to communicate a message of $\log_2 k$ bits using the one-time-pad scheme. Any eavesdropper holding the system E cannot decipher anything about the message because σ_E is independent of the symbol i, hence, ensuring secrecy of the communication.

In [9, 10], it has been shown that the distillation of a secret key is equivalent to the distillation of a bipartite private state of the following form:

$$\gamma^k_{A_0A_1B_0B_1} \coloneqq \frac{1}{k}\sum_{i,j=0}^{k-1} |ii\rangle\langle jj|_{A_0B_0} \otimes U_i\omega_{A_1B_1}U_j^\dagger, \quad (2)$$

where $\omega_{A_1B_1}$ is an arbitrary quantum state and $(U_i)_{i=0}^{k-1}$ is a tuple of unitary operators. The systems A_0B_0 are the key systems, and A_1B_1 are the shield systems. The bipartite private state defined in (2) can be used to distill at least $\log_2 k$ secret key bits. We can hence reframe the task of secret key distillation into the distillation of bipartite private states. From here on we simplify the labeling for the key systems and shield systems: when referring to a private state $\gamma^k_{A_0A_1B_0B_1}$, we group the systems held by Alice into a single system label $A \coloneqq A_0A_1$ and all the systems held by Bob into a single system label $B \coloneqq B_0B_1$.

In a probabilistic one-way secret-key distillation protocol, Alice and Bob use local operations and one-way classical communication from Alice to Bob to distill a secret key, or equivalently a bipartite private state, from a shared resource state ρ_{AB} with some probability $p \in [0,1]$. The distillation process can be mathematically described as the action of a one-way LOCC channel $\mathcal{L}^{\to}_{AB\to XA'B'}$ on the resource state ρ_{AB} as follows:

$$\mathcal{L}^{\to}_{AB\to XA'B'}(\rho_{AB}) = p[1]_X \otimes \gamma^k_{A'B'} + (1-p)[0]_X \otimes \sigma_{A'B'}, \quad (3)$$

where we have used the shorthand

$$[i] \coloneqq |i\rangle\langle i|. \quad (4)$$

In (3), $\gamma^k_{A'B'}$ is a bipartite private state with at least $\log_2 k$ bits of secrecy, system X is a classical flag indicating the success or failure of the protocol, and $\sigma_{A'B'}$ is an arbitrary quantum state generated when the protocol fails to distill a private state.

In an arbitrary probabilistic secret-key distillation protocol, both parties must have access to the flag X in order to use the distilled key for private communication. Suppose that a probabilistic secret-key distillation protocol fails to establish a secret key. In that case, both parties involved in the distillation process can discard their systems and repeat the protocol with another instance of the resource state. If one-way LOCC channels are available for free, it suffices to demand that Alice receives the flag X since she can send the flag to Bob using the freely available forward classical channel.

We can now quantify the resource in a bipartite state that is relevant for the task of secret-key distillation using one-way LOCC channels. For this purpose, we define the probabilistic one-way distillable secret key of a bipartite state as follows:

Definition 1 *The probabilistic one-way distillable secret key of a bipartite state ρ_{AB} is the maximum expected rate at which secret key bits can be distilled from a bipartite state using one-way LOCC channels. It is formally defined as*

$$K^{\to}_D(\rho_{AB}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} K^{(1),\to}_D(\rho^{\otimes n}_{AB}), \quad (5)$$

where the one-shot probabilistic one-way distillable secret key is defined as

$$K_D^{(1),\rightarrow}(\rho_{AB}) \coloneqq \sup_{\substack{p\in[0,1],k\in\mathbb{N}\\ \mathcal{L}^{\rightarrow}\in 1\mathrm{WL},\gamma^k_{A'B'}}} \left\{ \begin{array}{c} p\log_2 k : \\ \mathcal{L}^{\rightarrow}(\rho_{AB}) = p[1]_{X_A}\otimes\gamma^k_{A'B'} \\ +(1-p)[0]_{X_A}\otimes\frac{I_{A'B'}}{d'_A d'_B} \end{array} \right\}. \quad (6)$$

In the above, $\mathcal{L}^{\rightarrow}_{AB\to X_A A'B'}$ is a one-way LOCC channel, 1WL denotes the set of all one-way LOCC channels, the optimization is over every private state $\gamma^k_{A'B'}$ of $\log_2 k$ secret key bits, X_A is a classical flag held by Alice, and $I_{A'B'}$ is the identity operator.

In (6) we require that the state generated upon failure of the protocol is a maximally mixed state. This additional constraint on secret-key distillation protocols does not affect the maximum expected number of secret key bits that can be distilled from a bipartite state using one-way LOCC channels, as we show in Appendix A.

It is worthwhile to note that a maximally entangled state of Schmidt rank k is a private state holding $\log_2 k$ secret key bits [9, 10]. As such, an arbitrary entanglement distillation protocol can be transformed into a secret-key distillation protocol without affecting the rate of distillation. Hence, the one-way distillable secret key of a quantum state is not less than the one-way distillable entanglement of the state in both the probabilistic and approximate settings.

A simpler way to analyze the probabilistic distillation of secret keys under the action of one-way LOCC channels is by considering the erasure symbol. The erasure symbol $[e]$ is defined to be orthogonal to every state in the span of $\{|i\rangle\langle j|\}_{i,j=0}^{d-1}$, where d is the dimension of the underlying system. For practical purposes, one can think of the erasure symbol as a pure state in the $(d+1)$-dimensional Hilbert space that is orthogonal to every state in the d-dimensional Hilbert space representing the system of interest. In the case of a joint system S that comprises multiple subsystems, say, $S_1, S_2, \ldots, S_k$, the erasure symbol $[e]_S$ can be represented as follows:

$$[e]_S = [e]_{S_1}\otimes[e]_{S_2}\otimes\cdots\otimes[e]_{S_k}, \quad (7)$$

which is orthogonal to every state on the system S, and hence, it is consistent with the definition of the erasure symbol.

In a one-way secret-key distillation protocol, if Alice finds the flag X_A in the state $[0]_{X_A}$, she can erase her state, and she can instruct Bob to erase his state as well. We call the resulting state the doubly erased private state, which has the following form:

$$\eta^{p,k}_{AB} \coloneqq p\,\gamma^k_{AB} + (1-p)[e]_A\otimes[e]_B, \quad (8)$$

where both Alice and Bob can retrieve the flag by performing the POVM $\{\Pi, [e]\}$ on their respective systems, where $\Pi \coloneqq \sum_{i=0}^{d-1}[i]$. They can further replace their state with a maximally mixed state upon measuring the erasure symbol, hence retrieving the distilled state in (6). That is,

$$\eta^{p,k}_{AB} \overset{\mathrm{LO}}{\longleftrightarrow} p[1]_{X_A}\otimes\gamma^k_{A'B'} + (1-p)[0]_{X_A}\otimes\frac{I_{A'B'}}{d_{A'}d_{B'}}. \quad (9)$$

Since the transformation in (9) can be effected by one-way LOCC only, the distillation of the doubly erased private state $\eta^{p,k}_{AB}$ is equivalent to the distillation of $\log_2 k$ secret key bits with probability p.

3 Min-unextendible entanglement

The min-unextendible entanglement of a bipartite state was defined in [25, Sec. 4.2] as a monotone for the state-dependent resource theory of unextendibility. We briefly mention the relevant properties of this quantity here, and we refer the reader to [25] for a detailed presentation of the resource theory of unextendibility.

The min-unextendible entanglement is defined with respect to the min-relative entropy [26, Def. 2] as follows:

$$E^u_{\min}(\rho_{AB}) \coloneqq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} -\frac{1}{2}\log_2 \mathrm{Tr}[\Pi^{\rho}_{AB}\sigma_{AB}], \quad (10)$$

where Π^{ρ}_{AB} is the projection onto the support of ρ_{AB} and the optimization is over all states in the following set:

$$\mathcal{F}(\rho_{AB}) \coloneqq \left\{ \begin{array}{c} \mathrm{Tr}_B[\omega_{ABB'}] : \rho_{AB} = \mathrm{Tr}_{B'}[\omega_{ABB'}], \\ \omega_{ABB'}\in\mathcal{S}(ABB') \end{array} \right\}, \quad (11)$$

with $\mathcal{S}(ABB')$ the set of all states of the joint system ABB' and system B' being isomorphic to system B.

The min-unextendible entanglement of a bipartite state has several properties relevant to our discussion. Firstly, it is non-negative, and it is additive with respect to tensor products of states. It is monotonic under the action of two-extendible channels, as defined in [23, 24], which is a superset of one-way LOCC channels. As such, the min-unextendible entanglement of a bipartite state does not increase under the action of one-way LOCC channels. Lastly, the min-unextendible entanglement of a bipartite private state is not less than the number of secret key bits held by the private state. See Appendix B for more details.

