Commun. Math. Phys. (2024) 405:261
Digital Object Identifier (DOI) https://doi.org/10.1007/s00220-024-05121-4

Communications in
Mathematical Physics

Generalised Entropy Accumulation

Tony Metger[1], **Omar Fawzi**[2], **David Sutter**[3], **Renato Renner**[1]

[1] Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland. E-mail: tmetger@ethz.ch

[2] Univ Lyon, Inria, ENS Lyon, UCBL, LIP, 69342 Lyon, France.

[3] IBM Quantum, IBM Research Europe, Zurich, Switzerland.

Received: 19 March 2023 / Accepted: 12 August 2024

Abstract: Consider a sequential process in which each step outputs a system A_i and updates a side information register E. We prove that if this process satisfies a natural "non-signalling" condition between past outputs and future side information, the min-entropy of the outputs $A_1, \ldots, A_n$ conditioned on the side information E at the end of the process can be bounded from below by a sum of von Neumann entropies associated with the individual steps. This is a generalisation of the entropy accumulation theorem (EAT) (Dupuis et al. in Commun Math Phys 379: 867–913, 2020), which deals with a more restrictive model of side information: there, past side information cannot be updated in subsequent rounds, and newly generated side information has to satisfy a Markov condition. Due to its more general model of side-information, our generalised EAT can be applied more easily and to a broader range of cryptographic protocols. As examples, we give the first multi-round security proof for blind randomness expansion and a simplified analysis of the E91 QKD protocol. The proof of our generalised EAT relies on a new variant of Uhlmann's theorem and new chain rules for the Rényi divergence and entropy, which might be of independent interest.

Contents

Published online: 12 October 2024

1. Introduction

Suppose that Alice and Eve share a quantum state ρ_{A^nE}. From her systems $A^n := A_1 \dots A_n$, Alice would like to extract bits that look uniformly random to Eve, except with some small failure probability ε [1]. The number of such random bits that Alice can extract is given by the smooth min-entropy $H_{\min}^{\varepsilon}(A^n|E)_\rho$ [2]. This quantity plays a central role in quantum cryptography: for example, the main task in security proofs of quantum key distribution (QKD) protocols is usually finding a lower bound for the smooth min-entropy.

Unfortunately, for many cryptographic protocols deriving such a bound is challenging. Intuitively, the reason is the following: the state ρ_{A^nE} is usually created as the output of a multi-round protocol, where each round produces one of Alice's systems A_i and allows Eve to execute some attack to gain information about $A_1, \dots, A_i$. These attacks can depend on each other, i.e., Eve may use what she learnt in round $i-1$ to plan her attack in round i. This non-i.i.d. nature of the attacks makes it hard to find a lower bound on $H_{\min}^{\varepsilon}(A^n|E)_\rho$ that holds for any possible attack that Eve can execute. In contrast, it is typically much easier to compute a conditional von Neumann entropy associated with a single-round of the protocol, where the non-i.i.d. nature of Eve's attack plays no role. Therefore, it is desirable to relate the smooth min-entropy of the output of the multi-round protocol to the von Neumann entropies associated with the individual rounds.

From an information-theoretic point of view, this question can be phrased as follows: can the smooth min-entropy $H_{\min}^{\varepsilon}(A^n|E)_\rho$ be bounded from below in terms of von Neumann entropies $H(A_i|E_i)_{\rho^i_{A_iE_i}}$ for some (yet to be determined) systems E_i and states $\rho^i_{A_iE_i}$ related to ρ? While for general states ρ_{A^nE} no useful lower bound can be found, previous works have established such bounds under additional assumptions on the state ρ_{A^nE}.

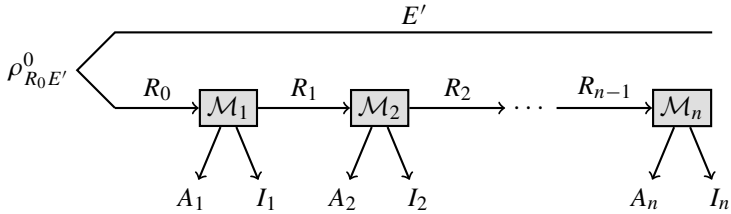
The first bound of this form was proven via the *asymptotic equipartition property* (AEP) [3]. It assumes that the system E is n-partite (i.e., we replace E by $E^n = E_1 \dots E_n$) and that the state $\rho_{A^nE^n} = \rho_{A_1E_1} \otimes \dots \otimes \rho_{A_nE_n}$ is a product of identical states. Then, the AEP shows that[1]

$$H_{\min}^{\varepsilon}(A^n|E^n)_\rho \geq \sum_{i=1}^{n} H(A_i|E_i)_\rho - O(\sqrt{n}) \,.$$

For applications in cryptography, the assumption that ρ is an i.i.d. product state is usually too strong: it corresponds to the (unrealistic) assumption that Eve executes the same independent attack in each round, a so-called *collective attack*.

[1] Since ρ is a product of identical states, all of the terms $H(A_i|E_i)_\rho$ are equal, i.e., $\sum_{i=1}^{n} H(A_i|E_i)_\rho = nH(A_i|E_i)_\rho$ for any i. We write the sum here explicitly to highlight the analogy with the EAT presented below.

The *entropy accumulation theorem* (EAT) [1] is a generalisation of the AEP which requires far weaker assumptions on the state $\rho_{A^n E}$. Specifically, the EAT considers states that result from a sequential process that starts with a state $\rho^0_{R_0 E'}$ and in every step outputs a system A_i and a piece of side information I_i. The system E' is not acted upon during the process. The full side information at the end of this process is $E = I_1 \dots I_n E'$. We can represent such a process by the following diagram, where $\mathcal{M}_i$ are quantum channels.



The EAT requires an additional condition on the side information: the new side information I_i generated in round i must be independent from the past outputs A^{i-1} conditioned on the existing side information $I^{i-1}E'$. Mathematically, this is captured by the condition that the systems $A^{i-1} \leftrightarrow I^{i-1}E' \leftrightarrow I_i$ form a Markov chain for any initial state $\rho^0_{R_0 E'}$. With this Markov condition, the EAT states that[2]

$$H^{\varepsilon}_{\min}(A^n|I^n E')_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0_{R_0 E'})} \geq \sum_{i=1}^{n} \inf_{\omega} H(A_i|I_i \tilde{E})_{\mathcal{M}_i(\omega)} - O(\sqrt{n}) \,, \tag{1.1}$$

where $\tilde{E}$ is a purifying system isomorphic to R_{i-1} and the infimum is taken over all states ω on systems $R_{i-1}\tilde{E}$.[3]

Let us discuss the model of side information used by the EAT in more detail. The EAT considers side information consisting of two parts: the initial side information E' (which is not acted upon during the process) and the outputs $I^n = I_1 \dots I_n$. This splitting of side information into a "static" part E' and a part I^n which is generated in each step of the process is particularly suited to device-independent cryptography: there, Eve prepares a device in an initial state $\rho^0_{R_0 E'}$, where R_0 is the device's internal memory and E' is Eve's initial side information from preparing the device. Then, Alice (and Bob, though we only consider Alice's system here) executes a multi-round protocol with this device, where each round leaks some additional piece of information I_i to Eve, so that Eve's side information at the end of the protocol is $I^n E'$. Indeed, the EAT has been used to establish tight security proofs in the device-independent setting, see e.g., [4,5].

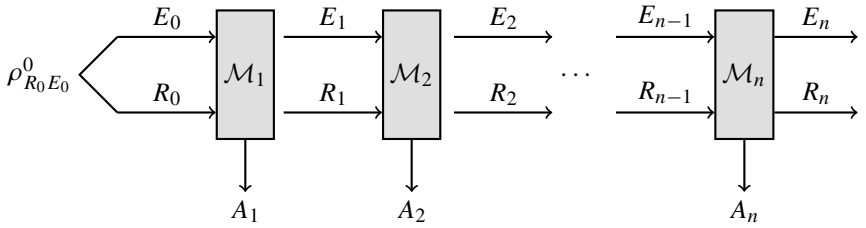
The Markov condition in the EAT captures the following intuition: if we want to find a bound on $H^{\varepsilon}_{\min}(A^n|I^n E')$ in terms of single-round quantities, it is required that side information about A_i is itself output in step i, as otherwise we cannot hope to estimate the contribution to the total entropy from step i. To illustrate what could happen without such a condition, consider a case where A_i is classical and no side information is output in the first $n-1$ rounds, but the side information I_n in the last round contains a copy of the systems A^n (which can be passed along during the process in the systems R_i). Then,

[2] The EAT from [1] also makes an analogous statement about an upper bound on the max-entropy $H_{\max}$. We derive a generalisation of that statement in Appendix A but only focus on $H_{\min}$ in the introduction and main text since that is the case that is typically relevant for applications.

[3] In fact, the EAT is more general in that it allows taking into account observed statistics to restrict the minimization over $\omega_{A_i B_i E}$, but we restrict ourselves to the simpler case without statistics in this introduction.

clearly $H_{\min}^{\varepsilon}(A^n|I^nE') = 0$, but for the first $n-1$ rounds, each single-round entropy bound that only considers the systems A_i and I_i can be positive.

Main result In this work, we further relax the assumptions on how the final state ρ_{A^nE} is generated. Specifically, we consider sequential processes as in the EAT, but with a fully general model of side information, i.e., the side information can be updated in each step in the process. Diagrammatically, such a process can be represented as follows:



Our generalised EAT then states the following.

Theorem 1.1. *Consider quantum channels $\mathcal{M}_i : R_{i-1}E_{i-1} \to A_iR_iE_i$ that satisfy the following "non-signalling" condition (discussed in detail below): for each $\mathcal{M}_i$, there must exist a quantum channel $\mathcal{R}_i : E_{i-1} \to E_i$ such that*

$$\mathrm{Tr}_{A_iR_i} \circ \mathcal{M}_i = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}} . \tag{1.2}$$

Then, the min-entropy of the outputs A^n conditioned on the final side information E_n can be bounded as

$$H_{\min}^{\varepsilon}(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho^0_{R_0E_0})} \geq \sum_{i=1}^{n} \inf_{\omega} H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} - O(\sqrt{n}) , \tag{1.3}$$

where $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}$ is a purifying system for the input to $\mathcal{M}_i$ and the infimum is taken over all states ω on systems $R_{i-1}E_{i-1}\tilde{E}_{i-1}$.[4]

We give a formal statement and proof in Sect. 4 and also show that, similarly to the EAT, statistics collected during the process can be used to restrict the minimization over ω (see Theorem 4.3 for the formal statement). By a simple duality argument, Eq. (1.3) also implies an upper bound on the smooth max-entropy $H_{\max}$, which we explain in Appendix A. This generalises a similar result from [1], although in [1] one could not make use of duality due to the Markov condition and instead had to prove the statement about $H_{\max}$ separately, again highlighting that our generalised EAT is easier to work with.

The intuition behind the non-signalling condition in our generalised EAT is similar to the Markov condition in the original EAT: by the same reasoning as for the Markov condition, since the lower bound is made up of terms of the form $H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}$, it is required that side information about A_i that is present in the final system E_n is already present in E_i. This means that side information about A_i should not be passed on via the R-systems and later be included in the E-systems. The non-signalling condition captures this requirement: it demands that if one only considers the marginal of the new

[4] As usual, the channels $\mathcal{M}_i$ act as identity on any additional systems that may be part of the input state, i.e. $\mathcal{M}_i(\omega_{R_{i-1}E_{i-1}\tilde{E}_{i-1}}) = (\mathcal{M}_i \otimes \mathrm{id}_{\tilde{E}_{i-1}})(\omega_{R_{i-1}E_{i-1}\tilde{E}_{i-1}})$ is a state on $A_iR_iE_i\tilde{E}_{i-1}$. In particular, the register $\tilde{E}_{i-1}$ containing a purification of the input is also part of the output state.

side information E_i (without the new output A_i), it must be possible to generate this state from the past side information E_{i-1} alone, without access to the system R_{i-1}. This means that any side information that E_i contains about the past outputs $A_1 \dots A_{i-1}$ must have essentially already been present in E_{i-1} and could not have been stored in R_{i-1}.

The name "non-signalling condition" is due to the fact that Eq. (1.2) is a natural generalisation of the standard non-signalling conditions in non-local games: if we view the systems R_{i-1} and $R_i A_i$ as the inputs and outputs on "Alice's side" of $\mathcal{M}_i$, and E_{i-1} and E_i as the inputs and outputs on "Eve's side", then Eq. (1.2) states that the marginal of the output on Eve's side cannot depend on the input on Alice's side. This is exactly the non-signalling condition in non-local games, except that here the inputs and outputs are allowed to be fully quantum.

To understand the relation between the Markov and non-signalling conditions, it is instructive to consider the setting of the original EAT as a special case of our generalised EAT. In the original EAT, the full side information available after step i is $E'I^i$, and past side information is not updated during the process. For our generalised EAT, we therefore set $E_i = E'I^i$ and consider maps $\mathcal{M}_i = \mathcal{M}'_i \otimes \mathrm{id}_{E_{i-1}}$, where $\mathcal{M}'_i : R_{i-1} \to A_i I_i R_i$ is the map used in the original EAT. We need to check that with this choice of systems and maps, the Markov condition of the original EAT implies the non-signalling condition of our generalised EAT. The Markov condition requires that for any state input $\omega^{i-1}_{A^{i-1}I^{i-1}R_{i-1}E'}$, the output state $\omega^i_{A^iI^iR_iE'} = \mathcal{M}_i(\omega^{i-1})$ satisfies $A^{i-1} \leftrightarrow I^{i-1}E' \leftrightarrow I_i$.[5] It is then a standard result on quantum Markov chains [6] that there must exist a quantum channel $\mathcal{R}_i : I^{i-1}E' \to I^iE'$ such that $\omega^i_{I^iE'} = \mathcal{R}_i(\omega^{i-1}_{I^{i-1}E'})$. Remembering that we defined $E_i = E'I^i$ (so that $\mathcal{R}_i : E_{i-1} \to E_i$) and adding the systems A^{i-1} (on which both $\mathcal{M}_i$ and $\mathcal{R}_i$ act as identity), we find that $\mathcal{M}_i$ satisfies the non-signalling condition:

$$\mathrm{Tr}_{A_iR_i} \circ \mathcal{M}_i(\omega^{i-1}_{A^{i-1}R_{i-1}E_{i-1}}) = \omega^i_{A^{i-1}E_i} = \mathcal{R}_i(\omega^{i-1}_{A^{i-1}E_{i-1}}) = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}(\omega^{i-1}_{A^{i-1}R_{i-1}E_{i-1}}) .$$

Then, noting that all conditioning systems on which $\mathcal{M}_i$ acts as the identity map can collectively be replaced by a single purifying system isomorphic to the input, we see that we recover the original EAT (Eq. (1.1)) from our generalised EAT (Eq. (1.3)).

We emphasise that while the original EAT with the Markov condition can be recovered as a special case, our model of side information and the non-signalling condition are much more general than the original EAT; arguably, for a sequential process they are the most natural and general way of expressing the notion that future side information should not contain new information about past outputs, which appears to be necessary for an EAT-like result. To demonstrate the greater generality of our result, in Sect. 5 we use it to give the first multi-round proof for blind randomness expansion, a task to which the original EAT could not be applied, and a more direct proof of the E91 QKD protocol than was possible with the original EAT. Our generalised EAT can also be used to prove security of a much larger class of QKD protocols than the original EAT. Interestingly, for (device-dependent) QKD protocols, no "hidden system" R is needed and therefore the non-signalling condition is trivially satisfied, i.e., the advantage of our generalised EAT for QKD security proofs stems entirely from the more general model of side information, not from replacing the Markov condition by the non-signalling condition; see Sect. 5.2

[5] Strictly speaking, the EAT as stated in [1] only requires that this Markov property holds for any input state ω^{i-1} in the image of the previous maps $\mathcal{M}_{i-1} \circ \dots \circ \mathcal{M}_1$. The same is true for the non-signalling condition, i.e., one can check that our proof of the generalised EAT still works if the map $\mathcal{R}_i$ only satisfies Eq. (1.2) on states in the image of $\mathcal{M}_{i-1} \circ \dots \circ \mathcal{M}_1$. To simplify the presentation, we use the stronger condition Eq. (1.2) throughout this paper.

for an informal comparison of how the original and generalised EAT can be applied to QKD, and [7] for a detailed treatment of the application of our generalised EAT to QKD, including protocols to which the original EAT could not be applied.

Proof sketch. The generalised EAT involves both the min-entropy, which can be viewed as a "worst-case entropy", and the von Neumann entropy, which can be viewed as an "average case entropy". These two entropies are special cases of a more general family of entropies called Rényi entropies, which are denoted by H_α for a parameter $\alpha > 1$ (see Sect. 2.2 for a formal definition).[6] The min-entropy can be obtained from the Rényi entropy by taking $\alpha \to \infty$, whereas the von Neumann entropy corresponds to the limit $\alpha \to 1$. Hence, the Rényi entropies interpolate between the min-entropy and the von Neumann entropy, and they will play a crucial role in our proof.

The key technical ingredient for our generalised EAT is a new chain rule for Rényi entropies (Theorem 3.6 in the main text).

Lemma 1.2. *Let $\alpha \in (1, 2)$, ρ_{ARE} a quantum state, and $\mathcal{M} : RE \to A'R'E'$ a quantum channel which satisfies the non-signalling condition in Eq. (1.2), i.e. there exists a channel $\mathcal{R} : E \to E'$ such that $\mathrm{Tr}_{A'R'} \circ \mathcal{M} = \mathcal{R} \circ \mathrm{Tr}_R$. Then*

$$H_\alpha(AA'|E')_{\mathcal{M}(\rho)} \geq H_\alpha(A|E)_\rho + \inf_{\omega_{RE\tilde{E}}} H_{\frac{1}{2-\alpha}}(A'|E'\tilde{E})_{\mathcal{M}(\omega)} \tag{1.4}$$

for a purifying system $\tilde{E} \equiv RE$, where the infimum is over all quantum states ω on systems $RE\tilde{E}$.

We first describe how this chain rule implies our generalised EAT, following the same idea as in [1,8]. For this, recall that our goal is to find a lower bound on $H^\varepsilon_{\min}(A^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0_{R_0E_0})}$ for a sequence of maps satisfying the non-signalling condition $\mathrm{Tr}_{A_iR_i} \circ \mathcal{M}_i = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}$. As a first step, we use a known relation between the smooth min-entropy and the Rényi entropy [3], which (up to a small penalty term depending on ε and α) reduces the problem to lower-bounding

$$H_\alpha(A^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0_{R_0E_0})} = H_\alpha(A_nA^{n-1}|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0_{R_0E_0})}\,.$$

To this, we can apply Lemma 1.2 by choosing $A = A^{n-1}$, $A' = A_n$, $E = E_{n-1}$, $E' = E_n$, $R = R_{n-1}$, $R' = R_n$, and $\rho = \mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1(\rho^0_{R_0E_0})$. Then, since the map $\mathcal{M}_n$ satisfies the non-signalling condition, Lemma 1.2 implies that

$$\begin{aligned} H_\alpha(A_1^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E_0})} \geq\ & H_\alpha(A_1^{n-1}|E_{n-1})_{\mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E_0})} \\ & + \inf_{\omega \in \mathrm{S}(R_{n-1}E_{n-1}\tilde{E}_{n-1})} H_{\frac{1}{2-\alpha}}(A_n|E_n\tilde{E}_{n-1})_{\mathcal{M}_n(\omega)}\,. \end{aligned}$$

We can now repeat this argument for the term $H_\alpha(A_1^{n-1}|E_{n-1})_{\mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E_0})}$. After n applications of Lemma 1.2, we find that

$$H_\alpha(A_1^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E_0})} \geq \sum_{i=1}^n \inf_{\omega \in \mathrm{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H_{\frac{1}{2-\alpha}}(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}\,.$$

[6] We note that the definition of Rényi entropies can be extended to $\alpha < 1$, but we will only need the case $\alpha > 1$.

To conclude, we use a continuity bound from [8] to relate $H_{\frac{1}{2-\alpha}}(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}$ to $H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}$. It can be shown that for a suitable choice of α, the penalty terms we incur by switching from the min-entropy to the Rényi entropy and then to the von Neumann entropy scale as $O(\sqrt{n})$. Therefore, we obtain Eq. (1.3). We also provide a version that allows for "testing" (which is crucial for application in quantum cryptography and explained in detail in Sect. 4.2) and features explicit second-order terms similar to those in [8].