Remark 1 *The min-unextendible entanglement of a bipartite state does not increase under one-way LOCC channels. Hence, the transformation in (9) implies the following equality:*

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) = E^u_{\min}\left(p[1]_{X_A}\otimes\gamma^k_{AB} + (1-p)[0]_{X_A}\otimes\frac{I_{AB}}{d_A d_B}\right). \quad (12)$$

4 Limitations on probabilistic one-way distillable secret key

The monotonicity of the min-unextendible entanglement of a bipartite state under the action of one-way LOCC channels implies that the min-unextendible entanglement of the target state in a probabilistic one-way secret-key distillation protocol does not exceed the min-unextendible entanglement of the source state. We first present a lower bound on the min-unextendible entanglement of the doubly erased private state, which is the target state of a probabilistic one-way secret-key distillation protocol.

Lemma 1 *For all $p \in [0,1]$ and every integer $k \geq 2$, the min-unextendible entanglement of a doubly erased private state $\eta^{p,k}_{AB}$ is bounded from below by the following quantity:*

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) \geq -\frac{1}{2}\log_2\left(\frac{p}{k^2}+1-p\right). \quad (13)$$

Proof. See Appendix C. ■

The min-unextendible entanglement of the doubly erased private state $\eta^{p,k}_{AB}$ is strictly positive for all $p \in (0,1]$ and every integer $k \geq 2$, and it is only equal to zero at $p = 0$ because the resulting state is a product state ([25, Proposition 3]). As a consequence of the one-way LOCC monotonicity of the min-unextendible entanglement, a state whose min-unextendible entanglement is equal to zero cannot be used to distill any number of secret key bits with a non-zero probability using one-way LOCC channels. In what follows, we identify the structure of the set of states for which the min-unextendible entanglement is equal to zero and state the main result of this work formally in Theorem 1.

Let us first analyze the set of states whose min-unextendible entanglement is equal to zero. If there exists a state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\rho_{AB} = \sigma_{AB}$, then ρ_{AB} is a two-extendible state [27, 28, 29], and its min-unextendible entanglement is equal to zero. A more general set of states for which the min-unextendible entanglement is equal to zero, which we call super two-extendible states, can be defined as follows:

$$\text{2-EXT}_{\sup}(A\!:\!B) := \left\{ \begin{array}{c} \rho_{AB} : \exists \sigma_{AB} \in \mathcal{F}(\rho_{AB}), \\ \operatorname{supp}(\sigma_{AB}) \subseteq \operatorname{supp}(\rho_{AB}) \end{array} \right\}. \quad (14)$$

The set of super two-extendible states is convex but not closed (see Appendix D).

Proposition 1 *The min-unextendible entanglement of a quantum state is equal to zero if and only if it is super two-extendible.*

Proof. See Appendix E. ■

While the approximate one-way distillable secret key of a two-extendible state, also known as an anti-degradable state [30], is equal to zero [31, Thm. 15.43], the same is not true for a general super two-extendible state, as we shall see later in this paper. However, a super two-extendible state cannot be used for probabilistic one-way secret key distillation since its min-unextendible entanglement is equal to zero. Combining this fact with the additive property of the min-unextendible entanglement, we arrive at our main no-go theorem stated as Theorem 1, which identifies a broad set of states for which the probabilistic one-way distillable secret key is equal to zero.

Theorem 1 *The probabilistic one-way distillable secret key of a super two-extendible state is equal to zero.*

Proof. See Appendix F. ■

4.1 Erased private state

Let us consider the following state, which is established if Bob's share of a bipartite private state γ^k_{AB} gets erased with probability $1-p$:

$$\widetilde{\eta}^{p,k}_{AB} := p\,\gamma^k_{AB} + (1-p)\operatorname{Tr}_B\left[\gamma^k_{AB}\right]\otimes[e]_B, \quad (15)$$

where $\operatorname{Tr}_B[\cdot]$ refers to the partial trace of the argument over system B. We call the state in (15) an erased private state.

Proposition 2 *For all $p \in [0,1)$ and every integer $k \geq 2$, the erased private state $\widetilde{\eta}^{p,k}_{AB}$ is a super two-extendible state and thus has probabilistic one-way distillable secret key equal to zero.*

Proof. See Appendix G. ■

An erased state is defined as follows:

$$\widetilde{\Phi}^{p,d}_{AB} := p\,\Phi^d_{AB} + (1-p)\frac{I_A}{d_A}\otimes[e]_B, \quad (16)$$

where Φ^d_{AB} is the maximally entangled state with Schmidt rank equal to d. Since the erased state is a special case of an erased private state, it is in the set of super two-extendible states for all $p \in [0,1)$, which leads to Corollary 1 stated below.

Corollary 1 *For all $p \in [0,1)$ and every integer $d \geq 2$, the probabilistic one-way distillable secret key of the erased state $\widetilde{\Phi}^{p,d}_{AB}$ is equal to zero.*

The set of full-rank states also lies inside the set of super two-extendible states, which leads to Corollary 2 below.

Corollary 2 *All full-rank states are super two-extendible states, and the probabilistic one-way distillable secret key of such quantum states is equal to zero.*

Proof. See Appendix H. ■

The inability to probabilistically distill resources from full-rank states has been observed in general quantum resource theories [32, 33, 22]. Corollary 2 extends this result to probabilistic secret-key distillation under one-way LOCC channels. This result also implies that the overhead of probabilistic secret-key distillation considered in [25, Sec. V-B] is infinite for quantum states with full-rank density matrices, thus providing a significant strengthening of the bounds from [25, Sec. V-B].

4.2 Approximate versus probabilistic secret key distillation

Given the inability to distill a secret key from super two-extendible states even probabilistically, it is natural to ask if one can distill a key from such states if an arbitrarily small error is allowed. The rate at which secret-key bits can be distilled from a state such that the error vanishes asymptotically, using a one-way LOCC protocol, is called the one-way distillable key of the state [12], or the approximate one-way distillable key of the state, as we call it in this paper to clearly distinguish it from the probabilistic one-way distillable key of the state.

Indeed, it is possible distill a secret key from a state when an asymptotically vanishing error is allowed in distillation even if a perfect key cannot be distilled with any non-zero probability from the states, as we can see from the example of erased states. The approximate one-way distillable secret key is not less than the approximate one-way distillable entanglement of a state, which in turn is bounded from below by the coherent information of the state [12, Thm. 10]. For $p > \frac{1}{2}$, the coherent information of an erased state $\widetilde{\Phi}_{AB}^{p,d}$ is strictly non-negative. Similarly, the coherent information of some isotropic [34] and Werner states [35], which are full-rank states, is non-zero (see Appendices I and J). However, Corollaries 1 and 2 state that the probabilistic one-way distillable secret key of these states is equal to zero, demonstrating an extreme gap between the probabilistic and approximate one-way distillable secret key.

5 Conclusion

We found a convex set of states, that we call super two-extendible states, from which it is impossible to probabilistically distill perfect secret-key bits with any non-zero probability. Our main result is a no-go theorem stating that the probabilistic one-way distillable secret key of a super two-extendible state, and consequently its probabilistic one-way distillable entanglement, is equal to zero.

We demonstrated an extreme gap between the probabilistic and approximate one-way distillable secret key for some states. As such, we showed that probabilistic distillation of perfect secret keys using one-way LOCC protocols is not feasible for most states of interest, and one must allow some error for practically reasonable key distillation protocols. Considering the intermediate regime between probabilistic and approximate distillation [33, 21, 36], where the goal is to distill high-fidelity maximal-resource states with a non-zero probability, would shed light on the trade-off between distillation error and success probability in the task of probabilistic distillation of noisy secret keys.

Acknowledgments

We are grateful to Kaiyuan Ji, Ludovico Lami, Felix Leditzky, Theshani Nuradha, Dhrumil Patel, Aby Philip, Bartosz Regula, and Soorya Rethinasamy for insightful discussions. We are especially grateful to Ludovico Lami and Bartosz Regula for feedback that greatly improved our paper. We acknowledge financial support from NSF Grant No. 2315398.

References

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

[2] Christopher Portmann and Renato Renner. "Security in quantum cryptography". Reviews of Modern Physics **94**, 025008 (2022).

[3] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. "Advances in device-independent quantum key distribution". npj Quantum Information **9**, 10 (2023).

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

[5] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and

coin tossing". Theoretical Computer Science **560**, 7–11 (2014).

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

[7] Jonathan Katz and Yehuda Lindell. "Introduction to modern cryptography: Principles and protocols". Chapman and Hall/CRC. (2007).

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

[9] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "Secure key from bound entanglement". Physical Review Letters **94**, 160502 (2005). arXiv:quant-ph/0309110.