We now turn our attention to the proof of Lemma 1.2. For this, we need to introduce the (sandwiched) Rényi divergence of order α between two (possibly unnormalised) quantum states ρ and σ, denoted by $D_\alpha\big(\rho \,\big\|\, \sigma\big)$. We refer to Sect. 2.2 for a formal definition; for this overview, it suffices to know that $D_\alpha\big(\rho \,\big\|\, \sigma\big)$ is a measure of how different ρ is from σ, and that the conditional Rényi entropy is related to the Rényi divergence by

$$H_\alpha(A|B)_\rho = -D_\alpha\big(\rho_{AB} \,\big\|\, \mathbb{1}_A \otimes \rho_B\big) \ .$$

Our starting point for proving Lemma 1.2 is the following chain rule for the Rényi divergence from [9]:

$$D_\alpha\big(\mathcal{M}(\rho) \,\big\|\, \mathcal{F}(\sigma)\big) \leq D_\alpha\big(\rho_{ARE} \,\big\|\, \sigma_{ARE}\big) + \lim_{n\to\infty} \frac{1}{n} \sup_{\omega_{R^nE^n\tilde{E}^n}} D_\alpha\big(\mathcal{M}^{\otimes n}(\omega) \,\big\|\, \mathcal{F}^{\otimes n}(\omega)\big) \ , \tag{1.5}$$

where $\mathcal{M}$ and $\mathcal{F}$ are (not necessarily trace preserving) quantum channels from RE to $A'R'E'$, and ρ and σ are any quantum states on ARE. The optimization is over all quantum states ω on n copies of the systems $RE\tilde{E}$ (with $\tilde{E} \equiv RE$ as before).

Making a suitable choice of $\mathcal{F}$ (which depends on $\mathcal{M}$) and σ (which depends on ρ), one can turn Eq. (1.5) into the following chain rule for the conditional Rényi entropy:

$$H_\alpha(AA'|E')_{\mathcal{M}(\rho)} \geq H_\alpha(A|RE)_\rho + \lim_{n\to\infty} \frac{1}{n} \inf_{\omega_{R^nE^n\tilde{E}^n}} H_\alpha((A')^n|(E')^n\tilde{E}^n)_{\mathcal{M}^{\otimes n}(\omega)} \ . \tag{1.6}$$

This chain rule resembles Lemma 1.2, but is significantly weaker and cannot be used to prove a useful entropy accumulation theorem. The reason for this is twofold:

(i) Equation (1.6) provides a lower bound in terms of $H_\alpha(A|RE)$, not $H_\alpha(A|E)$. The additional conditioning on the R-system can drastically lower the entropy: for example, in a device-independent scenario, R would describe the internal memory of the device. Then, Alice's output A contains no entropy when conditioned on the internal memory of the device that produced the output, i.e. $H_\alpha(A|RE) = 0$. On the other hand, Alice's output conditioned only on Eve's side information E may be quite large (and can usually be certified by playing a non-local game), i.e. $H_\alpha(A|E) > 0$.

(ii) Equation (1.6) contains the regularised quantity $\lim_{n\to\infty} \frac{1}{n} \inf_{\omega_{R^nE^n\tilde{E}^n}} H_\alpha((A')^n|(E')^n\tilde{E}^n)_{\mathcal{M}^{\otimes n}(\omega)}$. Due to the limit $n \to \infty$, this quantity cannot be computed numerically and therefore the bound in Eq. (1.6) cannot be evaluated for concrete examples.

We now describe how we overcome each of these issues in turn.

(i) We prove a new variant of Uhlmann's theorem [10], a foundational result in quantum information theory. The original version of Uhlmann's theorem deals with the case of $\alpha = 1/2$; we show that for $\alpha > 1$, a similar result holds, but an additional regularisation is required. Concretely, we prove that for any states ρ_{ARE} and σ_{AE}:

$$\lim_{k\to\infty} \frac{1}{k} \inf_{\substack{\hat{\sigma}_{A^kR^kE^k} \\ \text{s.t. } \hat{\sigma}_{A^kE^k} = \sigma_{AE}^{\otimes k}}} D_\alpha\left(\rho_{ARE}^{\otimes k} \,\middle\|\, \hat{\sigma}_{A^kR^kE^k}\right) = D_\alpha\left(\rho_{AE} \,\middle\|\, \sigma_{AE}\right) . \tag{1.7}$$

The proof of this result relies heavily on the spectral pinching technique [11,12] and we refer to Lemma 3.3 for details as well as a non-asymptotic statement with explicit error bounds. We make use of this extended Uhlmann's theorem as follows: for the case we are interested in, the map $\mathcal{F}$ in Eq. (1.5) satisfies a non-signalling condition. We can show that this condition implies that for any state $\hat{\sigma}_{A^kR^kE^k}$ s.t. $\hat{\sigma}_{A^kE^k} = \sigma_{AE}^{\otimes k}$:

$$D_\alpha\left(\mathcal{M}(\rho) \,\middle\|\, \mathcal{F}(\sigma)\right) = \frac{1}{k} D_\alpha\left(\mathcal{M}^{\otimes k}(\rho_{ARE}^{\otimes k}) \,\middle\|\, \mathcal{F}^{\otimes k}(\hat{\sigma}_{A^kR^kE^k})\right) .$$

Applying Eq. (1.5) to the r.h.s. of this equality results in a bound that contains $D_\alpha\left(\rho_{ARE}^{\otimes k} \,\middle\|\, \hat{\sigma}_{A^kR^kE^k}\right)$. We can now minimise over all states $\hat{\sigma}_{A^kR^kE^k}$ s.t. $\hat{\sigma}_{A^kE^k} = \sigma_{AE}^{\otimes k}$ and take the limit $k \to \infty$. Then, Eq. (1.7) allows us to drop the R-system. Therefore, under the non-signalling condition on $\mathcal{F}$, we obtain the following improved chain rule for the sandwiched Rènyi divergence, which might be of independent interest:

$$D_\alpha\left(\mathcal{M}(\rho) \,\middle\|\, \mathcal{F}(\sigma)\right) \leq D_\alpha\left(\rho_{AE} \,\middle\|\, \sigma_{AE}\right) + \lim_{n\to\infty} \frac{1}{n} \sup_{\omega_{R^nE^n\tilde{E}^n}} D_\alpha\left(\mathcal{M}^{\otimes n}(\omega) \,\middle\|\, \mathcal{F}^{\otimes n}(\omega)\right) .$$

Using this chain rule, we can show that Eq. (1.6) still holds if $H_\alpha(A|RE)$ is replaced by $H_\alpha(A|E)$.

(ii) To remove the need for a regularisation in Eq. (1.6), we show that due to the permutation-invariance of $\mathcal{M}^{\otimes n}$ and $\mathcal{F}^{\otimes n}$, for $\alpha > 1$ and $n \to \infty$ one can replace the optimization over $\omega_{R^nE^n\tilde{E}^n}$ with a fixed input state, namely the projector onto the symmetric subspace of $R^nE^n\tilde{E}^n$. For this replacement, one incurs a small loss in α, replacing it by $\frac{1}{2-\alpha}$ (which is only slightly larger than α in the typical regime where α is close to 1). The projector onto the symmetric subspace has a known representation as a mixture of tensor product states [13]. Combining these two steps, we show that the optimization over $\omega_{R^nE^n\tilde{E}^n}$ can be restricted to tensor product states, which means that the regularisation in Eq. (1.6) can be removed (see Sect. 3.2 for details):

$$\lim_{n\to\infty} \frac{1}{n} \inf_{\omega_{R^nE^n\tilde{E}^n}} H_\alpha((A')^n|(E')^n\tilde{E}^n)_{\mathcal{M}^{\otimes n}(\omega)} \geq \inf_{\omega_{RE\tilde{E}}} H_{\frac{1}{2-\alpha}}(A'|E'\tilde{E})_{\mathcal{M}(\omega)} .$$

Combining these results yields Lemma 1.2 and, as a result, our generalised EAT.

Sample application: blind randomness expansion. The main advantage of the generalised EAT over previous results is its broader applicability. For example, as demonstrated in [7], the generalised EAT can be used to prove the security of prepare-and-measure QKD protocols, which is of immediate practical relevance, and can also simplify the analysis of entanglement-based QKD protocols as discussed in Sect. 5.2. Here, we focus on the application of our generalised EAT to mistrustful device-independent (DI) cryptography.

In mistrustful DI cryptography, multiple parties each use a quantum device to execute a protocol with one another. Each party trusts neither its quantum device nor the other parties in the protocol. Hence, from the point of view of one party, say Alice, all the remaining parties in the protocol are collectively treated as an adversary Eve, who may also have prepared Alice's untrusted device.

While the original EAT could be used to analyse DI protocols in which the parties trust each other, e.g. DIQKD [14], the setting of mistrustful DI cryptography is significantly harder to analyse because the adversary Eve actively participates in the protocol and may update her side information during the protocol in arbitrary ways. Analysing such protocols requires the more general model of side information we deal with in this paper. As a concrete example for mistrustful DI cryptography, we consider blind randomness expansion, a primitive introduced in [15]. Previous work [15,16] could only analyse blind randomness expansion under the i.i.d. assumption. Here, we give the first proof that blind randomness expansion is possible for general adversaries. The proof is a straightforward application of our generalised EAT and briefly sketched below; we refer to Sect. 5.1 for a detailed treatment.

In blind randomness expansion, Alice receives an untrusted quantum device from the adversary Eve. Alice then plays a non-local game, e.g. the CHSH game, with this device and Eve, and wants to extract certified randomness from her outputs of the non-local game, i.e. we need to show that Alice's outputs contain a certain amount of min-entropy conditioned on Eve's side information. Concretely, in each round of the protocol Alice samples inputs x and y for the non-local game, inputs x into her device to receive outcome a, and sends y to Eve to receive outcome b; Alice then checks whether (x, y, a, b) satisfies the winning condition of the non-local game. For comparison, recall that in standard DI randomness expansion [17–21], Alice receives two devices from Eve and uses them to play the non-local game. This means that in standard DI randomness expansion, Eve never learns any of the inputs and outputs of the game. In contrast, in blind randomness expansion Eve learns one of the inputs, y, and is free to choose one of the outputs, b, herself. Hence, Eve can choose the output b based on past side information and update her side information in each round of the protocol using the values of y and b.

To analyse such a protocol, we use the setting of Theorem 1.1, with A_i representing the output of Alice's device D from the non-local game in the i-th round, R_i the internal memory of D after the i-th round, and E_i Eve's side information after the i-th round, which can be generated arbitrarily from entanglement shared between Eve and D at the start of the protocol and information Eve gathered during the first i rounds of the protocol. The map $\mathcal{M}_i$ describes one round of the protocol, and because Alice's device and Eve cannot communicate during the protocol it is easy to show that the non-signalling condition from Theorem 1.1 is satisfied. Therefore, we can apply Theorem 1.1 to lower-bound Alice's conditional min-entropy $H_{\min}(A^n|E_n)$ in terms of the single-round quantities $\inf_\omega H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}$.[7] This single-round quantity corresponds to the i.i.d. scenario, i.e. the generalised EAT has reduced the problem of showing blind randomness expansion against general adversaries to the (much simpler) problem of showing it against i.i.d. adversaries. The quantity $\inf_\omega H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}$ can be computed using a general numerical technique [22], and for certain classes of non-local games it may also be possible to find an analytical lower bound using ideas from [15,16].

[7] In fact, in order for this single-round quantity to be positive one has to restrict the infimum to input states that allow the non-local game to be won with a certain probability. This requires using the generalised EAT with testing (Sect. 4.2), not Theorem 1.1. We refer to Sect. 5.1 for details.

Inserting the single-round bound, we obtain a lower bound on $H_{\min}(A^n|E_n)$ that scales linearly with n, showing that blind randomness expansion is possible against general adversaries. We also note that as explained in [15], this result immediately implies that *unbounded* randomness expansion is possible with only three devices, whereas previous works required four devices [21,23,24].

Future work In this work, we have developed a new information-theoretic tool, the generalised EAT. The generalised EAT deals with a more general model of side information than previous techniques and is therefore more broadly and easily applicable. In particular, our generalised EAT can be used to analyse mistrustful DI cryptography. We have demonstrated this by giving the first proof of blind randomness expansion against general adversaries. We expect that the generalised EAT could similarly be used for other protocols such as two-party cryptography in the noisy storage model [25] or certified deletion [16,26,27]. In addition to mistrustful DI cryptography, our result can also be used to give new proofs for device-dependent QKD, as demonstrated in Sect. 5.2 and [7], and is applicable to proving the security of commercial quantum random number generators, which typically have correlations between rounds due to experimental imperfections [28].

Beyond cryptography, the generalised EAT is useful whenever one is interested in bounding the min-entropy of a large system that can be decomposed in a sequential way. Such problems are abundant in physics. For example, the dynamics of an open quantum system can be described in terms of interactions that take place sequentially with different parts of the system's environment [29]. In quantum thermodynamics, such a description is commonly employed to model the thermalisation of a system that is brought in contact with a thermal bath. For a lack of techniques, the entropy flow during a thermalisation process of this type is usually quantified in terms of von Neumann entropy rather than the operationally more relevant smooth min- and max-entropies [30]. The generalised EAT may be used to remedy this situation. A similar situation arises in quantum gravity, where smooth entropies play a role in the study of black holes [31].

In a different direction, one can also try to further improve the generalised EAT itself. Compared to the original EAT [1], our generalised EAT features a more general model of side information and a weaker condition on the relation between different rounds, replacing the Markov condition of [1] with our weaker non-signalling condition in Eq. (1.2). It is natural to ask whether a further step in this direction is possible: while the model of side information we consider is fully general, it may be possible to replace the non-signalling condition with a weaker requirement. We have argued above that our non-signalling condition appears to be the most general way of stating the requirement that future side information does not reveal information about past outputs, which seems necessary for an EAT-like theorem.[8] It would be interesting to formalise this intuition and see whether our theorem is provably "tight" in terms of the conditions placed on the sequential process. Furthermore, it might be possible to improve the way the statistical condition in Theorem 4.3 is dealt with in the proof, e.g. using ideas from [33,34].

[8] In an EAT-like theorem, the entropy contribution from a particular round i has to be calculated conditioned on the side information revealed in that round because we want to analyse the process round-by-round, not globally. If a future round revealed additional side information, then the total entropy contributed by round i would decrease, but there is no way of accounting for that in an EAT-like theorem that simply sums up single-round contributions. As an extreme case, the last round of the process could reveal all prior outputs as side information, so that the total amount of conditional entropy produced by the process is 0, but single-round entropy contributions could be positive. This demonstrates the need for some condition that enforces that future side information does not reveal information about past outputs. We note that this does not mean that there is no way of proving an entropy lower bound in more general settings: for example, [32] do show a bound on the entropy produced by parallel repeated non-local games, but this requires a global analysis.

Finally, one could attempt to extend entropy accumulation from conditional entropies to relative entropies. Such a *relative entropy accumulation theorem* (REAT) would be the following statement: for two sequences of channels $\{\mathcal{E}_1, \ldots, \mathcal{E}_n\}$ and $\{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ (where $\mathcal{F}_i$ need not necessarily be trace-preserving), and $\varepsilon > 0$,

$$D_{\max}^{\varepsilon}\big(\mathcal{E}_n \circ \cdots \circ \mathcal{E}_1 \,\big\|\, \mathcal{F}_n \circ \cdots \circ \mathcal{F}_1\big) \overset{?}{\leq} \sum_{i=1}^{n} D^{\mathrm{reg}}\big(\mathcal{E}_i \,\big\|\, \mathcal{F}_i\big) + O(\sqrt{n})\,.$$

Here, $D_{\max}^{\varepsilon}$ is the ε-smooth max-relative entropy [11] and we used the (regularised) channel divergences defined in Definition 2.5. The key technical challenge in proving this result is to show that the regularised channel divergence $D_{\alpha}^{\mathrm{reg}}\big(\mathcal{E}_i \,\big\|\, \mathcal{F}_i\big)$ is continuous in α at $\alpha = 1$, which is an important technical open question. If one had such a continuity statement and the maps $\mathcal{F}_i$ additionally satisfied a non-signalling condition (which is not required for the statement above), one could also use our Theorem 3.1 to derive a more general REAT, which would imply our generalised EAT.

2. Preliminaries

2.1. Notation. Throughout this paper, we restrict ourselves to finite-dimensional Hilbert spaces. The set of positive semidefinite operators on a quantum system A (with associated Hilbert space $\mathcal{H}_A$) is denoted by $\mathrm{Pos}(A)$. The set of quantum states is given by $\mathrm{S}(A) = \{\rho \in \mathrm{Pos}(A) \mid \mathrm{Tr}\big[\rho\big] = 1\}$. The set of completely positive maps from linear operators on A to linear operators on A' is denoted by $\mathrm{CP}(A, A')$. If such a map is additionally trace preserving, we call it a quantum channel and denote the set of such maps by $\mathrm{CPTP}(A, A')$. The identity channel on system A is denoted as id_A. The spectral norm is denoted by $\|\cdot\|_{\infty}$.

A cq-state is a quantum state $\rho \in \mathrm{S}(XA)$ on a *classical* system X (with alphabet $\mathcal{X}$) and a quantum system A, i.e. a state that can be written as

$$\rho_{XA} = \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes \rho_{A,x}$$

for subnormalised $\rho_{A,x} \in \mathrm{Pos}(A)$. For $\Omega \subset \mathcal{X}$, we define the conditional state

$$\rho_{XA|\Omega} = \frac{1}{\Pr_{\rho}[\Omega]} \sum_{x \in \Omega} |x\rangle\langle x| \otimes \rho_{A,x}\,, \quad \text{where } \Pr_{\rho}[\Omega] := \sum_{x \in \Omega} \mathrm{Tr}\big[\rho_{A,x}\big]\,.$$

If $\Omega = \{x\}$, we also write $\rho_{XA|x}$ for $\rho_{XA|\Omega}$.

2.2. Rényi divergence and entropy. We will make extensive use of the sandwiched Rényi divergence [35,36] and quantities associated with it, namely Rényi entropies and channel divergences. We recall the relevant definitions here.

Definition 2.1 (Rényi divergence). For $\rho \in \mathrm{S}(A)$, $\sigma \in \mathrm{Pos}(A)$, and $\alpha \in [1/2, 1) \cup (1, \infty)$ the (sandwiched) Rényi divergence is defined as

$$D_{\alpha}\big(\rho \,\big\|\, \sigma\big) := \frac{1}{\alpha - 1} \log\, \mathrm{Tr}\Big[\Big(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\Big)^{\alpha}\Big]$$

for $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$, and $+\infty$ otherwise.

From the Rényi divergence, one can define the conditional Rényi entropies as follows (see [11] for more details).

Definition 2.2 *(Conditional Rényi entropy).* For a bipartite state $\rho_{AB} \in \mathrm{S}(AB)$ and $\alpha \in [1/2, 1) \cup (1, \infty)$, we define the following two conditional Rényi entropies:

$$H_\alpha(A|B)_\rho = -D_\alpha(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B) \quad \text{and} \quad H_\alpha^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathrm{S}(B)} -D_\alpha(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B)\,.$$

From the definition it is clear that $H_\alpha(A|B) \leq H_\alpha^\uparrow(A|B)$. Importantly, a relation for the other direction also holds.

Lemma 2.3 *(*[11, Corollary 5.3]*). For $\rho_{AB} \in \mathrm{S}(AB)$ and $\alpha \in (1, 2)$:*

$$H_\alpha(A|B)_\rho \geq H_{\frac{1}{2-\alpha}}^\uparrow(A|B)_\rho\,.$$

In the limit $\alpha \to 1$ the sandwiched Rényi divergence converges to the relative entropy:

$$\lim_{\alpha\to 1} D_\alpha\big(\rho \,\big\|\, \sigma\big) = D(\rho\|\sigma) = \mathrm{Tr}\big[\rho(\log\rho - \log\sigma)\big]\,.$$

Accordingly, the conditional Rényi entropy converges to the conditional von Neumann entropy:

$$\lim_{\alpha\to 1} H_\alpha(A|B)_\rho = H(A|B)_\rho = H(AB)_\rho - H(B)_\rho = -\,\mathrm{Tr}\big[\rho_{AB}\log\rho_{AB}\big] + \mathrm{Tr}\big[\rho_B\log\rho_B\big]\,.$$

Conversely, in the limit $\alpha \to \infty$, the Rényi entropy $H_\alpha^\uparrow$ converges to the min-entropy. We will make use of a smoothed version of the min-entropy, which is defined as follows [2].

Definition 2.4 *(Smoothed min-entropy).* For $\rho_{AB} \in \mathrm{S}(AB)$ and $\varepsilon \in [0, 1]$, the ε-smoothed min-entropy of A conditioned on B is

$$H_{\min}^\varepsilon(A|B)_\rho = -\log \inf_{\tilde\rho_{AB}\in\mathcal{B}_\varepsilon(\rho_{AB})} \inf_{\sigma_B\in\mathrm{S}(B)} \left\|\sigma_B^{-\frac{1}{2}}\tilde\rho_{AB}\sigma_B^{-\frac{1}{2}}\right\|_\infty\,,$$

where $\|\cdot\|_\infty$ denotes the spectral norm and $\mathcal{B}_\varepsilon(\rho_{AB})$ is the ε-ball around ρ_{AB} in term of the purified distance [11].

Finally, we can extend the definition of the Rényi divergence from states to channels. The resulting quantity, the channel divergence (and its regularised version), will play an important role in the rest of the manuscript.