[10] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "General paradigm for distilling classical key from quantum states". IEEE Transactions on Information Theory **55**, 1898–1929 (2009). arXiv:quant-ph/0506189.

[11] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?". Physical Review Letters **80**, 5239–5242 (1998). arXiv:quant-ph/9801069.

[12] Igor Devetak and Andreas Winter. "Distillation of secret key and entanglement from quantum states". Proceedings of the Royal Society A **461**, 207–235 (2005). arXiv:quant-ph/0306078.

[13] Matthias Christandl. "The structure of bipartite quantum states—insights from group theory and cryptography" (2006). arXiv:quant-ph/0604183.

[14] Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner. "Unifying classical and quantum key distillation". In Salil P. Vadhan, editor, Theory of Cryptography. Pages 456–478. Berlin, Heidelberg (2007). Springer Berlin Heidelberg. arXiv:quant-ph/0608199.

[15] Karol Horodecki, Michał Horodecki, Paweł Horodecki, Debbie Leung, and Jonathan Oppenheim. "Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity". IEEE Transactions on Information Theory **54**, 2604–2620 (2008). arXiv:quant-ph/0608195.

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

[17] Mark M. Wilde, Marco Tomamichel, and Mario Berta. "Converse bounds for private communication over quantum channels". IEEE Transactions on Information Theory **63**, 1792–1817 (2017). arXiv:1602.08898.

[18] Haoyu Qi, Kunal Sharma, and Mark M Wilde. "Entanglement-assisted private communication over quantum broadcast channels". Journal of Physics A: Mathematical and Theoretical **51**, 374001 (2018). arXiv:1803.03976.

[19] N. Cai, A. Winter, and R. W. Yeung. "Quantum privacy and quantum wiretap channels". Problems of Information Transmission **40**, 318–336 (2004).

[20] I. Devetak. "The private classical capacity and quantum capacity of a quantum channel". IEEE Transactions on Information Theory **51**, 44–55 (2005). arXiv:quant-ph/0304127.

[21] Bartosz Regula. "Probabilistic transformations of quantum resources". Physical Review Letters **128**, 110505 (2022). arXiv:2109.04481.

[22] Bartosz Regula. "Tight constraints on probabilistic convertibility of quantum states". Quantum **6**, 817 (2022). arXiv:2112.11321.

[23] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. "Extendibility limits the performance of quantum processors". Physical Review Letters **123**, 070502 (2019). arXiv:2108.03137.

[24] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. "Resource theory of unextendibility and nonasymptotic quantum capacity". Physical Review A **104**, 022401 (2021). arXiv:1803.10710.

[25] Kun Wang, Xin Wang, and Mark M Wilde. "Quantifying the unextendibility of entanglement". New Journal of Physics **26**, 033013 (2024). arXiv:1911.07433.

[26] Nilanjana Datta. "Min- and max-relative entropies and a new entanglement monotone". IEEE Transactions on Information Theory **55**, 2816–2826 (2009). arXiv:0803.2770.

[27] Reinhard F. Werner. "An application of Bell's inequalities to a quantum state extension problem". Letters in Mathematical Physics **17**, 359–363 (1989).

[28] A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Distinguishing separable and entangled states". Physical Review Letters **88**, 187904 (2002). arXiv:quant-ph/0112007.

[29] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Complete family of separability criteria". Physical Review A **69**, 022308 (2004). arXiv:quant-ph/0308032.

[30] Felix Leditzky, Nilanjana Datta, and Graeme Smith. "Useful states and entanglement distillation". IEEE Transactions on Information Theory **64**, 4689–4708 (2018). arXiv:1701.03081.

[31] Sumeet Khatri and Mark M. Wilde. "Principles of quantum communication theory: A modern approach" (2024). arXiv:2011.04672v2.

[32] Adrian Kent. "Entangled mixed states and local purification". Physical Review Letters **81**, 2839–2841 (1998).

[33] Kun Fang and Zi-Wen Liu. "No-go theorems for quantum resource purification". Physical Review Letters **125**, 060405 (2020). arXiv:1909.02540.

[34] Michał Horodecki and Paweł Horodecki. "Reduction criterion of separability and limits for a class of distillation protocols". Physical Review A **59**, 4206–4216 (1999). arXiv:quant-ph/9708015.

[35] Reinhard F. Werner. "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". Physical Review A **40**, 4277–4281 (1989).

[36] Jens Eisert and Mark M. Wilde. "A smallest computable entanglement monotone". In 2022 IEEE International Symposium on Information Theory (ISIT). Pages 2439–2444. (2022). arXiv:2201.00835.

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

[38] T. Ogawa and H. Nagaoka. "A new proof of the channel coding theorem via hypothesis testing in quantum information theory". In Proceedings IEEE International Symposium on Information Theory. Page 73. (2002). arXiv:quant-ph/0208139.

[39] Benjamin Schumacher and M. A. Nielsen. "Quantum data processing and error correction". Physical Review A **54**, 2629–2635 (1996). arXiv:quant-ph/9604022.

[40] Johann von Neumann. "Thermodynamik quantenmechanischer gesamtheiten". Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1927**, 273–291 (1927). url: http://eudml.org/doc/59231.

A Equivalent definitions of probabilistic one-way distillable secret key

In this section, we justify the definition of one-shot probabilistic one-way distillable secret key of a bipartite state given in (6) by showing an equivalence between (6) and a more general definition of the one-shot probabilistic one-way distillable secret key that we propose in (18).

Consider a general probabilistic one-way secret-key distillation protocol in which a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to X_A A'B'}$ acts on a bipartite state ρ_{AB} to establish the following state:

$$\mathcal{L}^{\rightarrow}(\rho_{AB}) = p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \sigma_{A'B'}, \tag{17}$$

where $\gamma^k_{A'B'}$ is a bipartite private state holding $\log_2 k$ secret key bits and $\sigma_{A'B'}$ is an arbitrary bipartite state. As such, this protocol can be used to distill an expected number $p \log_2 k$ of secret key bits from a single instance of ρ_{AB}. The one-shot probabilistic one-way distillable secret key of the state ρ_{AB} is defined generally as

$$K_D^{(1),\rightarrow}(\rho_{AB}) \coloneqq \sup_{\substack{p\in[0,1],k\in\mathbb{N} \\ \mathcal{L}^{\rightarrow}\in 1\text{WL},\gamma^k_{A'B'}}} \left\{ \begin{array}{c} p\log_2 k : \\ \mathcal{L}^{\rightarrow}(\rho_{AB}) = p[1]_{X_A} \otimes \gamma^k_{A'B'} \\ +(1-p)[0]_{X_A} \otimes \sigma_{A'B'}, \\ \sigma_{A'B'} \in \mathcal{S}(A'B') \end{array} \right\}. \tag{18}$$

In the presence of forward classical communication, Alice can send a copy of the flag X_A to Bob, so that both parties know when the protocol is unsuccessful in establishing the private state $\gamma^k_{A'B'}$, hence, arriving at the following state:

$$\left(\mathcal{C}_{X_A\to X_A X_B} \circ \mathcal{L}^{\rightarrow}\right)(\rho_{AB}) = p[1]_{X_A} \otimes [1]_{X_B} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes [0]_{X_B} \otimes \sigma_{A'B'}, \tag{19}$$

where $\mathcal{C}_{X_A \to X_A X_B}$ is a classical channel that copies the classical data from X_A to X_B. Now that both parties hold a copy of the flag, they can trace out their states and replace them with a locally prepared maximally mixed state if the flag indicates that the protocol was unsuccessful in establishing a private state. That is, Alice applies the following local channel on her system:

$$\mathcal{R}_{X_A A' \to X_A A'}(\cdot) = \frac{I_{A'}}{d_{A'}} \otimes \mathrm{Tr}_{A'}[[0]_{X_A} (\cdot) [0]_{X_A}] + \mathrm{id}_{X_A A' \to X_A A'}([1]_{X_A} (\cdot) [1]_{X_A}), \tag{20}$$

and Bob applies the corresponding local channel on his systems. Tracing out Bob's flag, we arrive at the following quantum state:

$$(\mathcal{R} \circ \mathcal{C} \circ \mathcal{L}^{\to})(\rho_{AB}) = p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \frac{I_{A'}}{d_{A'}} \otimes \frac{I_{B'}}{d_{B'}} \tag{21}$$

$$= p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'} d_{B'}}. \tag{22}$$

Observe that $\mathcal{R} \circ \mathcal{C} \circ \mathcal{L}^{\to}$ is also a one-way LOCC channel that distills an expected number $p \log_2 k$ of secret key bits from a single instance of ρ_{AB}. Since such a one-way LOCC transformation can be designed for every one-way LOCC channel $\mathcal{L}^{\to}_{AB \to X_A A' B'}$, we can conclude the following statement: if there exists a one-way LOCC channel that distills a quantum state of the form given in (17), then there also exists a one-way LOCC channel that distills the quantum state of the form given in (22). As the expected number of secret key bits distilled from ρ_{AB} using either of the channels is equal to $p \log_2 k$, we can restrict the optimization in the definition of one-shot probabilistic one-way distillable secret key to channels that establish a quantum state of the form given in (22). Hence, we arrive at the equivalent definition of the one-shot probabilistic one-way distillable secret key given in (6).