Definition 2.5 *(Channel divergence).* For $\mathcal{E} \in \mathrm{CPTP}(A, A')$, $\mathcal{F} \in \mathrm{CP}(A, A')$, and $\alpha \in [1/2, 1) \cup (1, \infty)$, the (stabilised) channel divergence[9] is defined as

$$D_\alpha\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) = \sup_{\omega\in\mathrm{S}(A\tilde A)} D_\alpha\big(\mathcal{E}(\omega) \,\big\|\, \mathcal{F}(\omega)\big)\,, \tag{2.1}$$

where without loss of generality $\tilde A \equiv A$. The regularised channel divergence is defined as

$$D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) := \lim_{n\to\infty} \frac{1}{n} D_\alpha\big(\mathcal{E}^{\otimes n} \,\big\|\, \mathcal{F}^{\otimes n}\big) = \sup_n \frac{1}{n} D_\alpha\big(\mathcal{E}^{\otimes n} \,\big\|\, \mathcal{F}^{\otimes n}\big)\,.$$

[9] "Stabilised" refers to the fact that the supremum in Eq. (2.1) maximises over states in $\mathrm{S}(A\tilde A)$, not just $\mathrm{S}(A)$, i.e. the maximisation includes a purifying system $\tilde A$. One can also consider non-stabilised channel divergences, where the supremum is only over states in $\mathrm{S}(A)$. However, in this paper we only use the stabilised channel divergence.

We note that the channel divergence is in general not additive under the tensor product [37, Proposition 3.1], so the regularised channel divergence can be strictly larger that the non-regularised one, i.e., $D_\alpha^{\mathrm{reg}}(\mathcal{E} \,\|\, \mathcal{F}) > D_\alpha(\mathcal{E} \,\|\, \mathcal{F})$. The regularised channel divergence, however, does satisfy an additivity property:

$$\begin{aligned} &D_\alpha^{\mathrm{reg}}\Big(\mathcal{E}^{\otimes k} \,\|\, \mathcal{F}^{\otimes k}\Big) \\ &= \lim_{n\to\infty} \frac{1}{n} D_\alpha\Big(\mathcal{E}^{\otimes kn} \,\|\, \mathcal{F}^{\otimes kn}\Big) = k \lim_{n\to\infty} \frac{1}{n'} D_\alpha\Big(\mathcal{E}^{\otimes n'} \,\|\, \mathcal{F}^{\otimes n'}\Big) = k\, D_\alpha^{\mathrm{reg}}(\mathcal{E} \,\|\, \mathcal{F}) \,, \end{aligned} \tag{2.2}$$

where we switched to the index $n' = kn$ for the second equality.

2.3. Spectral pinching. A key technical tool in our proof will be the use of spectral pinching maps [38], which are defined as follows (see [12, Chapter 3] for a more detailed introduction).

Definition 2.6 *(Spectral pinching map).* Let $\rho \in \mathrm{Pos}(A)$ with spectral decomposition $\rho = \sum_\lambda \lambda P_\lambda$, where $\lambda \in \mathrm{Spec}(\rho) \subset \mathbb{R}_{\geq 0}$ are the distinct eigenvalues of ρ and P_λ are mutually orthogonal projectors. The *(spectral) pinching map* $\mathcal{P}_\rho \in \mathrm{CPTP}(A, A)$ associated with ρ is given by

$$\mathcal{P}_\rho(\omega) := \sum_{\lambda \in \mathrm{Spec}(\rho)} P_\lambda\, \omega\, P_\lambda \,.$$

We will need a few basic properties of pinching maps.

Lemma 2.7 (Properties of pinching maps). *For any $\rho, \sigma \in \mathrm{Pos}(A)$, the following properties hold:*

(i) Invariance: $\mathcal{P}_\rho(\rho) = \rho$.
(ii) Commutation of pinched state: $[\sigma, \mathcal{P}_\sigma(\rho)] = 0$.
(iii) Pinching inequality: $\mathcal{P}_\sigma(\rho) \geq \frac{1}{|\mathrm{Spec}(\sigma)|}\rho$.
(iv) Commutation of pinching maps: if $[\rho, \sigma] = 0$, *then* $\mathcal{P}_\rho \circ \mathcal{P}_\sigma = \mathcal{P}_\sigma \circ \mathcal{P}_\rho$.
(v) Partial trace: $\mathrm{Tr}_B\big[\mathcal{P}_{\rho_A \otimes \mathbb{1}_B}(\omega_{AB})\big] = \mathcal{P}_{\rho_A}(\omega_A) \quad \forall\, \omega_{AB} \in \mathrm{Pos}(AB)$.

Proof. Properties (i)–(iii) follow from the definition and [3, Chapter 2.6.3] or [12, Lemma 3.5].

For the fourth statement, note that since $[\rho, \sigma] = 0$, there exists a joint orthonormal eigenbasis $\{|x_i\rangle\}$ of ρ and σ. Let P_λ be the projector onto the eigenspace of ρ with eigenvalue λ, and Q_μ the projector onto the eigenspace of σ with eigenvalue μ. We can expand

$$P_\lambda = \sum_{i \text{ s.t. } \rho|x_i\rangle = \lambda|x_i\rangle} |x_i\rangle\langle x_i| \qquad \text{and} \qquad Q_\mu = \sum_{j \text{ s.t. } \sigma|x_j\rangle = \mu|x_j\rangle} |x_j\rangle\langle x_j| \,.$$

Since $\{|x_i\rangle\}$ is a family of orthonormal vectors,

$$P_\lambda Q_\mu = \sum_{\substack{i \text{ s.t. } \rho|x_i\rangle = \lambda|x_i\rangle \\ \text{and } \sigma|x_i\rangle = \mu|x_i\rangle}} |x_i\rangle\langle x_i| = Q_\mu P_\lambda \,,$$

which implies commutation of the pinching maps.

For the fifth statement, note that if we write $\rho = \sum_\lambda \lambda P_\lambda$ with eigenprojectors P_λ, then the set of eigenprojectors of $\rho_A \otimes \mathbb{1}_B$ is simply $\{P_\lambda \otimes \mathbb{1}_B\}$. Hence,

$$\begin{aligned}\mathrm{Tr}_B\big[\mathcal{P}_{\rho_A\otimes\mathbb{1}_B}(\omega_{AB})\big] &= \sum_\lambda \mathrm{Tr}_B[P_\lambda \otimes \mathbb{1}_B \omega_{AB} P_\lambda \otimes \mathbb{1}_B] \\ &= \sum_\lambda P_\lambda \,\mathrm{Tr}_B[\omega_{AB}]\, P_\lambda = \mathcal{P}_{\rho_A}(\omega_A)\,.\end{aligned}$$

□

It is often useful to use the pinching map associated with tensor power states, i.e., $\mathcal{P}_{\rho^{\otimes n}}$. This is because for $\rho \in \mathrm{Pos}(A)$, the factor $|\mathrm{Spec}(\rho^{\otimes n})|$ from the pinching inequality (see Lemma 2.7) only scales polynomially in n (see e.g. [12, Remark 3.9]):

$$|\mathrm{Spec}(\rho^{\otimes n})| \leq (n+1)^{\dim(A)-1}\,. \tag{2.3}$$

In fact, we can show a similar property for all permutation-invariant states, not just tensor product states.

Lemma 2.8. *Let $\rho \in \mathrm{Pos}(A^{\otimes n})$ be permutation invariant and denote $d = \dim(A)$. Then*

$$|\mathrm{Spec}(\rho)| \leq (n+d)^{d(d+1)/2}\,.$$

Proof. By Schur-Weyl duality and Schur's lemma (see e.g. [39, Lemma 0.8 and Theorem 1.10]), since ρ is permutation-invariant, we have

$$\rho \cong \bigoplus_{\lambda\in\mathcal{I}_{d,n}} \rho(\lambda)_{Q_\lambda} \otimes \mathbb{1}_{P_\lambda}\,,$$

where $\cong$ denotes equality up to unitary conjugation (which leaves the spectrum invariant), $\mathcal{I}_{d,n}$ is the set of Young diagrams with n boxes and at most d rows, Q_λ and P_λ are systems whose details need not concern us, and $\rho(\lambda) \in \mathrm{Pos}(Q_\lambda)$. From this it is clear that

$$|\mathrm{Spec}(\rho)| \leq \sum_{\lambda\in\mathcal{I}_{d,n}} |\mathrm{Spec}(\rho(\lambda))| \leq \sum_{\lambda\in\mathcal{I}_{d,n}} \dim(Q_\lambda)\,.$$

It is known that $|\mathcal{I}_{d,n}| \leq (n+1)^d$ and $\dim(Q_\lambda) \leq (n+d)^{d(d-1)/2}$ (see e.g. [40, Section 6.2]). Hence

$$|\mathrm{Spec}(\rho)| \leq (n+1)^d (n+d)^{d(d-1)/2} \leq (n+d)^{d(d+1)/2}\,.$$

□

Corollary 2.9. *Let $\rho, \sigma \in \mathrm{Pos}(A)$ and $d = \dim(A)$. Then*

$$|\mathrm{Spec}\big(\mathcal{P}_{\rho^{\otimes n}}(\sigma^{\otimes n})\big)| \leq (n+d)^{d(d+1)/2}\,.$$

Proof. Note that $\mathcal{P}_{\rho^{\otimes n}}(\sigma^{\otimes n})$ is itself not a product state because the eigenprojectors of $\rho^{\otimes n}$ do not have a product form. However, since every eigenspace of $\rho^{\otimes n}$ is permutation-invariant, $\mathcal{P}_{\rho^{\otimes n}}(\sigma^{\otimes n})$ is permutation-invariant, too, so we can apply Lemma 2.8. □

3. Strengthened Chain Rules

One of the crucial properties of entropies are chain rules, which allow us to relate entropies of large composite systems to sums of entropies of the individual subsystems. In this section, we prove two new such chain rules, one for the Rényi divergence (Theorem 3.1, which is a generalisation of [9, Corollary 5.1]) and one for the conditional entropy (Theorem 3.6). The chain rule from Theorem 3.6 is the key ingredient for our generalised EAT, to which we will turn our attention in Sect. 4. Theorem 3.6 plays a similar role for our generalised EAT as [1, Corollary 3.5] does for the original EAT, but while the latter requires a Markov condition, the former does not. As a result, our generalised EAT based on Theorem 3.6 also avoids the Markov condition.

The outline of this section is as follows: we first prove a generalised chain rule for the Rényi divergence (Theorem 3.1). This chain rule contains a regularised channel divergence. As the next step, we show that in the special case of conditional entropies, we can drop the regularisation (Sect. 3.2). This allows us to derive a chain rule for conditional entropies from the chain rule for channels (Sect. 3.3).

3.1. Strengthened chain rule for Rényi divergence. The main result of this section is the following chain rule for the Rényi divergence.

Theorem 3.1. *Let* $\alpha > 1$, $\rho \in \mathrm{S}(AR)$, $\sigma \in \mathrm{Pos}(AR)$, $\mathcal{E} \in \mathrm{CPTP}(AR, B)$, *and* $\mathcal{F} \in \mathrm{CP}(AR, B)$. *Suppose that there exists* $\mathcal{R} \in \mathrm{CP}(A, B)$ *such that* $\mathcal{F} = \mathcal{R} \circ \mathrm{Tr}_R$. *Then*

$$D_\alpha\big(\mathcal{E}(\rho_{AR}) \,\big\|\, \mathcal{F}(\sigma_{AR})\big) \leq D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big) + D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) \,. \tag{3.1}$$

This is a stronger version of an existing chain rule due to [9], which we will use in our proof of Theorem 3.1:

Lemma 3.2 *(*[9, Corollary 5.1]*). Let* $\alpha > 1$, $\rho \in \mathrm{S}(A)$, $\sigma \in \mathrm{Pos}(A)$, $\mathcal{E} \in \mathrm{CPTP}(A, B)$, *and* $\mathcal{F} \in \mathrm{CP}(A, B)$. *Then*

$$D_\alpha\big(\mathcal{E}(\rho) \,\big\|\, \mathcal{F}(\sigma)\big) \leq D_\alpha\big(\rho \,\big\|\, \sigma\big) + D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) \,. \tag{3.2}$$

The difference between Theorem 3.1 and Lemma 3.2 is that on the r.h.s. of Eq. (3.1), we only have the divergence $D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big)$ between the two reduced states on system A. In contrast, if we used Eq. (3.2) with systems AR, then we would get the divergence $D_\alpha\big(\rho_{AR} \,\big\|\, \sigma_{AR}\big)$ between the full states. In particular, the weaker Lemma 3.2 can easily be recovered from Theorem 3.1 by taking the system R to be trivial, in which case the condition $\mathcal{F} = \mathcal{R} \circ \mathrm{Tr}_R$ becomes trivial, too.

While the difference between Theorem 3.1 and Lemma 3.2 may look minor at first sight, the two chain rules can give considerably different results: in general, the data processing inequality ensures that $D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big) \leq D_\alpha\big(\rho_{AR} \,\big\|\, \sigma_{AR}\big)$, but the gap between the two quantities can be significant, i.e., there exist states for which $D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big) \ll D_\alpha\big(\rho_{AR} \,\big\|\, \sigma_{AR}\big)$. In such cases, Theorem 3.1 yields a significantly tighter bound. This turns out to be crucial if we want to apply this chain rule repeatedly to get an EAT.

We also note that the statement of Theorem 3.1 is known to be correct also for $\alpha = 1$ [37, Theorem 3.5]. However, this requires a separate proof and does not follow from Theorem 3.1 as it is currently not known whether the function $\alpha \mapsto D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big)$ is continuous in the limit $\alpha \searrow 1$.[10]

[10] It is well-known [3, Lemma 8] that $\lim_{\alpha \searrow 1} D_\alpha\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) = D\big(\mathcal{E} \| \mathcal{F}\big)$, but it is unclear whether the same holds for the regularised quantity.

We now turn to the proof of Theorem 3.1. The key question for the proof is the following: given states ρ_{AR} and σ_A, does there exist an extension σ_{AR} of σ_A such that $D_\alpha(\rho_A \,\|\, \sigma_A) = D_\alpha(\rho_{AR} \,\|\, \sigma_{AR})$? For the special case of $\alpha = 1/2$, an affirmative answer is given by Uhlmann's theorem [10] (see also [11, Corollary 3.14]). This also holds for $\alpha = \infty$, but not in general for $\alpha \geq 1$ as discussed in Sect. B. The following lemma shows that a similar property still holds for $\alpha > 1$ on a regularised level.

Lemma 3.3. *Consider quantum systems A and R with $d = \dim(A)$. For $n \in \mathbb{N}$, we define $A^n = A_1 \dots A_n$, where A_i are copies of the system A, and likewise $R^n = R_1 \dots R_n$. Then for $\rho \in \mathrm{S}(AR)$, $\sigma \in \mathrm{Pos}(A)$, and $\alpha > 1$ we have*

$$\begin{aligned} D_\alpha(\rho_A \,\|\, \sigma_A) &\leq \inf_{\hat{\sigma}_{A^nR^n} \text{ s.t. } \hat{\sigma}_{A^n} = \sigma_A^{\otimes n}} \frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\|\, \hat{\sigma}_{A^nR^n}\big) \\ &\leq D_\alpha(\rho_A \,\|\, \sigma_A) + \frac{\alpha}{\alpha - 1} \frac{d(d+1)\log(n+d)}{n} \,. \end{aligned}$$

Proof. The inequality

$$D_\alpha(\rho_A \,\|\, \sigma_A) \leq \inf_{\hat{\sigma}_{A^nR^n} \text{ s.t. } \hat{\sigma}_{A^n} = \sigma_A^{\otimes n}} \frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\|\, \hat{\sigma}_{A^nR^n}\big)$$

follows directly from the data processing inequality for taking the partial trace over R^n, and additivity of D_α under tensor product [11].

For the other direction, we consider n-fold tensor copies of ρ_{AR} and σ_A, which we denote by $\rho_{A^nR^n} = \rho_{A_1R_1} \otimes \cdots \otimes \rho_{A_nR_n}$ and $\sigma_{A^n} = \sigma_{A_1} \otimes \cdots \otimes \sigma_{A_n}$. We define the following two pinched states

$$\rho'_{A^nR^n} = \mathcal{P}_{\sigma_{A^n} \otimes \mathbb{1}_{R^n}}(\rho_{A^nR^n}) \qquad \text{and} \qquad \hat{\rho}_{A^nR^n} = \mathcal{P}_{\rho'_{A^n} \otimes \mathbb{1}_{R^n}}(\rho'_{A^nR^n}) \,. \tag{3.3}$$

By definition of $\hat{\rho}_{A^nR^n}$ and using the pinching inequality (see Lemma 2.7(iii)) twice, we have

$$\rho_{A^nR^n} \leq |\mathrm{Spec}(\sigma_{A^n})| |\mathrm{Spec}(\rho'_{A^n})| \, \hat{\rho}_{A^nR^n} \,.$$

Using the operator monotonicity of the sandwiched Rényi divergence in the first argument [11] we find for any state $\hat{\sigma}_{A^nR^n}$

$$\frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\|\, \hat{\sigma}_{A^nR^n}\big) \leq \frac{1}{n} D_\alpha\big(\hat{\rho}_{A^nR^n} \,\|\, \hat{\sigma}_{A^nR^n}\big) + \frac{1}{n} \frac{\alpha}{\alpha - 1} \eta(n) \,, \tag{3.4}$$

with the error term

$$\eta(n) = \log |\mathrm{Spec}(\sigma_{A^n})| + \log |\mathrm{Spec}(\rho'_{A^n})| \,.$$

To prove the lemma, we now need to bound the error term $\eta(n)$ and construct a specific choice for $\hat{\sigma}_{A^nR^n}$ for which $\hat{\sigma}_{A^n} = \sigma_A^{\otimes n}$ and $\frac{1}{n} D_\alpha\big(\hat{\rho}_{A^nR^n} \,\|\, \hat{\sigma}_{A^nR^n}\big) \leq D_\alpha(\rho_A \,\|\, \sigma_A)$. We first bound $\eta(n)$. Since $\sigma_{A^n} = \sigma_A^{\otimes n}$, we have from Eq. (2.3) that $|\mathrm{Spec}(\sigma_{A^n})| \leq (n+1)^{d-1}$, where $d = \dim(A)$. To bound $|\mathrm{Spec}(\rho'_{A^n})|$, we note that by Eq. (3.3) and Lemma 2.7(v)

$$\rho'_{A^n} = \mathrm{Tr}_{R^n}\big[\mathcal{P}_{\sigma_{A^n} \otimes \mathbb{1}_{R^n}}(\rho_{A^nR^n})\big] = \mathcal{P}_{\sigma_{A^n}}(\rho_{A^n}) = \mathcal{P}_{\sigma_A^{\otimes n}}(\rho_A^{\otimes n}) \,. \tag{3.5}$$

We can therefore use Lemma 2.9 to obtain $|\mathrm{Spec}(\rho'_{A^n})| \leq (n+d)^{d(d+1)/2}$. Hence,

$$\eta(n) \leq d(d+1)\log(n+d)\,. \tag{3.6}$$

It thus remains to construct $\hat{\sigma}_{A^nR^n}$ satisfying the properties mentioned above. To do so we first establish a number of commutation statements.

(i) From Lemma 2.7(ii) we have that $[\hat{\rho}_{A^nR^n}, \rho'_{A^n} \otimes \mathbb{1}_{R^n}] = 0$. Recalling the definition of ρ' from Eq. (3.3), we get

$$\hat{\rho}_{A^n} = \mathrm{Tr}_{R^n}\left[\mathcal{P}_{\rho'_{A^n}\otimes\mathbb{1}_{R^n}}(\rho'_{A^nR^n})\right] = \mathcal{P}_{\rho'_{A^n}}(\rho'_{A^n}) = \rho'_{A^n}\,, \tag{3.7}$$

where the final step uses Lemma 2.7(i). As a result we find

$$[\hat{\rho}_{A^nR^n}, \hat{\rho}_{A^n} \otimes \mathbb{1}_{R^n}] = 0\,. \tag{3.8}$$

(ii) From Lemma 2.7(ii) we have that $[\rho'_{A^nR^n}, \sigma_{A^n} \otimes \mathbb{1}_{R^n}] = 0$. Taking the partial trace over R^n, this implies $[\rho'_{A^n}, \sigma_{A^n}] = 0$, so by Lemma 2.7(iv) and Eq. (3.3)

$$\hat{\rho}_{A^nR^n} = \mathcal{P}_{\rho'_{A^n}\otimes\mathbb{1}_{R^n}}\left(\mathcal{P}_{\sigma_{A^n}\otimes\mathbb{1}_{R^n}}(\rho_{A^nR^n})\right) = \mathcal{P}_{\sigma_{A^n}\otimes\mathbb{1}_{R^n}}\left(\mathcal{P}_{\rho'_{A^n}\otimes\mathbb{1}_{R^n}}(\rho_{A^nR^n})\right)\,.$$

Therefore, by Lemma 2.7(ii),

$$[\hat{\rho}_{A^nR^n}, \sigma_{A^n} \otimes \mathbb{1}_{R^n}] = 0\,. \tag{3.9}$$

(iii) Taking the partial trace over R^n in Eq. (3.9), we get

$$[\hat{\rho}_{A^n}, \sigma_{A^n}] = 0\,. \tag{3.10}$$

Having established these commutation relations, we define $\mathcal{T} \in \mathrm{CPTP}(A^n, A^nR^n)$ by[11]

$$\mathcal{T}(\omega_{A^n}) = \hat{\rho}^{1/2}_{A^nR^n}\hat{\rho}^{-1/2}_{A^n}\omega_{A^n}\hat{\rho}^{-1/2}_{A^n}\hat{\rho}^{1/2}_{A^nR^n}\,.$$

By construction,

$$\mathcal{T}(\hat{\rho}_{A^n}) = \hat{\rho}_{A^nR^n}\,. \tag{3.11}$$

We define

$$\hat{\sigma}_{A^nR^n} = \mathcal{T}(\sigma_{A^n})\,. \tag{3.12}$$

To see that this is a valid choice of $\hat{\sigma}$, i.e., that $\hat{\sigma}_{A^n} = \sigma_{A^n} = \sigma_A^{\otimes n}$, we use Eqs. (3.8), (3.9) and (3.10) to find

$$\hat{\sigma}_{A^n} = \mathrm{Tr}_{R^n}\left[\hat{\rho}^{1/2}_{A^nR^n}\hat{\rho}^{-1/2}_{A^n}\sigma_{A^n}\hat{\rho}^{-1/2}_{A^n}\hat{\rho}^{1/2}_{A^nR^n}\right] = \mathrm{Tr}_{R^n}\left[\hat{\rho}_{A^nR^n}\hat{\rho}^{-1}_{A^n}\sigma_{A^n}\right] = \sigma_{A^n}\,.$$

Using Eqs. (3.11) and (3.12) followed by the data processing inequality [11], we obtain

$$\frac{1}{n}D_\alpha\left(\hat{\rho}_{A^nR^n} \,\middle\|\, \hat{\sigma}_{A^nR^n}\right) = \frac{1}{n}D_\alpha\left(\mathcal{T}(\hat{\rho}_{A^n}) \,\middle\|\, \mathcal{T}(\sigma_{A^n})\right) \leq \frac{1}{n}D_\alpha\left(\hat{\rho}_{A^n} \,\middle\|\, \sigma_{A^n}\right)\,. \tag{3.13}$$

[11] In case $\hat{\rho}_{A^n}$ does not have full support, we only take the inverse on the support of $\hat{\rho}_{A^n}$.

By Eqs. (3.7) and (3.3) we have $\hat{\rho}_{A^n} = \rho'_{A^n} = \mathcal{P}_{\sigma_{A^n}}(\rho_{A^n})$. Therefore, continuing from Eq. (3.13) and using $\sigma_{A^n} = \mathcal{P}_{\sigma_{A^n}}(\sigma_{A^n})$ followed by the data processing inequality gives

$$\frac{1}{n} D_\alpha\big(\hat{\rho}_{A^nR^n} \,\big\|\, \hat{\sigma}_{A^nR^n}\big) \leq \frac{1}{n} D_\alpha\big(\rho_{A^n} \,\big\|\, \sigma_{A^n}\big) = \frac{1}{n} D_\alpha\big(\rho_A^{\otimes n} \,\big\|\, \sigma_A^{\otimes n}\big) = D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big) \,.$$

Inserting this and our error bound from Eq. (3.6) into Eq. (3.4) proves the desired statement. □

With this, we can now prove Theorem 3.1.

Proof of Theorem 3.1. Because D_α is additive under tensor products, for any $n \in \mathbb{N}$ we have

$$\begin{aligned} D_\alpha\big(\mathcal{E}(\rho_{AR}) \,\big\|\, \mathcal{F}(\sigma_{AR})\big) &= \frac{1}{n} D_\alpha\big(\mathcal{E}^{\otimes n}(\rho_{AR}^{\otimes n}) \,\big\|\, \mathcal{F}^{\otimes n}(\sigma_{AR}^{\otimes n})\big) \\ &= \inf_{\hat{\sigma}_{A^nR^n} \text{ s.t. } \hat{\sigma}_{A^n} = \sigma_A^{\otimes n}} \frac{1}{n} D_\alpha\big(\mathcal{E}^{\otimes n}(\rho_{AR}^{\otimes n}) \,\big\|\, \mathcal{F}^{\otimes n}(\hat{\sigma}_{A^nR^n})\big) \,, \end{aligned} \tag{3.14}$$

where the second equality holds because $\mathcal{F} = \mathcal{R} \circ \mathrm{Tr}_R$, so $\mathcal{F}^{\otimes n}(\sigma_{AR}^{\otimes n}) = \mathcal{F}^{\otimes n}(\hat{\sigma}_{A^nR^n})$ for any $\hat{\sigma}_{A^nR^n}$ that satisfies $\hat{\sigma}_{A^n} = \sigma_A^{\otimes n}$. From the chain rule in Lemma 3.2 we get that for any $\hat{\sigma}_{A^nR^n}$:

$$\begin{aligned} \frac{1}{n} D_\alpha\big(\mathcal{E}^{\otimes n}(\rho_{AR}^{\otimes n}) \,\big\|\, \mathcal{F}^{\otimes n}(\hat{\sigma}_{A^nR^n})\big) &\leq \frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\big\|\, \hat{\sigma}_{A^nR^n}\big) + \frac{1}{n} D_\alpha^{\mathrm{reg}}\big(\mathcal{E}^{\otimes n} \,\big\|\, \mathcal{F}^{\otimes n}\big) \\ &= \frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\big\|\, \hat{\sigma}_{A^nR^n}\big) + D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) \,, \end{aligned}$$

where for the second line we used additivity of the regularised channel divergence (see Eq. (2.2)). Combining this with Eq. (3.14), we get

$$D_\alpha\big(\mathcal{E}(\rho_{AR}) \,\big\|\, \mathcal{F}(\sigma_{AR})\big) \leq \inf_{\hat{\sigma}_{A^nR^n} \text{ s.t. } \hat{\sigma}_{A^n} = \sigma_A^{\otimes n}} \frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\big\|\, \hat{\sigma}_{A^nR^n}\big) + D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) \,. \tag{3.15}$$

Finally, using Lemma 3.3 and the fact that $d := \dim(A)$ and $\alpha > 1$ are constants independent of n, we have

$$\begin{aligned} &\lim_{n\to\infty} \inf_{\hat{\sigma}_{A^nR^n} \text{ s.t. } \hat{\sigma}_{A^n} = \sigma_A^{\otimes n}} \frac{1}{n} D_\alpha\big(\rho_{AR}^{\otimes n} \,\big\|\, \hat{\sigma}_{A^nR^n}\big) \\ &\quad\leq D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big) + \lim_{n\to\infty} \frac{\alpha}{\alpha - 1} \frac{d(d+1)\log(n+d)}{n} \\ &\quad= D_\alpha\big(\rho_A \,\big\|\, \sigma_A\big) \,. \end{aligned}$$

Therefore, taking $n \to \infty$ in Eq. (3.15) and inserting this yields the theorem statement. □

3.2. Removing the regularisation. The chain rule presented in Theorem 3.1 contains a regularised channel divergence term, which cannot be computed easily and whose behaviour as $\alpha \searrow 1$ is not understood. In this section we show that in the specific case relevant for entropy accumulation, this regularisation can be removed. From this, we then derive a chain rule for Rényi entropies in Theorem 3.6.

Definition 3.4 *(Replacer map).* The replacer map $\mathcal{S}_A \in \mathrm{CP}(A, A)$ is defined by its action on an arbitrary state ω_{AR}:

$$\mathcal{S}_A(\omega_{AR}) = \mathbb{1}_A \otimes \omega_R \,.$$

Note that as usual, when we write $\mathcal{S}_A(\omega_{AR})$, we include an implicit tensoring with the identity channel, i.e. $\mathcal{S}_A(\omega_{AR}) = (\mathcal{S}_A \otimes \mathrm{id}_R)(\omega_{AR})$.

Lemma 3.5. *Let $\alpha \in (1, 2)$, $\mathcal{E} \in \mathrm{CPTP}(AR, A'R')$, and $\mathcal{F} = \mathcal{S}_{A'} \circ \mathcal{E}$, where $\mathcal{S}_{A'}$ is the replacer map. Then we have*

$$D_\alpha^{\mathrm{reg}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) \leq D_{\frac{1}{2-\alpha}}\big(\mathcal{E} \,\big\|\, \mathcal{F}\big) \,.$$

Proof. Due to the choice of $\mathcal{F}$, we have that for any state $\psi^n \in \mathrm{S}(A^n R^n \tilde{R}^n)$ (with $\tilde{R} \equiv AR$):

$$D_\alpha\big(\mathcal{E}^{\otimes n}(\psi^n) \,\big\|\, \mathcal{F}^{\otimes n}(\psi^n)\big) = -H_\alpha\left((A')^n|(R')^n\tilde{R}^n\right)_{\mathcal{E}^{\otimes n}(\psi^n)} \,.$$

From [41, Proposition II.4] and [2, Lemma 4.2.2] we know that for every n, there exists a symmetric pure state $|\hat{\psi}^n\rangle \in \mathrm{Sym}^n(AR\tilde{R})$ such that

$$D_\alpha\big(\mathcal{E}^{\otimes n} \,\big\|\, \mathcal{F}^{\otimes n}\big) = D_\alpha\Big(\mathcal{E}^{\otimes n}(\hat{\psi}^n) \,\Big\|\, \mathcal{F}^{\otimes n}(\hat{\psi}^n)\Big) = -H_\alpha\left((A')^n|(R')^n\tilde{R}^n\right)_{\mathcal{E}^{\otimes n}(\psi^n)} \,,$$

where $\hat{\psi}^n = |\hat{\psi}^n\rangle\langle\hat{\psi}^n|$ and the supremum in the definition of the channel divergence is achieved because the conditional entropy is continuous in the state. Let $d = \dim(AR\tilde{R})$ and $g_{n,d} = \dim(\mathrm{Sym}^n(AR\tilde{R})) \leq (n+1)^{d^2-1}$. We define the state

$$\tau^n_{A^nR^n\tilde{R}^n} = \int \mu(\sigma_{AR\tilde{R}})\sigma^{\otimes n}_{AR\tilde{R}} \,, \tag{3.16}$$

where μ is the Haar measure on pure states. We now claim that in the limit $n \to \infty$, we can essentially replace the optimizer $\hat{\psi}^n_{A^nR^n\tilde{R}^n}$ by the state $\tau^n_{A^nR^n\tilde{R}^n}$ in Eq. (3.16). More precisely, we claim that

$$\lim_{n\to\infty} \frac{1}{n} H_\alpha((A')^n|(R')^n\tilde{R}^n)_{\mathcal{E}^{\otimes n}(\hat{\psi}^n)} \geq \lim_{n\to\infty} \frac{1}{n} H_{\frac{1}{2-\alpha}}((A')^n|(R')^n\tilde{R}^n)_{\mathcal{E}^{\otimes n}(\tau^n)} \,. \tag{3.17}$$

To show this, we first use Lemma 2.3 to get

$$H_\alpha((A')^n|(R')^n\tilde{R}^n)_{\mathcal{E}^{\otimes n}(\hat{\psi}^n)} \geq H^\uparrow_{\frac{1}{2-\alpha}}\left((A')^n|(R')^n\tilde{R}^n\right)_{\mathcal{E}^{\otimes n}(\hat{\psi}^n)} \,.$$

It is know that $\tau^n_{A^nR^n\tilde{R}^n}$ is the maximally mixed state on $\mathrm{Sym}^n(AR\tilde{R})$ (see e.g. [13]). Therefore,

$$\rho^n_{A^nR^n\tilde{R}^n} := \frac{g_{n,d}\tau^n - \hat{\psi}^n}{g_{n,d} - 1}$$

is a valid quantum state (i.e. positive and normalised). Hence, we can write

$$\tau^n = \left(1 - \frac{1}{g_{n,d}}\right)\rho^n + \frac{1}{g_{n,d}}\hat{\psi}^n .$$

Using [1, Lemma B.5], it follows that

$$\frac{1}{n}H^{\uparrow}_{\frac{1}{2-\alpha}}\left((A')^n|(R')^n\tilde{R}^n\right)_{\mathcal{E}^{\otimes n}(\hat{\psi}^n)} \geq \frac{1}{n}H^{\uparrow}_{\frac{1}{2-\alpha}}\left((A')^n|(R')^n\tilde{R}^n\right)_{\mathcal{E}^{\otimes n}(\tau^n)} - \frac{\alpha}{\alpha-1}\frac{\log(g_{n,d})}{n} .$$

Since $\frac{\log(g_{n,d})}{n} \leq (d^2-1)\frac{\log n}{n}$ vanishes as $n \to \infty$, taking the limit and using $H^{\uparrow}_{\frac{1}{2-\alpha}}(\cdot|\cdot) \geq H_{\frac{1}{2-\alpha}}(\cdot|\cdot)$ proves Eq. (3.17).

Having established Eq. (3.17), we can now conclude the proof of the lemma as follows

$$\begin{aligned}
D^{\mathrm{reg}}_{\alpha}\big(\mathcal{E}\,\big\|\,\mathcal{F}\big) &= -\lim_{n\to\infty}\frac{1}{n}H_{\alpha}((A')^n|(R')^n\tilde{R}^n)_{\mathcal{E}^{\otimes n}(\hat{\psi}^n)} \\
&\leq -\lim_{n\to\infty}\frac{1}{n}H_{\frac{1}{2-\alpha}}((A')^n|(R')^n\tilde{R}^n)_{\mathcal{E}^{\otimes n}(\tau^n)} \\
&= \lim_{n\to\infty}\frac{1}{n}D_{\frac{1}{2-\alpha}}\left(\mathcal{E}^{\otimes n}\Big(\int \mu(\sigma_{AR\tilde{R}})\sigma^{\otimes n}_{AR\tilde{R}}\Big)\,\Big\|\,\mathcal{F}^{\otimes n}\Big(\int \mu(\sigma_{AR\tilde{R}})\sigma^{\otimes n}_{AR\tilde{R}}\Big)\right) \\
&\leq \lim_{n\to\infty}\sup_{\sigma_{AR\tilde{R}}\in\mathrm{S}(AR\tilde{R})}\frac{1}{n}D_{\frac{1}{2-\alpha}}\left(\mathcal{E}^{\otimes n}\left(\sigma^{\otimes n}_{AR\tilde{R}}\right)\,\Big\|\,\mathcal{F}^{\otimes n}\left(\sigma^{\otimes n}_{AR\tilde{R}}\right)\right) \\
&= D_{\frac{1}{2-\alpha}}\big(\mathcal{E}\,\big\|\,\mathcal{F}\big) ,
\end{aligned}$$

where we used joint quasi-convexity [11, Proposition 4.17] in the fourth line and additivity under tensor products in the last line. □

3.3. Strengthened chain rule for conditional Rényi entropy. We next combine Theorem 3.1 with Lemma 3.5 to derive a new chain rule for the conditional Rényi entropy which then allows us to prove the generalised EAT in Sect. 4.

Lemma 3.6. *Let $\alpha \in (1,2)$, $\rho \in \mathrm{S}(ARE)$, and $\mathcal{M} \in \mathrm{CPTP}(RE, A'R'E')$ such that there exists $\mathcal{R} \in \mathrm{CPTP}(E, E')$ such that $\mathrm{Tr}_{A'R'} \circ \mathcal{M} = \mathcal{R} \circ \mathrm{Tr}_R$. Then*

$$H_{\alpha}(AA'|E')_{\mathcal{M}(\rho)} \geq H_{\alpha}(A|E)_{\rho} + \inf_{\omega\in\mathrm{S}(RE\tilde{E})} H_{\frac{1}{2-\alpha}}(A'|E'\tilde{E})_{\mathcal{M}(\omega)} \tag{3.18}$$

for a purifying system $\tilde{E} \equiv RE$.

Proof. We define the following maps[12]

$$\begin{aligned}
\mathcal{N} &= \mathcal{S}_{A'} \circ \mathcal{M} && \in \mathrm{CP}(RE, A'R'E') , \\
\tilde{\mathcal{M}} &= \mathrm{id}_A \otimes \mathrm{Tr}_{R'} \circ \mathcal{M} && \in \mathrm{CPTP}(ARE, AA'E') , \\
\tilde{\mathcal{N}} &= \mathcal{S}_{A'} \circ \tilde{\mathcal{M}} && \in \mathrm{CP}(ARE, AA'E') .
\end{aligned}$$

[12] The map $\mathcal{M}$ in the theorem statement is also implicitly tensored with an identity map on A, but for the definition of $\tilde{M}$ we make this explicit to avoid confusion when applying Theorem 3.1.

Note that in Eq. (3.18), we can replace $\mathcal{M}$ by $\tilde{\mathcal{M}}$, as the system R' does not appear in Eq. (3.18). With $\sigma_{ARE} = \mathbb{1}_A \otimes \rho_{RE}$ and $\tilde{\mathcal{N}} = \mathcal{S}_{A'} \circ \tilde{\mathcal{M}}$, we can write

$$-H_\alpha(AA'|E')_{\mathcal{M}(\rho)} = D_\alpha\Big(\tilde{\mathcal{M}}(\rho_{ARE}) \,\Big\|\, \tilde{\mathcal{N}}(\sigma_{ARE})\Big) .$$

We now claim that there exists a map $\tilde{\mathcal{R}} \in \mathrm{CP}(AE, AA'E)$ such that $\tilde{\mathcal{N}} = \tilde{\mathcal{R}} \circ \mathrm{Tr}_R$. To see this, observe that by assumption, $\mathrm{Tr}_{A'} \circ \tilde{\mathcal{M}} = \mathrm{id}_A \otimes \mathcal{R} \circ \mathrm{Tr}_R$ for some $\mathcal{R} \in \mathrm{CP}(E, E')$. Then, we can define $\tilde{\mathcal{R}} \in \mathrm{CP}(AE, AA'E)$ by its action on an arbitrary state ω_{AE}:

$$\tilde{\mathcal{R}}(\omega_{AE}) := \mathbb{1}_{A'} \otimes (\mathrm{id}_A \otimes \mathcal{R})(\omega_{AE}) = \mathbb{1}_{A'} \otimes \mathrm{Tr}_{A'} \circ \tilde{\mathcal{M}}(\omega_{ARE}) = \tilde{\mathcal{N}}(\omega_{ARE})$$

for any extension ω_{ARE} of ω_{AE}. Therefore, we can apply Theorem 3.1 to find

$$D_\alpha\Big(\tilde{\mathcal{M}}(\rho_{ARE}) \,\Big\|\, \tilde{\mathcal{N}}(\sigma_{ARE})\Big) \leq D_\alpha\big(\rho_{AE} \,\big\|\, \sigma_{AE}\big) + D_\alpha^{\mathrm{reg}}\Big(\tilde{\mathcal{M}} \,\Big\|\, \tilde{\mathcal{N}}\Big) .$$

By definition of σ, we have $D_\alpha\big(\rho_{AE} \,\big\|\, \sigma_{AE}\big) = -H_\alpha(A|E)_\rho$. Since the channel divergence is stabilised (see Footnote 9), tensoring with id_A has no effect, i.e.,

$$D_\alpha^{\mathrm{reg}}\Big(\tilde{\mathcal{M}} \,\Big\|\, \tilde{\mathcal{N}}\Big) = D_\alpha^{\mathrm{reg}}\big(\mathrm{Tr}_{R'} \circ \mathcal{M} \,\big\|\, \mathrm{Tr}_{R'} \circ \mathcal{N}\big) = D_\alpha^{\mathrm{reg}}\big(\mathrm{Tr}_{R'} \circ \mathcal{M} \,\big\|\, \mathcal{S}_{A'} \circ \mathrm{Tr}_{R'} \circ \mathcal{M}\big) .$$

To this, we can apply Lemma 3.5 and obtain

$$D_\alpha^{\mathrm{reg}}\Big(\tilde{\mathcal{M}} \,\Big\|\, \tilde{\mathcal{N}}\Big) \leq D_{\frac{1}{2-\alpha}}\big(\mathrm{Tr}_{R'} \circ \mathcal{M} \,\big\|\, \mathcal{S}_{A'} \circ \mathrm{Tr}_{R'} \circ \mathcal{M}\big) = - \inf_{\omega \in \mathrm{S}(RE\tilde{E})} H_{\frac{1}{2-\alpha}}(A'|E'\tilde{E})_{\mathcal{M}(\omega)}$$

with $\tilde{E} \equiv RE$. Combining all the steps yields the desired statement. □

4. Generalised Entropy Accumulation

We are finally ready to state and prove the main result of this work which is a generalisation of the EAT proven in [1]. We first state a simple version of this theorem, which follows readily from the chain rule Theorem 3.6 and captures the essential feature of entropy accumulation: the min-entropy of a state $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho)$ produced by applying a sequence of n channels can be lower-bounded by a sum of entropy contributions of each channel $\mathcal{M}_i$. However, for practical applications, it is desirable not to consider the state $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho)$, but rather that state conditioned on some classical event, for example "success" in a key distribution protocol – a concept called "testing". Analogously to [1], we present an EAT adapted to that setting in Sect. 4.2.