B The min-unextendible entanglement of bipartite states

A measure for quantifying the unextendibility of quantum states, called unextendible entanglement, was introduced in [25]. Let us briefly discuss this quantity, which is one of the major components used to prove our main results. Recall that a generalized divergence $\mathbf{D}$ is a function of two quantum states that is non-increasing under the action of a quantum channel [37]. The unextendible entanglement of a bipartite state [25] is defined in terms of a generalized divergence as follows:

Definition 2 ([25]) *The generalized unextendible entanglement of a bipartite state ρ_{AB}, induced by a generalized divergence $\mathbf{D}$, is defined as*

$$\mathbf{E}^u(\rho_{AB}) \coloneqq \inf_{\sigma_{AB} \in \mathcal{F}(\rho_{AB})} \frac{1}{2} \mathbf{D}(\rho_{AB} \| \sigma_{AB}), \tag{23}$$

where $\mathcal{F}(\rho_{AB})$ is defined in (11).

We also use the notation $\mathbf{E}^u(\rho_{A:B})$ to clarify the bipartition of systems over which the unextendible entanglement is being considered.

The unextendible entanglement provides a framework for quantifying the unextendibility of a bipartite state ρ_{AB} with respect to the system B. Crucially, this quantity is monotonic under the action of two-extendible channels [25, Theorem 2], and hence, it is also monotonic under

the action of one-way LOCC channels. (See [23, 24, 25] for the definition of a two-extendible channel.) Stated formally, [25, Theorem 2] establishes the following: for every quantum state ρ_{AB} and two-extendible channel $\mathcal{N}_{AB\to A'B'}$, the following inequality holds:

$$\mathbf{E}^u(\rho_{AB}) \geq \mathbf{E}^u(\mathcal{N}_{AB\to A'B'}(\rho_{AB})). \tag{24}$$

A different measure for unextendibility was proposed in [23, 24] where the divergence was measured with respect to a fixed set of two-extendible states. However, in Definition 2, 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.

A particular example of interest and one of the main tools in our paper is the min-unextendible entanglement [25], defined as follows:

$$E^u_{\min}(\rho_{AB}) \coloneqq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2} D_{\min}(\rho_{AB}\|\sigma_{AB}), \tag{25}$$

where $D_{\min}$ is the min-relative entropy [26, Def. 2]:

$$D_{\min}(\omega\|\tau) \coloneqq -\log_2 \operatorname{Tr}[\Pi^\omega \tau], \tag{26}$$

with ω a state, τ a positive semidefinite operator, and Π^ω the projection onto the support of ω.

The min-unextendible entanglement has the following properties [25]:

1. **Non-negativity:** The min-unextendible entanglement is non-negative for a bipartite quantum state, as a consequence of the min-relative entropy being non-negative for all pairs of states. That is,
$$E^u_{\min}(\rho_{AB}) \geq 0 \quad \forall \rho_{AB} \in \mathcal{S}(AB). \tag{27}$$

2. **Additivity [25, Prop. 15]:** The min-unextendible entanglement is additive with respect to a tensor product of the states $\rho_{A_1B_1}$ and $\sigma_{A_2B_2}$:
$$E^u_{\min}(\rho_{A_1:B_1}\otimes\sigma_{A_2:B_2}) = E^u_{\min}(\rho_{A_1:B_1}) + E^u_{\min}(\sigma_{A_2:B_2}). \tag{28}$$

3. **Privacy bound [25, Prop. 21]** The min-unextendible entanglement of a bipartite private state γ^k_{AB}, holding $\log_2 k$ secret key bits, is bounded from below as follows:
$$E^u_{\min}\left(\gamma^k_{AB}\right) \geq \log_2 k. \tag{29}$$

C Proof of Lemma 1

We restate Lemma 1 here for the reader's convenience.

For all $p \in [0,1]$ and every integer $k \geq 2$, the min-unextendible entanglement of a doubly erased private state $\eta^{p,k}_{AB}$ is bounded from below by the following quantity:

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) \geq -\frac{1}{2}\log_2\left(\frac{p}{k^2}+1-p\right). \tag{30}$$

Consider the following partially dephasing channel:

$$\Delta_A(\cdot) \coloneqq \Pi_A(\cdot)\Pi_A + [e]_A(\cdot)[e]_A, \tag{31}$$

where $\Pi_A := \sum_{i=0}^{d-1}[i]$, so that $\Pi_A[e] = [e]\Pi_A = 0$. In Lemmas 2 and 3, we first characterize the action of Δ_A on an arbitrary state $\omega_{AE} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$. We then use Lemmas 2 and 3 to prove Lemma 1.

Lemma 2 *Let ω_{AE} be an arbitrary state in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$, where $\eta^{p,k}$ is a doubly erased state, as defined in (8). Then $\Delta_A(\omega_{AE})$ is also in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$, where Δ_A is defined in (31).*

Proof. For every quantum state $\omega_{AE} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$, there exists a state ω_{ABE} with the following marginals;

$$\mathrm{Tr}_E[\omega_{ABE}] = \eta_{AB}^{p,k}, \tag{32}$$
$$\mathrm{Tr}_B[\omega_{ABE}] = \omega_{AE}. \tag{33}$$

Note that the doubly erased state $\eta_{AB}^{p,k}$ is invariant under the action of Δ_A. Therefore, the following equalities hold:

$$\Delta_A\left(\eta_{AB}^{p,k}\right) = \Delta_A(\mathrm{Tr}_E[\omega_{ABE}]) \tag{34}$$
$$= \mathrm{Tr}_E[\Delta_A(\omega_{ABE})] \tag{35}$$
$$= \eta_{AB}^{p,k}. \tag{36}$$

This implies that $\Delta(\omega_{ABE})$ is also an extension of $\eta_{AB}^{p,k}$, and consequently, $\mathrm{Tr}_B[\Delta_A(\omega_{ABE})] = \Delta_A(\omega_{AE})$ is in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$. ∎

Lemma 3 *Let ω_{AE} be an arbitrary state in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$, where $\eta^{p,k}$ is a doubly erased state of the following form:*

$$\eta_{AB}^{p,k} = p\ \gamma_{AB}^{k} + (1-p)[e]_A \otimes [e]_B, \tag{37}$$

with γ_{AB}^{k} a bipartite private state holding $\log_2 k$ secret key bits. Here systems E and B are isomorphic to each other. The action of the partially dephasing channel Δ_A, defined in (31), on the state ω_{AE} results in the following state:

$$\Delta_A(\omega_{AE}) = p\ \sigma_{AE} + (1-p)[e]_A \otimes \tau_E, \tag{38}$$

where $\sigma_{AE} \in \mathcal{F}\left(\gamma_{AB}^{k}\right)$ and $\tau_E \in \mathcal{S}(E)$.

Proof. For every quantum state $\omega_{AE} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$, there exists a state ω_{ABE} with the following marginals;

$$\mathrm{Tr}_E[\omega_{ABE}] = \eta_{AB}^{p,k}, \tag{39}$$
$$\mathrm{Tr}_B[\omega_{ABE}] = \omega_{AE}. \tag{40}$$

Recall the definition of the partially dephasing channel Δ_A from (31). The state arising from the action of Δ_A on the state ω_{ABE} can be decomposed as follows:

$$\Delta_A(\omega_{ABE}) = X_{ABE} + [e]_A \otimes Y_{BE}, \tag{41}$$

where $[e]_A X_{ABE} = X_{ABE}[e]_A = 0$. Since $\Delta_A(\omega_{ABE})$ is a quantum state, $\Delta(\omega_{ABE}) \geq 0$, which implies the following operator inequalities:

$$X_{ABE} \geq 0, \tag{42}$$

$$[e]_A \otimes Y_{BE} \geq 0, \tag{43}$$
$$\Rightarrow Y_{BE} \geq 0, \tag{44}$$

where we have used the fact that X_{ABE} and $[e]_A \otimes Y_{BE}$ are orthogonal to each other.