4.1. Generalised EAT.

Theorem 4.1 (Generalised EAT). *Consider a sequence of channels $\mathcal{M}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, A_iR_iE_i)$ such that for all $i \in \{1, \ldots, n\}$, there exists $\mathcal{R}_i \in \mathrm{CPTP}(E_{i-1}, E_i)$ such that $\mathrm{Tr}_{A_iR_i} \circ \mathcal{M}_i = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}$. Then for any $\varepsilon \in (0, 1)$ and any $\rho_{R_0E_0} \in \mathrm{S}(R_0E_0)$*

$$H_{\min}^{\varepsilon}(A^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E_0})} \geq \sum_{i=1}^{n} \inf_{\omega \in \mathrm{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} - O(\sqrt{n})$$

for a purifying system $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}$. For a statement with explicit constants, see Eq. (4.1) in the proof.

Proof. By [1, Lemma B.10], we have for $\alpha \in (1, 2)$

$$H_{\min}^{\varepsilon}(A_1^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})} \geq H_\alpha(A_1^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})} - \frac{g(\varepsilon)}{\alpha-1}$$

with $g(\varepsilon) = \log(1-\sqrt{1-\varepsilon^2})$. From Theorem 3.6, we have

$$\begin{aligned} &H_\alpha(A_1^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})} \\ &\qquad \geq H_\alpha(A_1^{n-1}|E_{n-1})_{\mathcal{M}_{n-1}\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})} \\ &\quad + \inf_{\omega\in S(R_{n-1}E_{n-1}\tilde{E}_{n-1})} H_{\frac{1}{2-\alpha}}(A_n|E_n\tilde{E}_{n-1})_{\mathcal{M}_n(\omega)}\,. \end{aligned}$$

Repeating this step $n-1$ times, we get

$$\begin{aligned} H_\alpha(A_1^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})} &\geq H_\alpha(A_1|E_1)_{\mathcal{M}_1(\rho_{R_0E_0})} \\ &\quad + \sum_{i=2}^{n} \inf_{\omega\in S(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H_{\frac{1}{2-\alpha}}(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} \\ &\geq \sum_{i=1}^{n} \inf_{\omega\in S(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H_{\frac{1}{2-\alpha}}(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)}\,, \end{aligned}$$

where the final step uses the monotonicity of the Rényi divergence in α [11, Corollary 4.3]. From [1, Lemma B.9] we have for each $i \in \{1,\ldots,n\}$ and α sufficiently close to 1,

$$\begin{aligned} &\inf_{\omega\in S(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H_{\frac{1}{2-\alpha}}(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} \\ &\geq \inf_{\omega\in S(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} - \frac{\alpha-1}{2-\alpha}\log^2\big(1+2\,\dim(A_i)\big). \end{aligned}$$

Setting $d_A = \max_i \dim(A_i)$ and combining the previous steps, we obtain

$$\begin{aligned} &H_{\min}(A_1^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})} \\ &\geq \sum_{i=1}^{n} \inf_{\omega_i\in S(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega_i)} - n\,\frac{\alpha-1}{2-\alpha}\log^2(1+2d_A) - \frac{g(\varepsilon)}{\alpha-1}. \end{aligned} \tag{4.1}$$

Using $\alpha = 1 + O(1/\sqrt{n})$ yields the result. □

4.2. Generalised EAT with testing. In this section, we will extend Theorem 4.1 to include the possibility of "testing", i.e., of computing the min-entropy of a cq-state conditioned on some classical event. This analysis is almost identical to that of [8]; we give the full proof for completeness, but will appeal to [8] for specific tight bounds. The resulting EAT (Theorem 4.3) has (almost) the same tight bounds as the result in [8], but replaces the Markov condition with the more general non-signalling condition. Hence, relaxing the Markov condition does not result in a significant loss in parameters (including second-order terms).

Consider a sequence of channels $\mathcal{M}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, C_iA_iR_iE_i)$ for $i \in \{1, \ldots, n\}$, where C_i are classical systems with common alphabet $\mathcal{C}$. We require that these channels $\mathcal{M}_i$ satisfy the following condition: defining $\mathcal{M}'_i = \mathrm{Tr}_{C_i} \circ \mathcal{M}_i$, there exist channels $\mathcal{T}_i \in \mathrm{CPTP}(A_iE_i, C_iA_iE_i)$ and $\mathcal{T} \in \mathrm{CPTP}(A^nE_n, C^nA^nE_n)$ such that $\mathcal{M}_i = \mathcal{T}_i \circ \mathcal{M}'_i$ and $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1 = \mathcal{T} \circ \mathcal{M}'_n \circ \cdots \circ \mathcal{M}'_1$, where $\mathcal{T}_i$ and $\mathcal{T}$ have the form

$$\begin{aligned}\mathcal{T}_i(\omega_{A_iE_i}) &= \sum_{y\in\mathcal{Y}_i, z\in\mathcal{Z}_i} (\Pi_{A_i}^{(y)} \otimes \Pi_{E_i}^{(z)})\omega_{A_iE_i}(\Pi_{A_i}^{(y)} \otimes \Pi_{E_i}^{(z)}) \otimes |r_i(y,z)\rangle\langle r_i(y,z)|_{C_i} \\ \mathcal{T}(\omega_{A^nE_n}) &= \sum_{y\in\mathcal{Y}, z\in\mathcal{Z}} (\Pi_{A^n}^{(y)} \otimes \Pi_{E_n}^{(z)})\omega_{A^nE_n}(\Pi_{A^n}^{(y)} \otimes \Pi_{E_n}^{(z)}) \otimes |r(y,z)\rangle\langle r(y,z)|_{C^n}\,,\end{aligned} \tag{4.2}$$

where $\{\Pi_{A_i}^{(y)}\}_y$ and $\{\Pi_{E_i}^{(z)}\}_z$ are families of mutually orthogonal projectors on A_i and E_i, and $r_i : \mathcal{Y}_i \times \mathcal{Z}_i \to \mathcal{C}$ is a deterministic function Similarly, $\{\Pi_{A^n}^{(y)}\}_y$ and $\{\Pi_{E_n}^{(z)}\}_z$ are families of mutually orthogonal projectors on A^n and E_n, and $r : \mathcal{Y} \times \mathcal{Z} \to \mathcal{C}$ is a deterministic function. (Note that even though we use the same symbol for both, in principle there does not have to be any relationship between the single-round projectors Π_{A_i} and the projector Π_{A^n} (and likewise for Π_{E_i} and Π_{E_n}), although in practice the latter will usually be the tensor product of the former.) Intuitively, this condition says that for each round, the classical statistics can be reconstructed "in a projective way" from the systems A_i and E_i in that round, and furthermore the full statistics information C^n can be reconstructed in a projective way from the systems A^n and E_n at the end of the process. The latter condition is not implied by the former because future rounds may modify the E_i-system in such a way that C_i can no longer be reconstructed from the side information E_n at the end of the protocol. To rule this out, we need to specify the latter condition separately. In particular, this requirement is always satisfied if the statistics C_i are computed from classical information contained in A_i and E_i and this classical information is not deleted from E_i in future rounds. This is the scenario in all applications that we are aware of, but we state Eq. (4.2) more generally to allow for the possibility of protocols where the statistics are constructed in a more general way.

Let $\mathbb{P}$ be the set of probability distributions on the alphabet $\mathcal{C}$ of C_i, and let $\tilde{E}_{i-1}$ be a system isomorphic to $R_{i-1}E_{i-1}$. For any $q \in \mathbb{P}$ we define the set of states

$$\Sigma_i(q) = \left\{\nu_{C_iA_iR_iE_i\tilde{E}_{i-1}} = \mathcal{M}_i(\omega_{R_{i-1}E_{i-1}\tilde{E}_{i-1}}) \,|\, \omega \in \mathrm{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1}) \text{ and } \nu_{C_i} = q\right\}, \tag{4.3}$$

where ν_{C_i} denotes the probability distribution over $\mathcal{C}$ with the probabilities given by $\Pr[c] = \langle c|\nu_{C_i}|c\rangle$. In other words, $\Sigma_i(q)$ is the set of states that can be produced at the output of the channel $\mathcal{M}_i$ and whose reduced state on C_i is equal to the probability distribution q.

Definition 4.2. A function $f : \mathbb{P} \to \mathbb{R}$ is called a *min-tradeoff function* for $\{\mathcal{M}_i\}$ if it satisfies

$$f(q) \leq \min_{\nu\in\Sigma_i(q)} H(A_i|E_i\tilde{E}_{i-1})_\nu \quad \forall i = 1, \ldots, n\,.$$

Note that if $\Sigma_i(q) = \emptyset$, then $f(q)$ can be chosen arbitrarily.

Our result will depend on some simple properties of the tradeoff function, namely the maximum and minimum of f, the minimum of f over valid distributions, and the maximum variance of f:

$$\begin{aligned}
\mathsf{Max}(f) &:= \max_{q\in\mathbb{P}} f(q)\,,\\
\mathsf{Min}(f) &:= \min_{q\in\mathbb{P}} f(q)\,,\\
\mathsf{Min}_\Sigma(f) &:= \min_{q:\Sigma(q)\neq\emptyset} f(q)\,,\\
\mathsf{Var}(f) &:= \max_{q:\Sigma(q)\neq\emptyset} \sum_{x\in\mathcal{C}} q(x) f(\delta_x)^2 - \left(\sum_{x\in\mathcal{C}} q(x) f(\delta_x)\right)^2\,,
\end{aligned}$$

where $\Sigma(q) = \bigcup_i \Sigma_i(q)$ and δ_x is the distribution with all the weight on element x. We write $\mathsf{freq}(C^n)$ for the distribution on $\mathcal{C}$ defined by $\mathsf{freq}(C^n)(c) = \frac{|\{i\in\{1,\ldots,n\}:C_i=c\}|}{n}$. We also recall that in this context, an event Ω is defined by a subset of $\mathcal{C}^n$, and for a state $\rho_{C^nA^nE_nR_n}$ we write $\Pr_\rho[\Omega] = \sum_{c^n\in\Omega} \mathrm{Tr}\left[\rho_{A_1^nE_nR_n,c^n}\right]$ for the probability of the event Ω and

$$\rho_{C^nA^nE_nR_n|\Omega} = \frac{1}{\Pr_\rho[\Omega]} \sum_{c^n\in\Omega} |c^n\rangle\langle c^n|_{C^n} \otimes \rho_{A^nE_nR_n,c^n}$$

for the state conditioned on Ω.

Theorem 4.3. *Consider a sequence of channels $\mathcal{M}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, C_iA_iR_iE_i)$ for $i \in \{1,\ldots,n\}$, where C_i are classical systems with common alphabet $\mathcal{C}$ and the sequence $\{\mathcal{M}_i\}$ satisfies Eq. (4.2) and the non-signalling condition: for each $\mathcal{M}_i$, there exists $\mathcal{R}_i \in \mathrm{CPTP}(E_{i-1}, E_i)$ such that $\mathrm{Tr}_{A_iR_iC_i} \circ \mathcal{M}_i = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}$. Let $\varepsilon \in (0,1)$, $\alpha \in (1, 3/2)$, $\Omega \subset \mathcal{C}^n$, $\rho_{R_0E_0} \in \mathrm{S}(R_0E_0)$, and f be an affine[13] min-tradeoff function with $h = \min_{c^n\in\Omega} f(\mathsf{freq}(c^n))$. Then,*

$$\begin{aligned}
H_{\min}^\varepsilon(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})_{|\Omega}} \geq\; & n\,h - n\,\frac{\alpha-1}{2-\alpha}\,\frac{\ln(2)}{2}\,V^2 - \frac{g(\varepsilon)+\alpha\log(1/\Pr_{\rho^n}[\Omega])}{\alpha-1}\\
& - n\left(\frac{\alpha-1}{2-\alpha}\right)^2 K'(\alpha)\,, \qquad (4.4)
\end{aligned}$$

where $\Pr[\Omega]$ *is the probability of observing event* Ω*, and*

$$\begin{aligned}
g(\varepsilon) &= -\log(1-\sqrt{1-\varepsilon^2})\,,\\
V &= \log(2d_A^2+1) + \sqrt{2+\mathsf{Var}(f)}\,,\\
K'(\alpha) &= \frac{(2-\alpha)^3}{6(3-2\alpha)^3\ln 2}\, 2^{\frac{\alpha-1}{2-\alpha}(2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))} \ln^3\left(2^{2\log d_A+\mathsf{Max}(f)-\mathsf{Min}_\Sigma(f)} + e^2\right)\,,
\end{aligned}$$

with $d_A = \max_i \dim(A_i)$.

[13] A function f on the convex set $\mathbb{P}(\mathcal{C})$ is called *affine* if it is linear under convex combinations, i.e., for $\lambda \in [0,1]$ and $p_1, p_2 \in \mathbb{P}(\mathcal{C})$, $\lambda f(p_1) + (1-\lambda) f(p_2) = f(\lambda p_1 + (1-\lambda)p_2)$. Such functions are also sometimes called *convex-linear*.

Remark 4.4. The parameter in α in Theorem 4.3 can be optimized for specific problems, which leads to tighter bounds. Alternatively, it is possible to make a generic choice for α to recover a theorem that looks much more like Theorem 4.1, which is done in Corollary 4.6. We also remark that even tighter second order terms have been derived in [42]. To keep our theorem statement and proofs simpler, we do not carry out this additional optimization explicitly, but note that this can be done in complete analogy to [42].

To prove Theorem 4.3, we will need the following lemma (which is already implicit in [1, Claim 4.6], but we give a simplified proof here).

Lemma 4.5. *Consider a quantum state $\rho \in \mathrm{S}(CADE)$ that has the form*

$$\rho_{CADE} = \sum_{c\in\Omega} |c\rangle\langle c| \otimes \rho_{AE,c} \otimes \rho_{D|c}\,,$$

where $\Omega \subset \mathcal{C}$ is a subset of the alphabet $\mathcal{C}$ of the classical system C, and for each c, $\rho_{AE,c} \in \mathrm{Pos}(AE)$ is subnormalised and $\rho_{D|c} \in \mathrm{S}(D)$ is a quantum state. Then for $\alpha > 1$,

$$H_\alpha^\uparrow(ACD|E)_\rho \leq H_\alpha^\uparrow(AC|E)_\rho + \max_{c\in\Omega} H_\alpha(D)_{\rho_{D|c}}\,.$$

Proof. Let $\sigma_E \in \mathrm{S}(E)$ such that

$$H_\alpha^\uparrow(ACD|E)_\rho = -D_\alpha\big(\rho_{CADE} \,\big\|\, \mathbb{1}_{CAD} \otimes \sigma_E\big)\,.$$

Then

$$\left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{CADE} \sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha = \sum_{c\in\Omega} |c\rangle\langle c| \otimes \left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE,c} \sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha \otimes \rho_{D|c}^\alpha\,.$$

Hence,

$$\begin{aligned}
\mathrm{Tr}\left[\left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{CADE} \sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right] &= \sum_{c\in\Omega} \mathrm{Tr}\left[\left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE,c} \sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right] \mathrm{Tr}\left[\rho_{D|c}^\alpha\right] \\
&\leq \sup_{\tilde\sigma_E\in\mathrm{S}(E)} \mathrm{Tr}\left[\sum_{c\in\Omega} |c\rangle\langle c| \otimes \left(\tilde\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE,c} \tilde\sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right] \\
&\quad \times \max_{c\in\Omega} \mathrm{Tr}\left[\rho_{D|c}^\alpha\right] \\
&= \sup_{\tilde\sigma_E\in\mathrm{S}(E)} \mathrm{Tr}\left[\left(\tilde\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{CAE} \tilde\sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right] \max_{c\in\Omega} \mathrm{Tr}\left[\rho_{D|c}^\alpha\right]
\end{aligned}$$

Recalling the definitions of D_α (Definition 2.1) and $H_\alpha^\uparrow$ (Definition 2.2), we see that the lemma follows by taking the logarithm and multiplying by $\frac{1}{\alpha-1}$. □

Proof of Theorem 4.3. As in the proof of Theorem 4.1, we first use [1, Lemma B.10] to get

$$H_{\min}^\varepsilon(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})_{|\Omega}} \geq H_\alpha^\uparrow(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})_{|\Omega}} - \frac{g(\varepsilon)}{\alpha-1} \tag{4.5}$$

for $\alpha \in (1, 2]$ and $g(\varepsilon) = \log(1-\sqrt{1-\varepsilon^2})$. We therefore need to find a lower bound for

$$H_\alpha^\uparrow(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})|\Omega} = H_\alpha^\uparrow(A^nC^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})|\Omega}\,, \tag{4.6}$$

where the equality holds because of Eq. (4.2) and [1, Lemma B.7].

Before proceeding with the formal proof, let us explain the main difficulty compared to Theorem 4.1. The state for which we need to compute the entropy in Eq. (4.6) is conditioned on the event $\Omega \subset \mathcal{C}^n$. This is a global event, in the sense that it depends on the classical outputs $C_1, \ldots, C_n$ of all rounds. We essentially seek a lower bound that involves $\min_{\nu\in\Sigma_i(\mathsf{freq}(c^n))} H_\alpha(A_i|E_i)_\nu$ for some $c^n \in \Omega$, i.e., for every round we only want to minimize over output states of the channel $\mathcal{M}_i$ whose distribution on C_i matches the frequency distribution $\mathsf{freq}(c^n)$ of the n rounds we observed. This means that we must use the global conditioning on Ω to argue that in each round, we can restrict our attention to states whose outcome distribution matches the (worst-case) frequency distribution associated with Ω. The chain rule Theorem 3.1 does not directly allow us to do this as the r.h.s. of Eq. (3.18) always minimizes over all possible input states.

To circumvent this, we follow a strategy that was introduced in [1] and optimized in [8] (see also [16,21,43] for related ideas and [44] for follow-up work). For every i, we introduce a quantum system D_i with $\dim(D_i) = \lceil 2^{\mathsf{Max}(f)-\mathsf{Min}(f)}\rceil$ and define $\mathcal{D}_i \in \mathrm{CPTP}(C_i, C_iD_i)$ by

$$\mathcal{D}_i(\omega_{C_i}) = \sum_{c\in\mathcal{C}} \langle c|\omega_{C_i}|c\rangle \cdot |c\rangle\langle c| \otimes \tau_{D_i|c}\,.$$

For every $c \in \mathcal{C}$, the state $\tau_{D_i|c} \in \mathrm{S}(D)$ is defined as the mixture between a uniform distribution on $\{1, \ldots, \lfloor 2^{\mathsf{Max}(f)-f(\delta_c)}\rfloor\}$ and a uniform distribution on $\{1, \ldots, \lceil 2^{\mathsf{Max}(f)-f(\delta_c)}\rceil\}$ that satisfies

$$H(D_i)_{\tau_{D_i|c}} = \mathsf{Max}(f) - f(\delta_c)\,,$$

where δ_x stands for the distribution with all the weight on element x. This is clearly possible if $\dim(D_i) = \lceil 2^{\mathsf{Max}(f)-\mathsf{Min}(f)}\rceil$.

We define $\bar{\mathcal{M}}_i = \mathcal{D}_i \circ \mathcal{M}_i$ and denote

$$\rho^n_{C^nA^nR_nE_n} = \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E_0}) \quad \text{and} \quad \bar{\rho}^n_{C^nA^nD^nR_nE_n} = \bar{\mathcal{M}}_n \circ \cdots \circ \bar{\mathcal{M}}_1(\rho_{R_0E_0})\,.$$

The state $\bar{\rho}^n_{|\Omega}$ has the right form for us to apply Lemma 4.5 and get

$$H_\alpha^\uparrow(A^nC^n|E_n)_{\bar{\rho}^n_{|\Omega}} \geq -\max_{c^n\in\Omega} H_\alpha(D^n)_{\bar{\rho}^n_{D^n|c^n}} + H_\alpha^\uparrow(A^nC^nD^n|E_n)_{\bar{\rho}^n_{|\Omega}}\,, \tag{4.7}$$

where

$$\bar{\rho}^n_{D^n|c^n} = \tau_{D_1|c_1} \otimes \ldots \otimes \tau_{D_n|c_n}\,.$$

We treat each term in Eq. (4.7) in turn.

(i) For the term on the l.h.s., it is easy to see that $\bar{\rho}^n_{C^nA^nR_nE_n|\Omega} = \rho^n_{C^nA^nR_nE_n|\Omega}$, so

$$H_\alpha^\uparrow(A^nC^n|E_n)_{\bar{\rho}^n_{|\Omega}} = H_\alpha^\uparrow(A^nC^n|E_n)_{\rho^n_{|\Omega}}\,. \tag{4.8}$$

(ii) For the first term on the r.h.s., we compute

$$H_\alpha(D^n)_{\bar{\rho}^n_{D^n|c^n}} = \sum_i H_\alpha(D_i)_{\tau_{D_i|c_i}} \leq \sum_i H(D_i)_{\tau_{D_i|c_i}} = n\,\mathsf{Max}(f) - \sum_i f(\delta_{c_i}) = n\,\mathsf{Max}(f) - nf(\mathsf{freq}(c^n))\,, \tag{4.9}$$

where the last equality holds because f is affine.

(iii) For the second term on the r.h.s., we first use [1, Lemma B.5] to remove the conditioning on the event Ω, and then use that removing the classical system C^n and switching from $H^\uparrow_\alpha$ to H_α can only decrease the entropy:

$$H^\uparrow_\alpha(A^nC^nD^n|E_n)_{\bar{\rho}^n_{|\Omega}} \geq H_\alpha(A^nD^n|E_n)_{\bar{\rho}^n} - \frac{\alpha}{\alpha-1}\log(1/\mathrm{Pr}_{\rho^n}[\Omega])\,,$$

where we used $\mathrm{Pr}_{\rho^n}[\Omega] = \mathrm{Pr}_{\bar{\rho}^n}[\Omega]$. Now noting that $\mathrm{Tr}_{D_i}\circ\bar{\mathcal{M}}_i = \mathcal{M}_i$, we see that the non-signalling condition $\mathrm{Tr}_{A_iR_iC_i}\circ\mathcal{M}_i = \mathcal{R}_i\circ\mathrm{Tr}_{R_{i-1}}$ on $\mathcal{M}_i$ implies the non-signalling condition $\mathrm{Tr}_{A_iR_iC_iD_i}\circ\bar{\mathcal{M}}_i = \mathcal{R}_i\circ\mathrm{Tr}_{R_{i-1}}$ on $\bar{\mathcal{M}}_i$. We can therefore apply the chain rule in Theorem 3.6 to find

$$H_\alpha(A^nD^n|E_n)_{\bar{\rho}^n} \geq \sum_{i=1}^n \min_{\omega_{i-1}\in\mathrm{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1})} H_\beta(A_iD_i|E_i\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})}\,,$$

where we introduced the shorthand $\beta := \frac{1}{2-\alpha}$ and the purifying system $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}$. Noting that for $\alpha \in (1, 3/2)$ we have $\beta \in (1,2)$, we can now use [8, Corollary IV.2] to obtain

$$H_\beta(A_iD_i|E_i\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq H(A_iD_i|E_i\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} - (\beta-1)\frac{\ln(2)}{2}V^2 - (\beta-1)^2K(\beta)\,,$$

where V^2 and $K(\beta)$ are quantities from [8, Proposition V.3] that satisfy

$$K(\beta) \leq \frac{1}{6(2-\beta)^3\ln 2}\, 2^{(\beta-1)(2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))}\ln^3\left(2^{2\log d_A+\mathsf{Max}(f)-\mathsf{Min}_\Sigma(f)} + e^2\right)\,,$$

$$V^2 = \left(\log(2d_A^2+1) + \sqrt{2+\mathsf{Var}(f)}\right)^2\,,$$

where $d_A = \max_i \dim(A_i)$. Note that the above expressions derived in [8, Proposition V.3] also hold in our case due to the first part of Eq. (4.2). Furthermore, as in the proof of [8, Proposition V.3], we have

$$H(A_iD_i|E_i\tilde{E}_{i-1})_{\bar{\mathcal{M}}_i(\omega_{i-1})} \geq \mathsf{Max}(f)\,.$$

Therefore, the second term on the r.h.s. of Eq. (4.7) is bounded by

$$H^\uparrow_\alpha(A^nC^nD^n|E_n)_{\bar{\rho}^n_{|\Omega}} \geq n\,\mathsf{Max}(f) - n\,(\beta-1)\frac{\ln(2)}{2}V^2 - n\,(\beta-1)^2K(\beta) - \frac{\alpha}{\alpha-1}\log(1/\mathrm{Pr}_{\rho^n}[\Omega])\,. \tag{4.10}$$

Combining our results for each of the three terms (i.e. Eqs. (4.8), (4.9) and (4.10)) and recalling $h = \min_{x^n \in \Omega} f(\mathsf{freq}(x^n))$, Eq. (4.7) becomes

$$H_\alpha^\uparrow(A^n C^n|E_n)_{\rho^n_{|\Omega}} \geq n\,h - n\,(\beta-1)\frac{\ln(2)}{2}V^2 - \frac{\alpha}{\alpha-1}\log(1/\Pr_{\rho^n}[\Omega]) - n\,(\beta-1)^2 K(\beta)\,.$$

Inserting this into Eqs. (4.5) and (4.6), and defining $K'(\alpha) = K(\beta) = K(\frac{1}{2-\alpha})$ we obtain

$$\begin{aligned} H_{\min}^\varepsilon(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})_{|\Omega}} \geq\; & n\,h - n\,(\beta-1)\frac{\ln(2)}{2}V^2 - \frac{g(\varepsilon)+\alpha\log(1/\Pr_{\rho^n}[\Omega])}{\alpha-1} \\ & -n\,(\beta-1)^2 K(\beta) \end{aligned} \tag{4.11}$$

as desired. □

Corollary 4.6. *For the setting given in Theorem 4.3 we have*

$$H_{\min}^\varepsilon(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})_{|\Omega}} \geq nh - c_1\sqrt{n} - c_0\,,$$

where the quantities c_1 and c_0 are given by

$$\begin{aligned} c_1 &= \sqrt{\frac{2\ln(2)V^2}{\eta}\Big(g(\varepsilon) + (2-\eta)\log(1/\Pr_{\rho^n}[\Omega])\Big)}\,, \\ c_0 &= \frac{(2-\eta)\eta^2\log(1/\Pr_{\rho^n}[\Omega]) + \eta^2 g(\varepsilon)}{3(\ln 2)^2 V^2(2\eta-1)^3} \\ &\quad 2^{\frac{1-\eta}{\eta}(2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))}\ln^3\left(2^{2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2\right) \end{aligned}$$

with

$$\eta = \frac{2\ln(2)}{1+2\ln(2)}\,, \qquad g(\varepsilon) = \log(1-\sqrt{1-\varepsilon^2})\,, \qquad V = \log(2d_A^2+1) + \sqrt{2+\mathsf{Var}(f)}\,.$$

Proof. We first note that for any Ω with non-zero probability, $h \leq \log d_A$. Therefore, if $n \leq \left(\frac{c_1}{2\log d_A}\right)^2$, it is easy to check that $nh - c_1\sqrt{n} \leq -n\log d_A$, so the statement of Corollary 4.6 becomes trivial. We may therefore assume that $n \geq (\frac{c_1}{2\log d_A})^2$.

As in the proof of Theorem 4.3, we define $\beta = \frac{1}{2-\alpha}$. The first part of the proof works for any $\alpha \in (1, 2-\eta)$ for $\eta = \frac{2\ln(2)}{1+2\ln(2)} \approx 0.58$; later we will make a specific choice of α in this interval. Then, $\beta - 1 = \frac{1}{2-\alpha} - 1 \leq \frac{\alpha-1}{\eta}$ and $\beta \in (1, 1/\eta)$. Therefore, using $K(\beta)$ as defined in the proof of Theorem 4.3 and noting that in the interval $\beta \in (1, 1/\eta) \subset (1, 2)$ this quantity is monotonically increasing in β, we have

$$\begin{aligned} &K(\beta) \leq K := \\ &\frac{\eta^3}{6(2\eta-1)^3\ln 2}\,2^{\frac{1-\eta}{\eta}(2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))}\ln^3\left(2^{2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2\right)\,, \end{aligned}$$

Hence, we can simplify the statement of Theorem 4.3 to

$$\begin{aligned} &H_{\min}^{\varepsilon}(A^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho_{R_0E_0})_{|\Omega}} \\ &\geq n\,h - n\,(\alpha-1)\frac{\ln(2)}{2\eta}V^2 - \frac{g(\varepsilon)+(2-\eta)\cdot\log(1/\Pr_{\rho^n}[\Omega])}{\alpha-1} - n\,(\alpha-1)^2\frac{K}{\eta^2}. \end{aligned} \tag{4.12}$$

We now choose $\alpha > 1$ as a function of n and ε so that the terms proportional to $\alpha - 1$ and $\frac{1}{\alpha-1}$ match:

$$\alpha = 1 + \sqrt{\frac{2\eta}{n\ln(2)V^2}\Big(g(\varepsilon) + (2-\eta)\log(1/\Pr_{\rho^n}[\Omega])\Big)}\,.$$

Inserting this choice of α into Eq. (4.12) and combining terms yields the constants in Corollary 4.6. The final step is to show that this choice of α indeed satisfies $\alpha \leq 2-\eta$ for $n \geq (\frac{c_1}{2\log d_A})^2$. For this, we note that for $n \geq (\frac{c_1}{2\log d_A})^2$, we have

$$\alpha = 1 + \frac{\eta}{\ln(2)V^2}\frac{c_1}{\sqrt{n}} \leq 1 + \frac{2\eta\log d_A}{\ln(2)V^2}\,.$$

We can now use that $V^2 \geq \big(\log(2d_A^2)\big)^2 \geq 4\log d_A$ since $d_A \geq 2$, so

$$\alpha \leq 1 + \frac{2\eta\log d_A}{\ln(2)V^2} \leq 1 + \frac{\eta}{2\ln(2)} = 2 - \eta\,,$$

where the last inequality holds because $\eta = \frac{2\ln(2)}{1+2\ln(2)}$. □

In many applications, e.g. randomness expansion or QKD, a round can either be a "data generation round" (e.g. to generate bits of randomness or key) or a "test round" (e.g. to test whether a device used in the protocol behaves as intended). More formally, in this case the maps $\mathcal{M}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, C_iA_iR_iE_i)$ can be written as

$$\mathcal{M}_i = \gamma\mathcal{M}^{\mathrm{test}}_{i,R_{i-1}E_{i-1}\to C_iA_iR_iE_i} + (1-\gamma)\mathcal{M}^{\mathrm{data}}_{i,R_{i-1}E_{i-1}\to A_iR_iE_i}\otimes|\perp\rangle\langle\perp|_{C_i}\,, \tag{4.13}$$

where the output of $\mathcal{M}_i^{\mathrm{test}}$ on system C_i is from some alphabet $\mathcal{C}'$ that does not include $\perp$, so the alphabet of system C_i is $\mathcal{C} = \mathcal{C}' \cup \{\perp\}$. The parameter γ is called the *testing probability*, and for efficient protocols we usually want γ to be as small as possible.

For maps of the form in Eq. (4.13), there is a general way of constructing a min-tradeoff function for the map $\mathcal{M}_i$ based only on the statistics generated by the map $\mathcal{M}_i^{\mathrm{test}}$. This was shown in [8] and we reproduce their result (adapted to our notation) here for the reader's convenience.

Lemma 4.7 ([8, Lemma V.5]). *Let $\mathcal{M}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, C_iA_iR_iE_i)$ be channels satisfying the same conditions as in Theorem 4.3 that can furthermore be decomposed as in Eq. (4.13). Suppose that an affine function $g : \mathbb{P}(\mathcal{C}') \to \mathbb{R}$ satisfies for any $q' \in \mathbb{P}(\mathcal{C}')$ and any $i = 1, \ldots, n$*

$$g(q') \leq \min_{\omega\in\mathrm{S}(R_{i-1}E_{i-i}\tilde{E}_{i-1})} \Big\{H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} : \big(\mathcal{M}_i^{\mathrm{test}}(\omega)\big)_{C_i} = q'\Big\} \tag{4.14}$$

where $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}$ *is a purifying system. Then, the affine function* $f : \mathbb{P}(\mathcal{C}) \to \mathbb{R}$ *defined by*

$$f(\delta_x) = \mathsf{Max}(g) + \frac{1}{\gamma}(g(\delta_x) - \mathsf{Max}(g)) \qquad \forall x \in \mathcal{C}'$$
$$f(\delta_\perp) = \mathsf{Max}(g)$$

is a min-tradeoff function for $\{\mathcal{M}_i\}$. *Moreover,*

$$\begin{aligned}\mathsf{Max}(f) &= \mathsf{Max}(g)\\ \mathsf{Min}(f) &= \left(1 - \frac{1}{\gamma}\right)\mathsf{Max}(g) + \frac{1}{\gamma}\mathsf{Min}(g)\\ \mathsf{Min}_\Sigma(f) &\geq \mathsf{Min}(g)\\ \mathsf{Var}(f) &\leq \frac{1}{\gamma}\big(\mathsf{Max}(g) - \mathsf{Min}(g)\big)^2.\end{aligned}$$

5. Sample Applications

To demonstrate the utility of our generalised EAT, we provide two sample applications. Firstly, in Sect. 5.1 we prove security of blind randomness expansion against general attacks. The notion of blind randomness was defined in [15] and has potential applications in mistrustful cryptography (see [15,16] for a detailed motivation). Until now, no security proof against general attacks was known. In particular, the original EAT is not applicable because its model of side information is too restrictive. With our generalised EAT, we can show that security against general attacks follows straightforwardly from a single-round security statement.

Secondly, in Sect. 5.2 we give a simplified security proof for the E91 QKD protocol [45], which was also treated with the original EAT [1]. This example is meant to help those familiar with the original EAT understand the difference between that result and our generalised EAT. In particular, this application highlights the utility of our more general model of side information: in our proof, the non-signalling condition is satisfied trivially and the advantage over the original EAT stems purely from being able to update the side information register E_i. We point out that while here we focus on the E91 protocol to allow an easy comparison with the original EAT, our generalised EAT can be used for a large class of QKD protocols for which the original EAT was not applicable at all. A comprehensive treatment of this is given in [7].

5.1. Blind randomness expansion. We start by recalling the idea of standard (non-blind) device-independent randomness expansion [17–21]. Alice would like to generate a uniformly random bit string using devices D_1 and D_2 prepared by an adversary Eve. To this end, in her local lab (which Eve cannot access) she isolates the devices from one another and plays multiple round of a non-local game with them, e.g. the CHSH game. On a subset of the rounds of the game, she checks whether the CHSH condition is satisfied. If this is the case on a sufficiently high proportion of rounds, she can conclude that the devices' outputs on the remaining rounds must contain a certain amount of entropy, conditioned on the input to the devices and any quantum side information that Eve might have kept from preparing the devices. Using a quantum-proof randomness extractor, Alice can then produce a uniformly random string.

Blind randomness expansion [15,16] is a significant strengthening of the above idea. Here, Alice only receives one device D_1, which she again places in her local lab isolated from the outside world. Now, Alice plays a non-local game with her device D_1 and the adversary Eve: she samples questions for a non-local game as before, inputs one of the questions to D_1, and sends the other question to Eve. D_1 and Eve both provide an output. Alice then proceeds as in standard randomness expansion, checking whether the winning condition of the non-local game is satisfied on a subset of rounds and concluding that the output of her device D_1 must contain a certain amount of entropy conditioned on the adversary's side information.

For the purpose of applying the EAT, the crucial difference between the two notions of randomness expansion is the following: in standard randomness expansion, the adversary's quantum side information is not acted upon during the protocol, and additional side information (the inputs to the devices, which we also condition on) are generated independently in a round-by-round manner. This allows a relatively straightforward application of the standard EAT [4]. In contrast, in blind randomness expansion, the adversary's quantum side information gets updated in every round of the protocol and is not generated independently in a round-by-round fashion. This does not fit in the framework of the standard EAT, which requires the side information to be generated round-by-round subject to a Markov condition. As a result, [15,16] were not able to prove a general multi-round blind randomness expansion result.

In the rest of this section, we will show that our generalised EAT is capable of treating multi-round blind randomness expansion, using a protocol similar to [14, Protocol 3.1]. A formal description of the protocol is given in Protocol 1.

Protocol 1. General blind randomness expansion protocol

Protocol arguments

G	:	two-player non-local game, specified by a question set $\mathcal{X} \times \mathcal{Y}$, a probability distribution q on $\mathcal{X} \times \mathcal{Y}$, an answer set $\mathcal{A} \times \mathcal{B}$, and a winning condition $\omega : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$
$x^* \in \mathcal{X}$, $y^* \in \mathcal{Y}$	:	inputs used for generation rounds
D	:	untrusted device capable of playing one side of G repeatedly
$n \in \mathbb{N}$	:	number of rounds
$\gamma \in (0, 1]$	:	expected fraction of test rounds
ω_{exp}	:	expected winning probability in G
δ	:	error tolerance

Protocol steps

For rounds $i = 1, \ldots, n$, Alice performs the following steps:

(1) Alice chooses $T_i \in \{0, 1\}$ with $\Pr[T_i = 1] = \gamma$. If $T_i = 1$, Alice chooses $X_i, Y_i \in \mathcal{X} \times \mathcal{Y}$ according to the question distribution q. If $T_i = 0$, Alice chooses $X_i = x^*, Y_i = y^*$.
(2) Alice inputs X_i into her device D and sends Y_i to Eve. She receives answers A_i and B_i, respectively.
(3) If $T_i = 0$, Alice sets $C_i = \perp$. If $T_i = 1$, Alice sets $C_i = \omega(X_i, Y_i, A_i, B_i)$.

At the end of the protocol, Alice aborts if $|\{i \text{ s.t. } C_i = 0\}| > (1 - \omega_{\text{exp}} + \delta) \cdot \gamma n$.

The following proposition shows a lower bound on on the amount of randomness Alice can extract from this protocol, as specified by the min-entropy. For this, we assume a lower-bound on the single-round von Neumann entropy. Such a single-round bound can be found numerically using a generic method as explained after the proof of Lemma 5.1.

Proposition 5.1. *Suppose Alice executes Protocol 1 with a device D that cannot communicate with Eve. We denote by R_i and E_i' the (arbitrary) quantum systems of the device D and the adversary Eve after the i-th round, respectively. Eve's full side-information after the i-th round is $E_i := T^i X^i Y^i B^i E_i'$. A single round of the protocol can be described by a quantum channel $\mathcal{N}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, C_i A_i R_i E_i)$. We also define $\mathcal{N}_i^{\mathrm{test}}$ to be the same as $\mathcal{N}_i$, except that $\mathcal{N}_i^{\mathrm{test}}$ always picks $T_i = 1$. Let $\rho_{A^n C^n R_n E_n}$ be the state at the end of the protocol and Ω the event that Alice does not abort.*

Let $g : \mathbb{P}(\{0,1\}) \to \mathbb{R}$ be an affine function satisfying the conditions

$$g(p) \leq \inf_{\omega \in \mathrm{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1}):\, \mathcal{N}_i^{\mathrm{test}}(\omega)_{C_i} = p} H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{N}_i(\omega)}\,, \qquad \mathsf{Max}(g) = g(\delta_1)\,, \tag{5.1}$$

where $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}$ is a purifying system. Then, for any $\varepsilon_a, \varepsilon_s \in (0,1)$, either $\Pr[\Omega] \leq \varepsilon_a$ *or*

$$H_{\min}^{\varepsilon_s}(A^n|E_n)_{\rho_{|\Omega}} \geq nh - c_1\sqrt{n} - c_0$$

for $c_1, c_0 \geq 0$ independent of n and

$$h = \min_{p' \in \mathbb{P}(\{0,1\}):\, p'(0) \leq 1 - \omega_{\exp} + \delta} g(p')\,,$$

where $\omega_{\exp}$ is the expected winning probability and δ the error tolerance from Protocol 1. If we treat ε_s, ε_a, $\dim(A_i)$, δ, $\mathsf{Max}(g)$, and $\mathsf{Min}(g)$ as constants, then $c_1 = O(1/\sqrt{\gamma})$ and $c_0 = O(1)$.

Furthermore, if there exists a quantum strategy that wins the game G with probability $\omega_{\exp}$, there is an honest behaviour of D and Eve for which $\Pr[\Omega] \geq 1 - \exp(-\frac{\delta^2}{1-\omega_{\exp}+\delta}\gamma n)$.

Remark 5.2. The condition on $g(p)$ in Eq. (5.1) is formulated in terms of the entropy

$$H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{N}_i(\omega)} = H(A_i|T^i X^i Y^i B^i E_i'\tilde{E}_{i-1})_{\mathcal{N}_i(\omega)}$$

with $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}$. However, the map $\mathcal{N}_i$ corresponding to the i-th round does not act on the systems $T^{i-1}X^{i-1}Y^{i-1}B^{i-1}$. Therefore, we can view these systems as part of the purifying system. Since the infimum in Eq. (5.1) already includes a purifying $\tilde{E}_{i-1}$, we can drop these additional systems and without loss of generality choose $\tilde{E}_{i-1}$ to be isomorphic to those input systems on which $\mathcal{N}_i$ acts non-trivially, i.e. $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}'$. This means that we can replace the upper bound on g in Eq. (5.1) by the equivalent condition

$$g(p) \leq \inf_{\omega \in \mathrm{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1}):\, \mathcal{N}_i^{\mathrm{test}}(\omega)_{C_i} = p} H(A_i|B_i X_i Y_i T_i E_i'\tilde{E}_{i-1})_{\mathcal{N}_i(\omega)} \tag{5.2}$$

with $\tilde{E}_{i-1} \equiv R_{i-1}E_{i-1}'$. For the proof of Lemma 5.1 we will use Eq. (5.1) since it more closely matches the notation of Theorem 4.3, but intuitively, Eq. (5.2) is more natural as it only involves quantities related to the i-th round of the protocol.