Consider the marginal of $\Delta_A(\omega_{ABE})$ on systems AB, which is equal to the following:

$$\mathrm{Tr}_E[\Delta_A(\omega_{ABE})] = \mathrm{Tr}_E[X_{ABE}] + \mathrm{Tr}_E[Y_{BE}] \otimes [e]_A. \tag{45}$$

We can also evaluate the marginal by first tracing out the system E and then applying the partially dephasing channel; that is,

$$\mathrm{Tr}_E[\Delta_A(\omega_{ABE})] = \Delta_A\left(\mathrm{Tr}_E[\omega_{ABE}]\right) \tag{46}$$
$$= p\ \gamma^k_{AB} + (1-p)[e]_A \otimes [e]_B. \tag{47}$$

Comparing (45) and (47), and using the fact that $[e]_A X_{ABE} = 0$, we arrive at the following equalities:

$$\mathrm{Tr}_E[X_{ABE}] = p\ \gamma^k_{AB}, \tag{48}$$
$$\mathrm{Tr}_E[Y_{BE}] = (1-p)[e]_B. \tag{49}$$

Recall from (42) and (44) that X_{ABE} and Y_{BE} are positive semidefinite operators. Using (48), we can further conclude that $\frac{X_{ABE}}{p}$ is a quantum state that extends γ^k_{AB}. Similarly, (49) implies that $\frac{Y_{BE}}{1-p}$ is a quantum state that extends $[e]_B$.

Any quantum state that extends $[e]_B$ is of the form $[e]_B \otimes \tau_E$, where τ_E is an arbitrary quantum state (and which can even be $[e]_E$). Let us define the quantum state $\sigma_{AE} \coloneqq \frac{1}{p}\mathrm{Tr}_B[X_{ABE}]$. Since $\frac{1}{p}\mathrm{Tr}_E[X_{ABE}] = \gamma^k_{AB}$, σ_{AE} is in the set $\mathcal{F}\left(\gamma^k_{AB}\right)$. The marginal of the state $\Delta_A(\omega_{ABE})$ on systems AE can now be written as follows:

$$\Delta_A(\omega_{AE}) = p\ \sigma_{AE} + (1-p)[e]_A \otimes \tau_E, \tag{50}$$

where $\tau_E \in \mathcal{S}(E)$ and $\sigma_{AE} \in \mathcal{F}\left(\gamma^k_{AB}\right)$. ■

Proof of Lemma 1. The min-unextendible entanglement of $\eta^{p,k}_{AB}$ is equal to the following:

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) = \inf_{\omega_{AB} \in \mathcal{F}\left(\eta^{p,k}\right)} \frac{1}{2} D_{\min}\left(\eta^{p,k}_{AB} \middle\| \omega_{AB}\right), \tag{51}$$

where $\eta^{p,k}_{AB} = p\ \gamma^k_{AB} + (1-p)[e]_A \otimes [e]_B$ with γ^k_{AB} a bipartite private state holding $\log_2 k$ secret key bits.

Consider an arbitrary state $\omega_{AB} \in \mathcal{F}\left(\eta^{p,k}_{AB}\right)$. The min-relative entropy between $\eta^{p,k}_{AB}$ and ω_{AB} obeys the following inequality:

$$D_{\min}\left(\eta^{p,k}_{AB} \middle\| \omega_{AB}\right) \geq D_{\min}\left(\Delta_A\left(\eta^{p,k}_{AB}\right) \middle\| \Delta_A(\omega_{AB})\right) \tag{52}$$
$$= D_{\min}\left(\eta^{p,k}_{AB} \middle\| \Delta_A(\omega_{AB})\right), \tag{53}$$

where Δ_A is defined in (31). The above inequality follows from the data-processing of min-relative entropy and the subsequent equality follows from the invariance of the doubly erased state under

the action of the partially dephasing channel Δ_A. We have shown in Lemma 2 that $\Delta_A(\omega_{AB})$ also is in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$. Then the inequality in (52)–(53) implies that we can restrict the optimization in (51) to states ω_{AB} such that $\omega_{AB} = \Delta_A(\omega_{AB})$. Alternatively, we can write the min-unextendible entanglement of the doubly erased state as follows:

$$E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) = \inf_{\omega_{AB}\in\mathcal{F}\left(\eta^{p,k}\right)} \frac{1}{2} D_{\min}\left(\eta_{AB}^{p,k}\middle\|\Delta_A(\omega_{AB})\right). \tag{54}$$

We have shown in Lemma 3 that the action of the channel Δ_A on every state $\omega_{AB} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$ results in a state of the following form:

$$\Delta_A(\omega_{AB}) = p\ \sigma_{AB} + (1-p)[e]_A \otimes \tau_B, \tag{55}$$

where $\tau_B \in \mathcal{S}(B)$, and $\sigma_{AB} \in \mathcal{F}\left(\gamma_{AB}^{k}\right)$. This leads to the following equalities:

$$\begin{aligned} E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) &= \inf_{\omega_{AB}\in\mathcal{F}\left(\eta^{p,k}\right)} \frac{1}{2} D_{\min}\left(\eta_{AB}^{p,k}\middle\|\Delta_A(\omega_{AB})\right) && (56)\\ &= \inf_{\sigma,\tau} -\frac{1}{2}\log_2 \operatorname{Tr}\left[\Pi^{\eta^{p,k}}\left(p\ \sigma_{AB} + (1-p)[e]_A \otimes \tau_B\right)\right] && (57)\\ &= -\frac{1}{2}\log_2 \sup_{\sigma,\tau} \operatorname{Tr}\left[\Pi^{\eta^{p,k}}\left(p\ \sigma_{AB} + (1-p)[e]_A \otimes \tau_B\right)\right], && (58) \end{aligned}$$

where $\Pi^{\eta^{p,k}}$ is the projection onto the support of $\eta_{AB}^{p,k}$. The optimization in the second and third equalities is over all $\sigma_{AB} \in \mathcal{F}\left(\gamma_{AB}^{k}\right)$ and $\tau_B \in \mathcal{S}(B)$. The last equality follows from the monotonicity of the logarithm.

Note that γ_{AB}^{k} is orthogonal to $[e]_A \otimes [e]_B$, and $[e]_A \otimes [e]_B$ is a projection. Therefore, we can write the projection onto the support of $\eta_{AB}^{p,k}$ as the following sum:

$$\Pi_{AB}^{\eta^{p,k}} = \Pi_{AB}^{\gamma^{k}} + [e]_A \otimes [e]_B, \tag{59}$$

where $\Pi_{AB}^{\gamma^{k}}$ is the projection onto the support of the bipartite private state γ_{AB}^{k}. Consequently,

$$\begin{aligned} E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) &= -\frac{1}{2}\log_2 \sup_{\sigma,\tau}\left(p \operatorname{Tr}\left[\Pi_{AB}^{\gamma^{k}}\sigma_{AB}\right] + (1-p)\operatorname{Tr}[([e]_A \otimes [e]_B)([e]_A \otimes \tau_B)]\right) && (60)\\ &= -\frac{1}{2}\log_2 \sup_{\sigma,\tau}\left(p \operatorname{Tr}\left[\Pi_{AB}^{\gamma^{k}}\sigma_{AB}\right] + (1-p)\operatorname{Tr}[[e]_A \otimes ([e]_B\tau_B)]\right), && (61) \end{aligned}$$

where the first equality follows from the fact that $([e]_A \otimes I_B)\,\sigma_{AB} = 0$ and $\Pi_{AB}^{\gamma^{k}}([e]_A \otimes \tau_B) = 0$ for every quantum state τ_B.

It is clear that τ_B should be $[e]_B$ in order for the second term inside the logarithm in (61) to be non-zero. Therefore,

$$\begin{aligned} E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) &= -\frac{1}{2}\log_2 \sup_{\sigma\in\mathcal{F}\left(\gamma_{AB}^{k}\right)}\left(p \operatorname{Tr}\left[\Pi^{\gamma^{k}}\sigma_{AB}\right] + 1 - p\right) && (62)\\ &= -\frac{1}{2}\log_2 \sup_{\sigma\in\mathcal{F}\left(\gamma_{AB}^{k}\right)}\left(p\ 2^{-D_{\min}\left(\gamma_{AB}^{k}\middle\|\sigma_{AB}\right)} + 1 - p\right) && (63) \end{aligned}$$

$$= -\frac{1}{2}\log_2\left(p\ 2^{-\inf_{\sigma\in\mathcal{F}\left(\gamma_{AB}^k\right)} D_{\min}\left(\gamma_{AB}^k\middle\|\sigma_{AB}\right)} + 1 - p\right) \tag{64}$$

$$= -\frac{1}{2}\log_2\left(p\ 2^{-2E_{\min}^u\left(\gamma_{AB}^k\right)} + 1 - p\right), \tag{65}$$

where the second equality follows from the definition of min-relative entropy, the third equality follows from the monotonicity of the exponential function, and the last equality follows from the definition of the min-unextendible entanglement of quantum states.

It has been shown in [25, Corollary 22] that the min-unextendible entanglement of a bipartite private state holding $\log_2 k$ bits of secrecy is not less than $\log_2 k$. That is,

$$E_{\min}^u\left(\gamma_{AB}^k\right) \geq \log_2 k. \tag{66}$$

Therefore,

$$p\ 2^{-2E_{\min}^u\left(\gamma^k\right)} \leq p\ 2^{-2\log_2 k} = \frac{p}{k^2}. \tag{67}$$

From the monotonicity of the logarithm function,

$$\log_2\left(p\ 2^{-2E_{\min}^u\left(\gamma_{AB}^k\right)} + 1 - p\right) \leq \log_2\left(\frac{p}{k^2} + 1 - p\right), \tag{68}$$

and hence,

$$E_{\min}^u\left(\eta_{AB}^{p,k}\right) \geq -\frac{1}{2}\log_2\left(\frac{p}{k^2} + 1 - p\right) \quad \forall p \in (0,1), k \geq 2. \tag{69}$$

When $p = 0$, $\eta_{AB}^{p,k}$ is a separable state, and hence, its min-unextendible entanglement is equal to zero [25, Proposition 3]. When $p = 1$, $\eta_{AB}^{p,k}$ is a bipartite private state holding $\log_2 k$ bits of secrecy, and hence, its min-unextendible entanglement is not less than $\log_2 k$ as stated in [25, Corollary 22]. Thus, we conclude the statement of Lemma 1. ■

D The set of super two-extendible states is convex but not closed

First we show that the set of super two-extendible states is convex. Consider two quantum states ρ_{AB} and τ_{AB} that are in the set of super two-extendible states. Let $\overline{\rho}_{ABE}$ be an extension of ρ_{AB} such that the following containment holds:

$$\operatorname{supp}(\mathrm{id}_{E\to B}(\mathrm{Tr}_B[\overline{\rho}_{ABE}])) \subseteq \operatorname{supp}(\rho_{AB}), \tag{70}$$

where both systems E and B are modeled by the same Hilbert space. Note that the existence of such an extension is guaranteed by the fact that ρ_{AB} is in the set of super two-extendible states. Similarly, let $\overline{\tau}_{ABE}$ be an extension of τ_{AB} such that the following containment holds:

$$\operatorname{supp}(\mathrm{id}_{E\to B}(\mathrm{Tr}_B[\overline{\tau}_{ABE}])) \subseteq \operatorname{supp}(\tau_{AB}). \tag{71}$$

From now on, we will assume that the identity channel $\mathrm{id}_{E\to B}$ is implicit when we compare the supports of two operators in $\mathcal{S}(AB)$ and $\mathcal{S}(AE)$, respectively.

Consider an arbitrary convex combination of the states ρ_{AB} and τ_{AB}:

$$\sigma_{AB} \coloneqq p\ \rho_{AB} + (1-p)\tau_{AB}, \tag{72}$$

where $p \in [0,1]$. The following state is a valid extension of σ_{AB}:

$$\omega_{ABE} \coloneqq p\ \overline{\rho}_{ABE} + (1-p)\overline{\tau}_{ABE}, \tag{73}$$

because

$$\mathrm{Tr}_E[\omega_{ABE}] = p\ \rho_{AB} + (1-p)\tau_{AB} = \sigma_{AB}. \tag{74}$$

The other relevant marginal of ω_{ABE} can be expressed as follows:

$$\mathrm{Tr}_B[\omega_{ABE}] = p\,\mathrm{Tr}_B[\overline{\rho}_{ABE}] + (1-p)\,\mathrm{Tr}_B[\overline{\tau}_{ABE}]\,. \tag{75}$$

Note that σ_{AB} is in the set of super two-extendible states for $p = 0$ and $p = 1$ by the assumption that ρ_{AB} and τ_{AB} are super two-extendible states. For all $p \in (0,1)$, the following holds:

$$\begin{aligned}
\mathrm{supp}(\mathrm{Tr}_B[\omega_{ABE}]) &= \mathrm{supp}(\mathrm{Tr}_B[\overline{\rho}_{ABE}]) \cup \mathrm{supp}(\mathrm{Tr}_B[\overline{\tau}_{ABE}]) && (76)\\
&\subseteq \mathrm{supp}(\mathrm{Tr}_E[\overline{\rho}_{ABE}]) \cup \mathrm{supp}(\mathrm{Tr}_E[\overline{\tau}_{ABE}]) && (77)\\
&= \mathrm{supp}(\mathrm{Tr}_E[\omega_{ABE}]) && (78)\\
&= \mathrm{supp}(\sigma_{AB})\,, && (79)
\end{aligned}$$

where the containment of the sets follows from (70) and (71).

Since the support of $\mathrm{Tr}_B[\omega_{ABE}]$ is in the support of $\mathrm{Tr}_E[\omega_{ABE}]$, we conclude that $\mathrm{Tr}_E[\omega_{ABE}] = \sigma_{AB}$ is a super two-extendible state for all $p \in (0,1)$ as well. Therefore, the state σ_{AB}, which is a convex combination of two arbitrary super two-extendible states, is super two-extendible for every $p \in [0,1]$, justifying that the set of super two-extendible states is convex.

To show that the set of super two-extendible states is not closed, let us consider the example of erased states defined in (16). The erased state $\widetilde{\Phi}^{p,k}_{AB}$ is a special case of an erased private state $\widetilde{\eta}^{p,k}_{AB}$. Appendix G establishes that an erased private state is super two-extendible for every $p \in [0,1)$. This implies that an erased state $\widetilde{\Phi}^{p,k}_{AB}$ is also super two-extendible for every $p \in [0,1)$. However, for $p = 1$, $\widetilde{\Phi}^{p,k}_{AB}$ is a maximally entangled state of Schmidt rank k, which is not super two-extendible. In fact, this state has a min-unextendible entanglement of $\log_2 k$. As such, the maximally entangled state is a limit point of the set of super two-extendible states, but it is not a super two-extendible state itself. Hence, the set of super two-extendible states is not closed.

E Proof of Proposition 1

We restate Proposition 1 here for the reader's convenience.

The min-unextendible entanglement of a quantum state is equal to zero if and only if it is super two-extendible.

For every super two-extendible state ρ_{AB}, there exists a quantum state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\mathrm{supp}(\sigma_{AB}) \subseteq \mathrm{supp}(\rho_{AB})$. This implies that $\Pi^{\rho}_{AB}\sigma_{AB} = \sigma_{AB}$, where Π^{ρ}_{AB} is the projection onto the support of ρ_{AB}. The min-unextendible entanglement of ρ_{AB} can then be bounded as follows:

$$\begin{aligned}
0 &\leq E^{u}_{\min}(\rho_{AB}) && (80)\\
&= \inf_{\tau \in \mathcal{F}(\rho)} -\frac{1}{2}\log_2 \mathrm{Tr}[\Pi^{\rho}_{AB}\tau_{AB}] && (81)\\
&\leq -\frac{1}{2}\log_2 \mathrm{Tr}[\Pi^{\rho}_{AB}\sigma_{AB}] && (82)
\end{aligned}$$

$$= -\frac{1}{2}\log_2 \mathrm{Tr}[\sigma_{AB}] \tag{83}$$
$$= 0, \tag{84}$$

where the first inequality follows from (27), the first equality follows from the definition of min-unextendible entanglement of a bipartite state, and the last equality follows from the fact that σ_{AB} is a quantum state with unit trace. Therefore, the min-unextendible entanglement of a super two-extendible state is equal to zero.

We now establish the opposite implication. Consider an arbitrary quantum state ρ_{AB} such that $E^u_{\min}(\rho_{AB}) = 0$. This is true only if there exists a quantum state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\mathrm{Tr}[\Pi^{\rho}_{AB}\sigma_{AB}] = 1$, which follows from the definition of the min-unextendible entanglement of a bipartite state. From the gentle measurement lemma [38, Lemma 5], it is known for a state τ and a projector P that

$$\frac{1}{2}\left\|\tau - P\tau P\right\|_1 \leq \sqrt{1 - \mathrm{Tr}[P\tau]}. \tag{85}$$

Applying this to our case, we conclude that

$$\left\|\Pi^{\rho}_{AB}\sigma_{AB}\Pi^{\rho}_{AB} - \sigma_{AB}\right\|_1 = 0, \tag{86}$$

which implies that $\Pi^{\rho}_{AB}\sigma_{AB}\Pi^{\rho}_{AB} = \sigma_{AB}$. This in turns implies that the support of σ_{AB} is in the support of ρ_{AB}. We finally conclude that the min-unextendible entanglement of ρ_{AB} is equal to zero only if there exists a quantum state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\mathrm{supp}(\sigma_{AB}) \subseteq \mathrm{supp}(\rho_{AB})$, which is precisely the definition of a super two-extendible state.

F Proof of Theorem 1

Let us restate Theorem 1 for the reader's convenience.

The probabilistic one-way distillable secret key of a super two-extendible state is equal to zero.