Proof of Lemma 5.1. To show the min-entropy lower bound, we will make use of Corollary 4.6. For this, we first check that the maps $\mathcal{N}_i$ satisfy the required conditions. Since C_i is a deterministic function of the (classical) variables X_i, Y_i, A_i, and B_i, it is clear that Eq. (4.2) is satisfied. For the non-signalling condition, we define the map $\mathcal{R}_i \in \mathrm{CPTP}(E_{i-1}, E_i)$ as follows: $\mathcal{R}_i$ samples T_i, X_i and Y_i as Alice does in Step 5.1 of Protocol 1. $\mathcal{R}$ then performs Eve's actions in the protocol (which only act on Y_i and E'_{i-1}, which is part of E_{i-1}). It is clear that the distribution on X_i and Y_i produced by $\mathcal{R}_i$ is the same as for $\mathcal{N}_i$. By the assumption that D and Eve cannot communicate, the marginal of the output of $\mathcal{N}_i$ on Eve's side must be independent of the device's system R_{i-1}. Hence, $\mathrm{Tr}_{A_i R_i C_i} \circ \mathcal{N}_i = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}$.

To construct a min-tradeoff function, we note that we can split $\mathcal{N}_i = \gamma \mathcal{N}_i^{\text{test}} + (1-\gamma)\mathcal{N}_i^{\text{data}}$, with $\mathcal{N}_i^{\text{test}}$ always picking $T_i = 1$ and $\mathcal{N}_i^{\text{data}}$ always picking $T_i = 0$. Then, we get from Lemma 4.7 and the condition $\mathsf{Max}(g) = g(\delta_1)$ that the affine function f defined by

$$f(\delta_0) = g(\delta_1) + \frac{1}{\gamma}(g(\delta_0) - g(\delta_1)), \qquad f(\delta_1) = f(\delta_\perp) = g(\delta_1)$$

is an affine min-tradeoff function for $\{\mathcal{N}_i\}$.

Viewing the event Ω as a subset of the range $\{0,1\}^n$ of the random variable C^n and comparing with the abort condition in Protocol 1, we see that $c^n \in \Omega$ implies $\mathsf{freq}(c^n)(0) \leq (1 - \omega_{\text{exp}} + \delta)\gamma$. Therefore, for $c^n \in \Omega$ and denoting $p = \mathsf{freq}(c^n)$,

$$f(\mathsf{freq}(c^n)) = p(0)f(\delta_0) + (1-p(0))f(\delta_1) = \frac{p(0)}{\gamma} g(\delta_0) + \left(1 - \frac{p(0)}{\gamma}\right) g(\delta_1) \geq h,$$

where the last inequality holds because g is affine and the distribution $p'(0) = p(0)/\gamma, p'(1) = 1 - p(0)/\gamma$ satisfies $p'(0) \leq 1 - \omega_{\text{exp}} + \delta$. The proposition now follows directly from Corollary 4.6 and the scaling of c_1 and c_0 is easily obtained from the expressions in Corollary 4.6.

To show that an honest strategy succeeds in the protocol with high probability, we define a random variable F_i by $F_i = 1$ if $C_i = 0$, and $F_i = 0$ otherwise. If D and Eve execute the quantum strategy that wins the game G with probability ω_{exp} in each round, then $\mathbb{E}[F_i] = (1 - \omega_{\text{exp}})\gamma$. Using the abort condition in the protocol, we then find

$$\begin{aligned}
\Pr[\text{abort}] &= \Pr\left[\sum_{i=1}^n F_i > (1 - \omega_{\text{exp}} + \delta) \cdot \gamma n\right] \\
&= \Pr\left[\sum_{i=1}^n F_i > \left(1 + \frac{\delta}{1 - \omega_{\text{exp}}}\right) \cdot \mathbb{E}\left[\sum_{i=1}^n F_i\right]\right] \\
&\leq e^{-\frac{\delta^2}{1-\omega_{\text{exp}}+\delta}\gamma n},
\end{aligned}$$

where in the last line we used a Chernoff bound. □

To make use of Lemma 5.1, we need to construct a function $g(p)$ that satisfies the condition in Eq. (5.1). For this, we will use the equivalent condition Eq. (5.2). A general way of obtaining such a bound automatically is using the recent numerical method [22].[14]

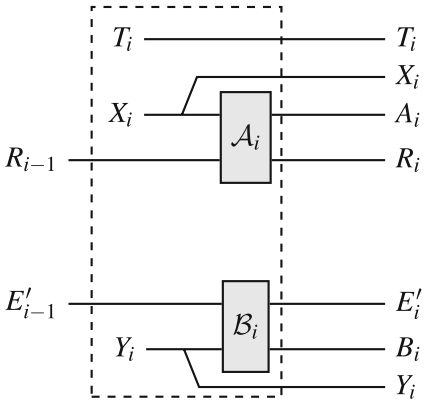


Fig. 1. Circuit diagram of $\mathcal{N} : R_{i-1}E'_{i-1} \to A_i R_i T_i X_i Y_i B_i E'_i$. For every round of the protocol, a circuit of this form is applied, where $\mathcal{A}$ and $\mathcal{B}$ are the (arbitrary) channels applied by Alice's device and Eve, respectively. As in the protocol, T_i is a bit equal to 1 with probability γ, and X_i and Y_i are generated according to q whenever $T_i = 1$, and are fixed to x^*, y^* otherwise. We did not include the register C_i in the figure as it is a deterministic function of $T_i X_i Y_i A_i B_i$

Specifically, using the assumption that Alice's lab is isolated, the maps $\mathcal{N}_i$ describing a single round of the protocol take the form described in Fig. 1.

The method of [22] allows one to obtain lower bounds on the infimum of

$$H(A_i|B_i X_i Y_i T_i E'_i \tilde{E}_{i-1})_{\mathcal{N}_i(\omega_{R_{i-1}E'_{i-1}\tilde{E}_{i-1}})}$$

over all input states $\omega_{R_{i-1}E'_{i-1}\tilde{E}_{i-1}}$ and for any map $\mathcal{N}_i$ of the form depicted in Fig. 1. Importantly, for any $\mathcal{N}_i$ we may also restrict the infimum to states ω that are consistent with the observed statistics, i.e., $\mathcal{N}^{\text{test}}(\omega)_{C_i} = p$ for some distribution p on C_i, using the notation of Lemma 5.1. Using this numerical method for the CHSH game, we obtain the values shown in Fig. 2. From this, one can also construct an explicit affine min-tradeoff function $g(p)$ in an automatic way using the same method as in [46]. As our focus is on illustrating the use of the generalised EAT, not the single-round bound, we do not carry out these steps in detail here.

Combining this single-round bound and Lemma 5.1, one obtains that for Protocol 1 instantiated with the CHSH game, ω_{exp} sufficiently close to the maximal winning probability of $\frac{1}{2} + \frac{1}{2\sqrt{2}}$, and $\gamma = \Theta(\frac{\log n}{n})$, one can extract $\Omega(n)$ bits of uniform randomness from $A_1 \dots A_n$ while using only polylog(n) bits of randomness to run the protocol. In other words, Protocol 1 achieves exponential blind randomness expansion with the CHSH game.

[14] The main result of [15] (Theorem 14) does not appear to be sufficient for this. The reason is that the statement made in [15] essentially concerns the randomness produced on average over the question distribution q of the game G. However, choosing a question at random consumes randomness, so to achieve exponential randomness expansion, in Protocol 1 we fix the inputs x^*, y^* used for generation rounds. To the best of our knowledge, the results of [15] do not give a bound on the randomness produced in the non-local game for any *fixed* inputs x^*, y^*. If one could prove an analogous statement to [15, Theorem 14] that also certifies randomness on fixed inputs for a large class of games, our Lemma 5.1 would then imply exponential blind randomness expansion for any such game. Alternatively, one can also assume that public (non-blind) randomness is a free resource and use this to choose the inputs for the non-local game. Then, no special inputs x^*, y^* are needed in Protocol 1 to "save randomness" and the result of [15] combined with our generalised EAT implies that such a conversion from public to blind randomness is possible for any complete-support game.

5.2. E91 quantum key distribution protocol. The E91 protocol is one of the simplest entanglement-based QKD protocols [45,47]. This protocol was already treated using the original EAT in [1]. Here, we do not give a formal security definition and proof, only an informal comparison of how the original EAT and our generalised EAT can be applied to this problem; the remainder of the security proof is then exactly as in [1]. For a detailed treatment of the application of our generalised EAT to QKD, see [7]. To facilitate the comparison with [1], in this section we label systems the same as in [1] even though this differs from the system labels used earlier in this paper. The protocol we are considering is described explicitly in Protocol 2. It is the same as in [1] except for minor modifications to simplify the notation.

Protocol 2. E91 quantum key distribution protocol

Protocol arguments

$n \in \mathbb{N}$	:	number of uses of qubit channel
$\mu \in (0, 1)$	:	probability for measurements in diagonal basis
$e \in (0, \frac{1}{2})$	:	maximum tolerated phase error ratio
$\vartheta_{\mathrm{EC}} \in [0, 1]$	:	relative communication cost of error correction scheme EC
$r \in [0, 1]$	:	key rate

Protocol steps

(1) *Distribution:* For $i \in \{1, \ldots, n\}$, Alice prepares a pair $(Q_i, \bar{Q}_i)$ of entangled qubits and sends $\bar{Q}_i$ to Bob. Alice generates a random bit B_i such that $P_{B_i}(1) = \mu$ and, depending on whether $B_i = 0$ or $B_i = 1$, measures Q_i in either the computational or the diagonal basis, storing the outcome as A_i. In the same way, Bob measures $\bar{Q}_i$ in a basis determined by a random bit $\bar{B}_i$, storing the outcome as $\bar{A}_i$.

(2) *Sifting and information reconciliation:* Alice and Bob announce B_i and $\bar{B}_i$. On indices i where $B_i \neq \bar{B}_i$, they set $A_i = \bar{A}_i = \perp$. They invoke a reliable[15] error correction scheme EC, allowing Bob to compute a guess $\hat{A}^n$ for Alice's string A^n. If EC does not output a guess then the protocol is aborted.

(3) *Parameter estimation:* Bob counts the number of indices $i \in S$ for which $\bar{B}_i = 1$ and $\bar{A}_i \neq \hat{A}_i$. If this number is larger than $e\mu^2 n$ then the protocol is aborted.

(4) *Privacy amplification:* See [1, p. 894] for details.

We consider the systems $B_i, \bar{B}_i, A_i, \bar{A}_i, Q_i, \bar{Q}_i$ as in Protocol 2 and additionally define the system X_i storing the statistical information used in the parameter estimation step:

$$X_i = \begin{cases} A_i \oplus \bar{A}_i & \text{if } B_i = \bar{B}_i = 1, \\ \perp & \text{otherwise.} \end{cases}$$

Denoting by E the side information gathered by Eve during the distribution step, we can follow the same steps as for [1, Equation (57)] to show that the security of Protocol 2 follows from a lower bound on

$$H_{\min}^{\varepsilon}(A^n | B^n \bar{B}^n E)_{\rho_{|\Omega}} . \tag{5.3}$$

Here, $\rho_{|\Omega}$ is the state at the end of the protocol conditioned on acceptance.

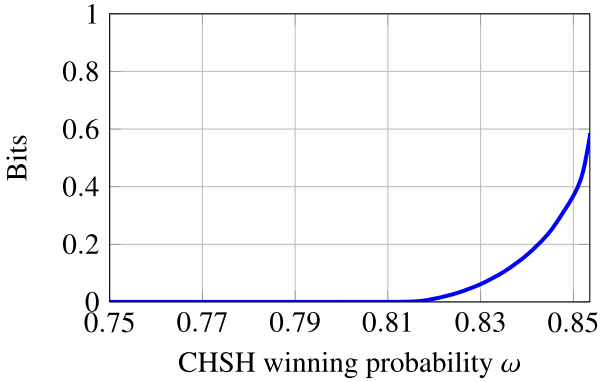


Fig. 2. Lower bound on the conditional entropy $H(A_i|B_i X_i Y_i T_i E_i')_{\rho|T_i=0}$ for any state generated as in Fig. 1 and such that on test rounds the obtained winning probability for the CHSH game is ω. This lower bound was obtained by using the method from [22]. For each input $y \in \mathcal{Y}$, the channel $\mathcal{B}_y$ is modelled as $\mathcal{B}_y(\omega) = \sum_b \Pi_y^{(b)} \omega \Pi_y^{(b)}$, where $\{\Pi_y^{(b)}\}_{b\in\mathcal{B}}$ are orthogonal projectors summing to the identity, and similarly for the map $\mathcal{A}$. It is simple to see that this is without loss of generality

We first sketch how the original EAT (whose setup was described in Sect. 1) is applied to this problem in [1]. One cannot bound $H_{\min}^{\varepsilon}(A^n|B^n\bar{B}^n E)_{\rho|\Omega}$ directly using the EAT because a condition similar to Eq. (4.2) has to be satisfied. Therefore, one modifies the systems $\bar{A}_i$ from Protocol 2 by setting $\bar{A}_i = \perp$ if $B_i = \bar{B}_i = 0$ and then applies the EAT to find a lower bound on

$$H_{\min}^{\varepsilon}(A^n\bar{A}^n|B^n\bar{B}^n E)_{\rho|\Omega}\,. \tag{5.4}$$

For this, a round of Protocol 2 is viewed as a map $\mathcal{M}_i : Q_i^n \bar{Q}_i^n \to Q_{i+1}^n \bar{Q}_{i+1}^n A_i \bar{A}_i B_i \bar{B}_i X_i$, which chooses $B_i\bar{B}_i$ as in Protocol 2, applies Alice and Bob's (trusted) measurements on systems $Q_i\bar{Q}_i$ to generate $A_i\bar{A}_i$, and generates X_i as described before. To apply the EAT, $R_{i-1} := Q_i^n \bar{Q}_i^n$ takes the role of the "hidden sytem", and $A_i\bar{A}_i$ and $B_i\bar{B}_i$ are the output and side information of the i-th round, respectively. It is easy to see that with this choice of systems, the Markov condition of the EAT is satisfied, so, using a min-tradeoff function derived from an entropic uncertainty relation [48], one can find a lower bound on Eq. (5.4).

However, adding the system $\bar{A}_i$ in this manner has the following disadvantage: to relate the lower bound on $H_{\min}^{\varepsilon}(A^n\bar{A}^n|B^n\bar{B}^n E)_{\rho|\Omega}$ to the desired lower bound on $H_{\min}^{\varepsilon}(A^n|B^n\bar{B}^n E)_{\rho|\Omega}$ one needs to use a chain rule for min-entropies, incurring a penalty term of the form $H_{\max}^{\varepsilon}(\bar{A}^n|A^n B^n \bar{B}^n E)_{\rho|\Omega}$. This penalty term is relatively easy to bound for the case of the E91 protocol, but can cause problems in general.[15]

We now turn our attention to proving Eq. (5.3) using our generalised EAT. For this, we first observe that

$$H_{\min}^{\varepsilon}(A^n|B^n\bar{B}^n E)_{\rho|\Omega} \geq H_{\min}^{\varepsilon}(A^n|B^n\bar{B}^n X^n E)_{\rho|\Omega}\,,$$

so it suffices to find a lower bound on the r.h.s. This step is similar to adding the $\bar{A}_i$ systems in Eq. (5.4) in that its purpose is to satisfy Eq. (4.2). However, it has the advantage that here, X^n can be added to the *conditioning* system and therefore lowers the

[15] An error correction scheme is reliable if, except with negligible probability, either Bob's guess of Alice's string is correct or the protocol aborts.

entropy, not raises it like going from Eqs. (5.3) to (5.4). The same step is not possible in the original EAT due to the restrictive Markov condition.

Using the same system names as before, we define $E_i := Q_{i+1}^n \bar{Q}_{i+1}^n B^i \bar{B}^i X^i E$.[16] Then, analogously to the original EAT, we can describe a single round of Protocol 2 by a map $\mathcal{M}_i : E_{i-1} \to A_i E_i X_i$. (Compared to the map $\mathcal{M}_i$ we described above for the original EAT, we have traced out $\bar{A}_i$, added a copy of X_i, and added identity maps on the other additional systems in E_{i-1}.) Denoting by $\rho^0_{Q^n \bar{Q}^n E}$ the joint state of Alice and Bob's systems $Q^n \bar{Q}^n$ before measurement and the information E that Eve gathered during the distribution step, the state at the end of the protocol is $\rho = \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0)$. To apply Corollary 4.6 to find a lower bound on

$$H_{\min}^{\varepsilon}(A^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0)_{|\Omega}},$$

we first observe that the condition in Eq. (4.2) is satisfied because the system X^n is part of E_n, and the non-signalling condition is trivially satisfied because there is no R_i-system. A min-tradeoff function can be constructed in exactly the same way as in [1, Claim 5.2] by noting that all systems in E_i on which $\mathcal{M}_i$ does not act can be viewed as part of the purifying system.

This comparison highlights the advantage of the more general model of side information in our generalised EAT: for the original EAT, one has to first bound $H_{\min}^{\varepsilon}(A^n \bar{A}^n | B^n \bar{B}^n E)$ (rather than $H_{\min}^{\varepsilon}(A^n | B^n \bar{B}^n E)$) in order to be able to satisfy the Markov condition, and then perform a separate step to remove the $\bar{A}^n$ system. In our case, the non-signalling condition, the analogue of the Markov condition, is trivially satisfied because we need no R_i-system. This is because we can add the quantum systems $Q^n \bar{Q}^n$ to the side information register E_0 at the start and then, since we allow side information to be updated and Alice and Bob act on $Q_i \bar{Q}_i$ using trusted measurement devices, we can remove the systems $Q_i \bar{Q}_i$ one by one during the rounds of the protocol.

Acknowledgement We thank Rotem Arnon-Friedman, Peter Brown, Kun Fang, Raban Iten, Joseph M. Renes, Martin Sandfuchs, Ernest Tan, Jinzhao Wang, John Wright, and Yuxiang Yang for helpful discussions. We further thank Mario Berta and Marco Tomamichel for insights on Lemma 3.2, and Frédéric Dupuis and Carl Miller for discussions about blind randomness expansion.

Funding Open access funding provided by Swiss Federal Institute of Technology Zurich TM and RR acknowledge support from the National Centres of Competence in Research (NCCRs) QSIT (funded by the Swiss National Science Foundation under grant number 51NF40-185902) and SwissMAP, the Air Force Office of Scientific Research (AFOSR) via project No. FA9550-19-1-0202, the SNSF project No. 200021_188541 and the QuantERA project eDICT. OF acknowledges funding from the European Research Council (ERC Grant AlgoQIP, Agreement No. 851716), from the European Union's Horizon 2020 QuantERA II Programme (VERIqTAS, Agreement No 101017733) and from a government grant managed by the Agence Nationale de la Recherche under the Plan France 2030 with the reference ANR-22-PETQ-0009. Part of this work was carried out when DS was with the Institute for Theoretical Physics at ETH Zurich.

[16] In Protocol 2, instead of Alice distributing the systems $Q_i \bar{Q}_i$ and Eve gathering side information E by intercepting $\bar{Q}_i$, we can equivalently imagine that Eve first prepares a state $\rho^0_{Q^n \bar{Q}^n E}$ and distributes $Q_i \bar{Q}_i$ to Alice and Bob in each round. Then, the choice of E_i intuitively captures the side information available to Eve from the first i rounds: Eve still possesses the systems $Q_{i+1}^n \bar{Q}_{i+1}^n$ to be distributed in future rounds, has gathered classical information $B^i \bar{B}^i X^i$, and keeps the static side information E from preparing the initial state.

Data Availability No experimental data has been generated as part of this project. The introduction of this work has been published as an extended abstract in the proceedings of FOCS 2022 [49].

Declarations

Conflict of interest The authors have no Conflict of interest to declare.

A. Dual Statement for Smooth Max-Entropy

In the main text we have focused on deriving a lower bound on the smooth min-entropy. Here, we show that this also implies an upper bound on the smooth max-entropy by applying a simple duality relation between min- and max-entropy. A similar upper bound was also derived in [1]. However, that bound is subject to a Markov condition and cannot be derived by a simple duality argument since the "dual version" of the Markov condition is unwieldy. We show that the bound from [1] follows as a special case of our more general bound even without any Markov conditions or other non-signalling constraints. For simplicity, we restrict ourselves to an asymptotic statement without "testing", i.e. we derive an $H_{\max}^{\varepsilon}$-version of Theorem 4.1. By applying the same duality relation to the more involved statement in Theorem 4.3, one can also obtain an $H_{\max}^{\varepsilon}$-bound with explicit constants and testing.