Consider a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{A^nB^n\to X_AA'B'}$ that acts on n copies of a super two-extendible state ρ_{AB} as follows:

$$\mathcal{L}^{\rightarrow}\left((\rho_{AB})^{\otimes n}\right) = q[1]_{X_A} \otimes \gamma^{k'}_{A'B'} + (1-q)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'}d_{B'}}, \tag{87}$$

for some $q \in [0,1]$ and integer $k' \geq 2$. Then

$$0 \leq E^u_{\min}\left(q[1]_{X_A} \otimes \gamma^{k'}_{A'B'} + (1-q)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'}d_{B'}}\right) \tag{88}$$
$$= E^u_{\min}\left(\eta^{q,k'}_{A'B'}\right) \tag{89}$$
$$= E^u_{\min}\left(\mathcal{L}^{\rightarrow}\left((\rho_{AB})^{\otimes n}\right)\right) \tag{90}$$
$$\leq E^u_{\min}\left((\rho_{AB})^{\otimes n}\right) \tag{91}$$
$$= nE^u_{\min}(\rho_{AB}) \tag{92}$$
$$= 0, \tag{93}$$

The first inequality follows from (27). The first equality follows from Remark 1 (the min-unextendible entanglement of the state in (87) is the same as the min-unextendible entanglement

of the doubly erased private state $\eta^{q,k'}_{A'B'}$). The second inequality follows from the monotonicity of min-unextendible entanglement under one-way LOCC channels, the third equality follows from the additivity of min-unextendible entanglement (recall (28)), and the final equality follows from Proposition 1.

Inspecting (88) and (93), it follows that $E^u_{\min}\left(\eta^{q,k'}_{A'B'}\right) = 0$. By applying Lemma 1, using the fact that $-\frac{1}{2}\log_2\left(\frac{q}{k'^2}+1-q\right) \geq 0$ for all $q \in [0,1]$ and integer $k' \geq 2$, and solving the equation $0 = -\frac{1}{2}\log_2\left(\frac{q}{k'^2}+1-q\right)$, along with the assumption that $k' \geq 2$, we conclude that $q = 0$. As such, the expected number of secret key bits distilled by the channel $\mathcal{L}^{\rightarrow}_{A^nB^n\to X_AA'B'}$ from n copies of ρ_{AB} is equal to zero. This conclusion holds for every one-way LOCC channel $\mathcal{L}^{\rightarrow}_{A^nB^n\to X_AA'B'}$, every super two-extendible state ρ_{AB}, and every $n \in \mathbb{N}$. Hence, the one-shot probabilistic one-way distillable secret key of $(\rho_{AB})^{\otimes n}$ is equal to zero for all $n \in \mathbb{N}$, and consequently, the probabilistic one-way distillable secret key of every super two-extendible state is equal to zero.

G Proof of Proposition 2

Let us restate Proposition 2 for the reader's convenience.

For all $p \in [0,1)$ and every integer $k \geq 2$, the erased private state $\widetilde{\eta}^{p,k}_{AB}$ is a super two-extendible state and thus has probabilistic one-way distillable secret key equal to zero.

Consider the following extension of an erased private state $\widetilde{\eta}^{p,k}_{AB}$:

$$\omega_{ABE} \coloneqq p\ \gamma^k_{AB} \otimes [e]_E + (1-p)\gamma^k_{AE} \otimes [e]_B, \tag{94}$$

where E is isomorphic to B. The two relevant marginals of the state ω_{ABE} are

$$\mathrm{Tr}_E[\omega_{ABE}] = p\ \gamma^k_{AB} + (1-p)\gamma^k_A \otimes [e]_B = \widetilde{\eta}^{p,k}_{AB}, \tag{95}$$

$$\mathrm{Tr}_B[\omega_{ABE}] = (1-p)\gamma^k_{AE} + p\ \gamma^k_A \otimes [e]_E = \widetilde{\eta}^{1-p,k}_{AE}, \tag{96}$$

where $\gamma^k_A \coloneqq \mathrm{Tr}_B\left[\gamma^k_{AB}\right] = \mathrm{Tr}_E\left[\gamma^k_{AE}\right]$.

Note that the min-relative entropy between two quantum states, ρ and σ, is equal to zero if $\mathrm{supp}(\rho) = \mathrm{supp}(\sigma)$. We know that $\mathrm{supp}(\widetilde{\eta}^{p,k}_{AB}) = \mathrm{supp}(\widetilde{\eta}^{1-p,k}_{AB})$ for all $p \in (0,1)$ and every integer $k \geq 2$. Therefore, we arrive at the following relations:

$$E^u_{\min}\left(\widetilde{\eta}^{p,k}_{AB}\right) \leq \frac{1}{2}D_{\min}\left(\widetilde{\eta}^{p,k}_{AB}\middle\|\widetilde{\eta}^{1-p,k}_{AB}\right) = 0 \quad \forall p \in (0,1), k \geq 2. \tag{97}$$

The min-unextendible entanglement of a bipartite state is a non-negative quantity since the underlying divergence is non-negative. Therefore,

$$E^u_{\min}\left(\widetilde{\eta}^{p,k}_{AB}\right) = 0 \quad \forall p \in (0,1), k \geq 2. \tag{98}$$

Finally, the erased private state $\widetilde{\eta}^{p,k}_{AB}$ is a separable state for $p = 0$, and the min-unextendible entanglement of a separable state is equal to zero [25, Proposition 3]. Thus, we conclude the statement of Proposition 2.

H Proof of Corollary 2

Let us restate Corollary 2 for the reader's convenience.

All full-rank states are super two-extendible states, and the probabilistic one-way distillable secret key of such quantum states is equal to zero.

Consider a bipartite quantum state that has a full-rank density operator ρ_{AB}. The quantum state $\rho_{AB} \otimes \frac{I_E}{d_E}$ is a valid extension of the state, and its marginal $\frac{1}{d_E} \operatorname{Tr}_B[\rho_{AB} \otimes I_E]$ is in the set $\mathcal{F}(\rho_{AB})$ when $E \cong B$. The min-unextendible entanglement of the state ρ_{AB} obeys the following inequality by definition:

$$E^u_{\min}(\rho_{AB}) \leq \frac{1}{2} D_{\min}\left(\rho_{AB} \middle\| \frac{1}{d_E} \operatorname{Tr}_B[\rho_{AB} \otimes I_E]\right) \tag{99}$$

$$= \frac{1}{2} D_{\min}\left(\rho_{AB} \middle\| \rho_A \otimes \frac{I_E}{d_E}\right) \tag{100}$$

$$= -\frac{1}{2} \log_2\left(\operatorname{Tr}\left[\Pi^{\rho}_{AB}\left(\rho_A \otimes \frac{I_E}{d_E}\right)\right]\right), \tag{101}$$

where Π^{ρ}_{AB} is the projection onto the support of ρ_{AB}, and $\rho_A \coloneqq \operatorname{Tr}_B[\rho_{AB}]$. Since ρ_{AB} is a full-rank density operator, the projection onto the support of ρ_{AB} is the identity operator; that is,

$$\Pi^{\rho}_{AB} = I_{AB}. \tag{102}$$

Therefore,

$$0 \leq E^u_{\min}(\rho_{AB}) \tag{103}$$

$$\leq -\frac{1}{2} \log_2\left(\frac{1}{d_E} \operatorname{Tr}[I_{AB}\,(\rho_A \otimes I_E)]\right) \tag{104}$$

$$= -\frac{1}{2} \log_2(\operatorname{Tr}[\rho_A]) \tag{105}$$

$$= 0, \tag{106}$$

where the first inequality follows from the non-negativity of the min-unextendible entanglement of states. The first equality follows from the the fact that $E \cong B$, and the last equality follows from the fact that ρ_A is a quantum state with unit trace. Since (103) and (106) hold for every full-rank state ρ_{AB}, we conclude that the min-unextendible entanglement of all full-rank states is equal to zero; that is, all full-rank states are super two-extendible.

As a consequence of Theorem 1, all full-rank states being contained in the set of super two-extendible states implies that the probabilistic one-way distillable secret key of all full-rank states is also equal to zero.

I Coherent information of Werner states

Proposition 3 *Consider a d-dimensional Werner state defined as follows:*

$$W^{p,d}_{AB} \coloneqq p \frac{I_{AB} + F_{AB}}{d(d+1)} + (1-p) \frac{I_{AB} - F_{AB}}{d(d-1)}, \tag{107}$$

where $p \in [0,1]$, $d = d_A = d_B \in \{2,3,4,\ldots\}$, and F_{AB} is the swap operator defined as $F_{AB} \coloneqq \sum_{i,j=0}^{d-1} |i\rangle\langle j|_A \otimes |j\rangle\langle i|_B$. The coherent information of the state $W^{p,d}_{AB}$ is equal to the following quantity:

$$I(A\rangle B)_{W^{p,d}} = 1 - h_2(p) - p \log_2(d+1) - (1-p) \log_2(d-1)\,. \tag{108}$$

Proof. The coherent information of a bipartite state ρ_{AB} is defined as follows [39]:

$$I(A\rangle B)_\rho \coloneqq H(\mathrm{Tr}_A[\rho_{AB}]) - H(\rho_{AB})\,, \tag{109}$$

where $H(\rho)$ is the von Neumann entropy [40], defined as

$$H(\rho) \coloneqq -\,\mathrm{Tr}[\rho \log_2 \rho]\,. \tag{110}$$

The d-dimensional Werner state defined in (107) can be rearranged into the following form:

$$W_{AB}^{p,d} = p\frac{2}{d(d+1)}\Pi_{AB}^{\mathrm{sym}} + (1-p)\frac{2}{d(d-1)}\Pi_{AB}^{\mathrm{asym}}, \tag{111}$$

where Π^{sym} and Π^{asym} are the projections onto the symmetric and asymmetric subspaces of the underlying Hilbert space, respectively. This is easily seen from the fact that the symmetric and asymmetric projection operators for a bipartite system can be written as follows:

$$\Pi_{AB}^{\mathrm{sym}} = \frac{1}{2}\left(I_{AB} + F_{AB}\right), \tag{112}$$

$$\Pi_{AB}^{\mathrm{asym}} = \frac{1}{2}\left(I_{AB} - F_{AB}\right), \tag{113}$$

where F_{AB} is the swap operator. The symmetric and asymmetric projection operators are orthogonal to each other:

$$\Pi_{AB}^{\mathrm{sym}}\Pi_{AB}^{\mathrm{asym}} = 0. \tag{114}$$

Let us first evaluate the von Neumann entropy of $\mathrm{Tr}_A\left[W_{AB}^{p,d}\right]$. Note that

$$\mathrm{Tr}_A[F_{AB}] = I_B. \tag{115}$$

Therefore,

$$\mathrm{Tr}_A[\Pi_{AB}^{\mathrm{sym}}] = \frac{d+1}{2} I_B, \tag{116}$$

$$\mathrm{Tr}_A[\Pi_{AB}^{\mathrm{asym}}] = \frac{d-1}{2} I_B, \tag{117}$$

and consequently,

$$\mathrm{Tr}_A\left[W_{AB}^{p,d}\right] = \frac{p}{d} I_B + \frac{1-p}{d} I_B = \frac{I_B}{d}, \tag{118}$$

which is the maximally mixed state on system B. The von Neumann entropy of a d-dimensional maximally mixed state is equal to $\log_2 d$. Therefore,

$$H\left(\mathrm{Tr}_A\left[W_{AB}^{p,d}\right]\right) = \log_2 d. \tag{119}$$

Now let us evaluate the von Neumann entropy of the Werner state $W_{AB}^{p,d}$:

$$H\left(W_{AB}^{p,d}\right) = -\,\mathrm{Tr}\left[W_{AB}^{p,d} \log_2 W_{AB}^{p,d}\right]. \tag{120}$$

Since Π_{AB}^{sym} and Π_{AB}^{asym} are orthogonal to each other, we can reduce the von Neumann entropy of the Werner state into the following form:

$$H\left(W_{AB}^{p,d}\right) = -\operatorname{Tr}\left[p\frac{2}{d(d+1)}\Pi_{AB}^{\mathrm{sym}}\log_2\left(p\frac{2}{d(d+1)}\Pi_{AB}^{\mathrm{sym}}\right)\right] - \operatorname{Tr}\left[\frac{2(1-p)}{d(d-1)}\Pi_{AB}^{\mathrm{asym}}\log_2\left(\frac{2(1-p)}{d(d-1)}\Pi_{AB}^{\mathrm{asym}}\right)\right]. \quad (121)$$

The eigenvalues of a projection operator are either equal to one or zero. Hence, for an arbitrary scalar α and an arbitrary projection operator Π^x,

$$\log_2(\alpha\Pi^x) = \Pi^x \log_2 \alpha. \quad (122)$$

Therefore,

$$H\left(W_{AB}^{p,d}\right) = -p\frac{2}{d(d+1)}\log_2\left(p\frac{2}{d(d+1)}\right)\operatorname{Tr}[\Pi_{AB}^{\mathrm{sym}}] - (1-p)\frac{2}{d(d-1)}\log_2\left((1-p)\frac{2}{d(d-1)}\right)\operatorname{Tr}[\Pi_{AB}^{\mathrm{asym}}]. \quad (123)$$

From (116) and (117), it is straightforward to see the following equalities:

$$\operatorname{Tr}[\Pi_{AB}^{\mathrm{sym}}] = \frac{d(d+1)}{2}, \quad (124)$$

$$\operatorname{Tr}[\Pi_{AB}^{\mathrm{asym}}] = \frac{d(d-1)}{2}. \quad (125)$$

Substituting these values in (128), we arrive at the following expression for the von Neumann entropy of the Werner state:

$$H\left(W_{AB}^{p,d}\right) = -p\log_2\left(p\frac{2}{d(d+1)}\right) - (1-p)\log_2\left((1-p)\frac{2}{d(d-1)}\right) \quad (126)$$

$$= h_2(p) + p\log_2(d(d+1)) - p + (1-p)\log_2(d(d-1)) - (1-p) \quad (127)$$

$$= \log_2 d + h_2(p) - 1 + p\log_2(d+1) + (1-p)\log_2(d-1), \quad (128)$$

where $h_2(p) \coloneqq -p\log_2 p - (1-p)\log_2(1-p)$. Combining (109), (119), and (128), we conclude (108). ■

J Coherent information of isotropic states

Proposition 4 *Consider a d-dimensional isotropic state $\zeta_{AB}^{F,d}$ which is defined as follows:*

$$\zeta_{AB}^{F,d} = F\ \Phi_{AB}^{d} + (1-F)\frac{I_{AB} - \Phi_{AB}^{d}}{d^2-1}, \quad (129)$$

where $F \in [0,1]$ and $d = d_A = d_B \in \{2,3,4,\ldots\}$. The coherent information of the state $\zeta_{AB}^{F,d}$ is equal to the following quantity:

$$I(A\rangle B)_{\zeta^{F,d}} = \log_2 d - h_2(F) - (1-F)\log_2(d^2-1), \quad (130)$$

where $h_2(x) \coloneqq -x\log_2 x - (1-x)\log_2(1-x)$.

Proof. Recall the definition of coherent information of a bipartite state ρ_{AB} from (109):

$$I(A\rangle B)_{\rho} \coloneqq H(\mathrm{Tr}_A[\rho_{AB}]) - H(\rho_{AB})\,. \tag{131}$$

The marginal of the isotropic state on either systems, A or B, is equal to the maximally mixed state for all $F \in [0,1]$ and $d \geq 2$. Therefore,

$$H\Big(\mathrm{Tr}_B\Big[\zeta_{AB}^{F,d}\Big]\Big) = H\left(\frac{I_A}{d}\right) = \log_2 d. \tag{132}$$

Now let us evaluate the von Neumann entropy of the isotropic state. Note that Φ_{AB}^d and $I_{AB} - \Phi_{AB}^d$ are orthogonal projectors. This implies the following equalities:

$$\begin{aligned}
H\Big(\zeta_{AB}^{F,d}\Big) &= -\,\mathrm{Tr}\Big[\zeta_{AB}^{F,d}\log_2\zeta_{AB}^{F,d}\Big] && (133)\\
&= -\,\mathrm{Tr}\Big[F\Phi_{AB}^d\log_2\Big(F\Phi_{AB}^d\Big)\Big] - \mathrm{Tr}\Big[\frac{1-F}{d^2-1}\Big(I_{AB}-\Phi_{AB}^d\Big)\log_2\Big(\frac{1-F}{d^2-1}\Big(I_{AB}-\Phi_{AB}^d\Big)\Big)\Big] && (134)\\
&= -F\log_2 F\,\mathrm{Tr}\Big[\Phi_{AB}^d\Big] - \frac{1-F}{d^2-1}\log_2\Big(\frac{1-F}{d^2-1}\Big)\,\mathrm{Tr}\Big[I_{AB}-\Phi_{AB}^d\Big] && (135)\\
&= -F\log_2 F - (1-F)\log_2\Big(\frac{1-F}{d^2-1}\Big) && (136)\\
&= -F\log_2 F - (1-F)\log_2(1-F) + (1-F)\log_2\Big(d^2-1\Big) && (137)\\
&= h_2(F) + (1-F)\log_2\Big(d^2-1\Big)\,, && (138)
\end{aligned}$$

where we have used the property of projection operators mentioned in (122) to arrive at the third equality. Substituting (132) and (138) in the definition of coherent information, we arrive at (130). This concludes the proof. ■