Recall that for $\rho_{AB} \in \mathrm{S}(AB)$ and $\varepsilon \in [0,1]$, the ε-smoothed max-entropy of A conditioned on B is defined as

$$H_{\max}^{\varepsilon}(A|B)_{\rho} = \log \inf_{\tilde{\rho}_{AB} \in \mathcal{B}_{\varepsilon}(\rho_{AB})} \sup_{\sigma_B \in \mathrm{S}(B)} \left\| \tilde{\rho}_{AB}^{\frac{1}{2}} \sigma_B^{\frac{1}{2}} \right\|_1^2 ,$$

where $\|\cdot\|_1$ denotes the trace norm and $\mathcal{B}_{\varepsilon}(\rho_{AB})$ is the ε-ball around ρ_{AB} in terms of the purified distance [11]. The smooth min- and max-entropy satisfy the following duality relation [11, Proposition 6.2]: for a pure quantum state ψ_{ABC},

$$H_{\min}^{\varepsilon}(A|B)_{\psi} = -H_{\max}^{\varepsilon}(A|C)_{\psi} .$$

For the setting of Theorem 4.1, let $V_i : R_{i-1}E_{i-1} \to A_i R_i E_i F_i$ be the Stinespring dilation of the map $\mathcal{M}_i$, and let $|\rho^0\rangle_{R_0 E_0 F_0}$ be a purification of the input state $\rho^0_{R_0 E_0}$. Then, $V_n \cdots V_1 |\rho^0\rangle$ is a purification of $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0)$, so by the duality of the smooth min- and max-entropy,

$$H_{\min}^{\varepsilon}(A^n|E_n)_{\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho^0)} = -H_{\max}^{\varepsilon}(A^n|F^n R_n)_{V_n \cdots V_1 |\rho^0\rangle} .$$

Furthermore, by concavity of the conditional entropy the infimum in Theorem 4.1 can be restricted to pure states $|\omega\rangle_{R_{i-1}E_{i-1}\tilde{E}_{i-1}}$, so $V_i|\omega\rangle$ is a purification of $\mathcal{M}_i(\omega)$. Then, by the duality relation for von Neumann entropies,

$$H(A_i|E_i\tilde{E}_{i-1})_{\mathcal{M}_i(\omega)} = -H(A_i|R_iF_i)_{V_i|\omega\rangle}\,.$$

Therefore, we obtain the following dual statement to Theorem 4.1:

$$H^{\varepsilon}_{\max}(A^n|F^nR_n)_{V_n\cdots V_1|\rho^0\rangle} \leq \sum_{i=1}^{n} \max_{|\omega\rangle} H(A_i|R_iF_i)_{V_i|\omega\rangle} + O(\sqrt{n})\,, \tag{A.1}$$

where the maximisation is over pure states on $R_{i-1}E_{i-1}\tilde{E}_{i-1}$. This holds for any sequence of isometries V_i for which the maps $\mathcal{M}_{V_i} : R_{i-1}E_{i-1} \to A_iR_iE_i$ given by $\mathcal{M}_{V_i}(\rho) = \mathrm{Tr}_{F_i}\left[V_i\rho V_i^\dagger\right]$ satisfy the non-signalling condition of Theorem 4.1: for each i, there must exist a map $\mathcal{R}_i \in \mathrm{CPTP}(E_{i-1}, E_i)$ such that $\mathrm{Tr}_{A_iR_i} \circ \mathcal{M}_{V_i} = \mathcal{R}_i \circ \mathrm{Tr}_{R_{i-1}}$.

To gain some intuition for the above statement, consider a setting where an information source generates systems $A_1, \ldots, A_n$ and $F_1, \ldots, F_n$ by applying isometries $V_i : S_{i-1} \to A_iF_iS_i$ to some pure intial state $|\rho^0\rangle_{S_0}$. We might be interested in compressing the information in A^n in such a way that given F^n, one can reconstruct A^n except with some small failure probability ε. Then, the amount of storage needed for the compressed information is given by $H^{\varepsilon}_{\max}(A^n|F^n)$. To apply Eq. (A.1), for $i < n$ we split the systems S_i into R_iE_i in such a way that the channel $\mathcal{M}_{V_i}$ defined above satisfies the non-signalling condition, and set $E_n = S_n$ (so that R_n is trivial). Then Eq. (A.1) gives an upper bound on $H^{\varepsilon}_{\max}(A^n|F^n)$. Note that this bound depends on how we split the systems $S_i = R_iE_i$: the non-signalling condition can always be trivially satisfied by choosing R_i to be trivial, but Eq. (A.1) tells us that if we can describe the source in such a way that E_i is relatively small and R_i is relatively large while still satisfying the non-signalling condition, we obtain a tighter bound on the amount of required storage.

From Eq. (A.1) we can also recover the max-entropy version of the original EAT, but without requiring a Markov condition. To facilitate the comparison with [1], we first re-state their theorem with their choice of system labels, but add a bar to every system label to avoid confusion with our notation from before. The max-entropy statement in [1] considers a sequence of channels $\bar{\mathcal{M}}_i : \bar{R}_{i-1} \to \bar{A}_i\bar{B}_i\bar{R}_i$ and asserts that under a Markov condition, for any initial state $\rho_{\bar{R}_0\bar{E}}$ with a purifying system $\bar{E} \equiv \bar{R}_0$:

$$H^{\varepsilon}_{\max}(\bar{A}^n|\bar{B}^n\bar{E})_{\bar{\mathcal{M}}_n\circ\cdots\circ\bar{\mathcal{M}}_1(\rho_{\bar{R}_0\bar{E}})} \leq \sum_{i=1}^{n} \max_{\omega\in S(\bar{R}_{i-1}\bar{R})} H(\bar{A}_i|\bar{B}_i\bar{R})_{\bar{\mathcal{M}}_i(\omega)} + O(\sqrt{n})\,, \tag{A.2}$$

where $\bar{R} \equiv \bar{R}_{i-1}$. We want to recover this statement from Eq. (A.1) *without any Markov condition*. For this, we consider the Stinepring dilations $\bar{V}_i : \bar{R}_{i-1} \to \bar{R}_i\bar{A}_i\bar{B}_i\bar{F}_i$ of $\bar{\mathcal{M}}_i$. We make the following choice of systems:

$$R_i = \bar{B}^i\bar{E}\,, \quad A_i = \bar{A}_i\,, \quad E_i = \bar{R}_i\bar{F}_i\,,$$

and choose F_i to be trivial. By tensoring with the identity, we can then extend $\bar{V}_i$ to an isometry $V_i : R_{i-1}E_{i-1} \to A_iR_iE_i$. Then, the maps $\mathcal{M}_{V_i}$ satisfy the non-signalling condition since V_i acts as identity on R_{i-1}. Therefore, remembering that $R_n = \bar{B}^n\bar{E}$

and F^n is trivial, we see that Eq. (A.1) implies Eq. (A.2). Note that our derivation did not require any conditions on the channels $\bar{\mathcal{M}}_i$ we started with, i.e. we have shown Eq. (A.2) holds for any sequence of channels $\bar{\mathcal{M}}_i$, not just channels satisfying a Markov or non-signalling condition.

B. Uhlmann Property for the Rényi Divergence

We establish that for the max-divergence (where $\alpha \to \infty$), Uhlmann's theorem holds.

Proposition B.1. *Let $\sigma_A \in \mathrm{S}(A)$ and $\rho_{AR} \in \mathrm{S}(AR)$. Then we have*

$$D_{\max}(\rho_A \| \sigma_A) = \inf_{\hat{\sigma}_{AR} \,:\, \hat{\sigma}_A = \sigma_A} D_{\max}(\rho_{AR} \| \hat{\sigma}_{AR}) \,. \tag{B.1}$$

In addition, if $\rho_{AR}, \rho_A \otimes \mathrm{id}_R$ and $\sigma_A \otimes \mathrm{id}_R$ all commute, then for any $\alpha \in [\frac{1}{2}, \infty)$, we have

$$D_\alpha(\rho_A \| \sigma_A) = \inf_{\hat{\sigma}_{AR} \,:\, \hat{\sigma}_A = \sigma_A} D_\alpha(\rho_{AR} \| \hat{\sigma}_{AR}) \,. \tag{B.2}$$

Proof. We start with Eq. (B.1). The inequality $\leq$ is a direct consequence of the data-processing inequality for $D_{\max}$. For the inequality $\geq$, we use semidefinite programming duality, see e.g., [50]. Observe that we can write $2^{D_{\max}(\rho_A \| \sigma_A)}$ as the following semidefinite program

$$\min_{\tau_A \in \mathrm{Pos}(A), \lambda \in \mathbb{R}} \{ \mathrm{Tr}[\tau_A] \;\text{ subject to }\; \rho_A \leq \tau_A \;\text{ and }\; \tau_A = \lambda \sigma_A \} \,.$$

Using semidefinite programming duality, this is also equal to

$$\max_{X_A \in \mathrm{Pos}(A), Y_A \in \mathrm{Herm}(A)} \{ \mathrm{Tr}\big[X_A \rho_A\big] \;\text{ subject to }\; \mathrm{id}_A + Y_A = X_A \;\text{ and }\; \mathrm{Tr}[Y_A \sigma_A] = 0 \} \,. \tag{B.3}$$

We can also write a semidefinite program for $\inf_{\hat{\sigma}_{AR} \,:\, \hat{\sigma}_A = \sigma_A} 2^{D_{\max}(\rho_{AR} \| \hat{\sigma}_{AR})}$. We introduce the variable $\theta_{AR} = \lambda \hat{\sigma}_{AR}$ and get

$$\min_{\theta \in \mathrm{Pos}(A \otimes R), \lambda \in \mathbb{R}} \{ \mathrm{Tr}[\theta_{AR}] \;\text{ subject to }\; \rho_{AR} \leq \theta_{AR} \;\text{ and }\; \theta_A = \lambda \sigma_A \} \,.$$

Again, by semidefinite programming duality, we get that it is equal to

$$\max_{X_{AR} \in \mathrm{Pos}(A \otimes R), Y_A \in \mathrm{Herm}(A)} \{ \mathrm{Tr}\big[X_{AR} \rho_{AR}\big] \;\text{ subject to }\; (\mathrm{id}_A + Y_A) \otimes \mathrm{id}_R = X_{AR} \;\text{ and }\; \mathrm{Tr}[Y_A \sigma_A] = 0 \} \,. \tag{B.4}$$

Eliminating the variable X_{AR}, we can write this last program as

$$\max_{Y_A \in \mathrm{Herm}(A)} \{ \mathrm{Tr}\big[(\mathrm{id}_A + Y_A) \rho_A\big] \;\text{ subject to }\; \mathrm{id}_A + Y_A \in \mathrm{Pos}(A) \;\text{ and }\; \mathrm{Tr}[Y_A \sigma_A] = 0 \} \,,$$

which is the same as Eq. (B.3). This proves Eq. (B.1). Equation (B.2) follows immediately by choosing $\hat{\sigma}_{AR} = \sigma_A \rho_A^{-1} \rho_{AR}$ and using the commutation conditions. □

However, for $\alpha \geq 1$ and arbitrary $\sigma_A \in \mathrm{S}(A)$, $\rho_{AE} \in \mathrm{S}(AE)$, the Uhlmann property given by Eq. (B.2) does not hold. A concrete example is $\rho_{AR} = |\psi\rangle\langle\psi|_{AR}$ with

$$|\psi\rangle_{AR} = \sqrt{\frac{1}{4}}|00\rangle_{AR} + \sqrt{\frac{3}{4}}|11\rangle_{AR}$$

and $\sigma_A = \frac{1}{3}|+\rangle\langle+| + \frac{2}{3}|-\rangle\langle-|$. In this case, $D_2(\rho_A\|\sigma_A) < 0.476$ whereas

$$\inf_{\hat{\sigma}_{AR} : \hat{\sigma}_A = \sigma_A} D_2(\rho_{AR}\|\hat{\sigma}_{AR}) \geq \inf_{\hat{\sigma}_{AR} : \hat{\sigma}_A = \sigma_A} D(\rho_{AR}\|\hat{\sigma}_{AR}) > 0.48\,.$$

This computation was performed by numerically solving the semidefinite programs via CVXQUAD [51]. Putting everything together shows that Eq. (B.2) does not hold for $\alpha \in \{1, 2\}$:

$$D(\rho_A\|\sigma_A) \leq D_2(\rho_A\|\sigma_A) < \inf_{\hat{\sigma}_{AR} : \hat{\sigma}_A = \sigma_A} D(\rho_{AR}\|\hat{\sigma}_{AR}) \leq \inf_{\hat{\sigma}_{AR} : \hat{\sigma}_A = \sigma_A} D_2(\rho_{AR}\|\hat{\sigma}_{AR})\,.$$

References

1. Dupuis, F., Fawzi, O., Renner, R.: Entropy accumulation. Commun. Math. Phys. **379**(3), 867–913 (2020)
2. Renner, R.: Security of quantum key distribution. Int. J. Quantum Inf. **6**(01), 1–127 (2008)
3. Tomamichel, M., Colbeck, R., Renner, R.: A fully quantum asymptotic equipartition property. IEEE Trans. Inf. Theory **55**(12), 5840–5847 (2009)
4. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R., Vidick, T.: Practical device-independent quantum cryptography via entropy accumulation. Nat. Commun. **9**(1), 459 (2018)
5. Bamps, C., Massar, S., Pironio, S.: Device-independent randomness generation with sublinear shared quantum resources. Quantum **2**, 86 (2018)
6. Petz, D.: Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. Commun. Math. Phys. **105**(1), 123–131 (1986)
7. Metger, T., Renner, R.: Security of quantum key distribution from generalised entropy accumulation. Preprint at arXiv:2203.04993 (2022)
8. Dupuis, F., Fawzi, O.: Entropy accumulation with improved second-order term. IEEE Trans. Inf. Theory **65**(11), 7596–7612 (2019)
9. Fawzi, H., Fawzi, O.: Defining quantum divergences via convex optimization. Quantum **5**, 387 (2021)
10. Uhlmann, A.: The "transition probability" in the state space of a $*$-algebra. Rep. Math. Phys. **9**(2), 273–279 (1976)
11. Tomamichel, M.: Quantum Information Processing with Finite Resources: Mathematical Foundations, vol. 5. Springer, Cham, Switzerland (2015)
12. Sutter, D.: Approximate Quantum Markov Chains. Springer, Cham (2018)
13. Christandl, M., König, R., Renner, R.: Postselection technique for quantum channels with applications to quantum cryptography. Phys. Rev. Lett. **102**(2), 020504 (2009)
14. Arnon-Friedman, R., Renner, R., Vidick, T.: Simple and tight device-independent security proofs. SIAM J. Comput. **48**(1), 181–225 (2019)
15. Miller, C.A., Shi, Y.: Randomness in nonlocal games between mistrustful players. Quantum Inf. Comput. **17**(7), 595 (2017)
16. Honghao, F., Miller, C.A.: Local randomness: examples and application. Phys. Rev. A **97**(3), 032324 (2018)
17. Colbeck, R.: Quantum and relativistic protocols for secure multi-party computation. PhD Thesis, University of Cambridge (2006)
18. Colbeck, R., Kent, A.: Private randomness expansion with untrusted devices. J. Phys. A Math. Theor. **44**(9), 095305 (2011)
19. Pironio, S., Acín, A., Massar, S., de La Giroday, A.B., Matsukevich, D.N., Maunz, P., Olmschenk, S., Hayes, D., Le Luo, L., Manning, T.A., et al.: Random numbers certified by Bell's theorem. Nature **464**(7291), 1021–1024 (2010)

20. Vazirani, U., Vidick, T..: Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In: Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, pp. 61–76 (2012)
21. Miller, C.A., Shi, Y.: Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. J. ACM (JACM) **63**(4), 1–63 (2016)
22. Brown, P., Fawzi, H., Fawzi, O.: Computing conditional entropies for quantum correlations. Nat. Commun. **12**(1), 1–12 (2021)
23. Chung, K.M., Shi, Y., Wu, X.: Physical randomness extractors: generating random numbers with minimal assumptions. Preprint at arXiv:1402.4797 (2014)
24. Coudron, M., Yuen, H..: Infinite randomness expansion with a constant number of devices. In: Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing, STOC '14, pp. 427-436, New York, NY, USA. Association for Computing Machinery (2014)
25. Kaniewski, J., Wehner, S.: Device-independent two-party cryptography secure against sequential attacks. New J. Phys. **18**(5), 055004 (2016)
26. Broadbent, A., Islam, R.: Quantum encryption with certified deletion. In: Theory of Cryptography Conference, pp. 92–122. Springer (2020)
27. Kundu, S., Tan, E.: Composably secure device-independent encryption with certified deletion. Preprint at arXiv:2011.12704 (2020)
28. Frauchiger, D., Renner, R., Troyer, M.: True randomness from realistic quantum devices. Preprint at arXiv:1311.4547 (2013)
29. Campbell, S., Vacchini, B.: Collision models in open system dynamics: A versatile tool for deeper insights? Europhys. Lett. **133**(6), 60001 (2021)
30. del Rio, L., Hutter, A., Renner, R., Wehner, S.: Relative thermalization. Phys. Rev. E **94**(2), 022104 (2016)
31. Akers, C., Penington, G.: Leading order corrections to the quantum extremal surface prescription. J. High Energy Phys. **2021**(4), 1–73 (2021)
32. Jain, R., Kundu, S.: A direct product theorem for quantum communication complexity with applications to device-independent QKD. In: 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS), pp. 1285–1295. IEEE (2022)
33. Zhang, Y., Fu, H., Knill, E.: Efficient randomness certification by quantum probability estimation. Phys. Rev. Res. **2**, 013016 (2020)
34. Knill, E., Zhang, Y., Bierhorst, P.: Generation of quantum randomness by probability estimation with classical side information. Phys. Rev. Res. **2**, 033465 (2020)
35. Müller-Lennert, M., Dupuis, F., Szehr, O., Fehr, S., Tomamichel, M.: On quantum Rényi entropies: a new generalization and some properties. J. Math. Phys. **54**(12), 122203 (2013)
36. Wilde, M.M., Winter, A., Yang, D.: Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. Commun. Math. Phys. **331**(2), 593–622 (2014)
37. Fang, K., Fawzi, O., Renner, R., Sutter, D.: Chain rule for the quantum relative entropy. Phys. Rev. Lett. **124**, 100501 (2020)
38. Hayashi, M.: Quantum Information Theory. Springer, Berlin Heidelberg (2017)
39. Christandl, M.: The Structure of Bipartite Quantum States-Insights from Group Theory and Cryptography. Ph. D. Thesis (2006)
40. Harrow, A.W.: Applications of coherent classical communication and the Schur transform to quantum information theory. Preprint at arXiv:quant-ph/0512255 (2005)
41. Leditzky, F., Kaur, E., Datta, N., Wilde, M.M.: Approaches for approximate additivity of the Holevo information of quantum channels. Phys. Rev. A **97**(1), 012332 (2018)
42. Liu, W.-Z., Li, M.-H., Ragy, S., Zhao, S.-R., Bai, B., Liu, Y., Brown, P.J., Zhang, J., Colbeck, R., Fan, J., et al.: Device-independent randomness expansion against quantum side information. Nat. Phys. **17**(4), 448–451 (2021)
43. Miller, C.A., Shi, Y.: Universal security for randomness expansion from the spot-checking protocol. SIAM J. Comput. **46**(4), 1304–1335 (2017)
44. Arqand, A., Hahn, T.A., Tan, E.Y.-Z.: Generalized renyi entropy accumulation theorem and generalized quantum probability estimation. Preprint at arXiv:2405.05912 (2024)
45. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
46. Brown, P., Ragy, S., Colbeck, R.: A framework for quantum-secure device-independent randomness expansion. IEEE Trans. Inf. Theory **66**(5), 2964–2987 (2019)
47. Christandl, M., Renner, R., Ekert, A.: A generic security proof for quantum key distribution. Preprint at arXiv:quant-ph/0402131 (2004)
48. Berta, M., Christandl, M., Colbeck, R., Renes, J.M., Renner, R.: The uncertainty principle in the presence of quantum memory. Nat. Phys. **6**(9), 659–662 (2010)
49. Metger, T., Fawzi, O., Sutter, D., Renner, R.: Generalised entropy accumulation. In: 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), pp. 844–850. IEEE (2022)

50. Watrous, J.: The Theory of Quantum Information. Cambridge University Press, Cambridge (2018)
51. Fawzi, H., Fawzi, O.: Efficient optimization of the quantum relative entropy. J. Phys. A Math. Theor. **51**(15), 154003 (2018)

Communicated by N. Linden