

Generalized Rényi Entropy Accumulation Theorem and Generalized Quantum Probability Estimation

Amir Arqand¹, Thomas A. Hahn², and Ernest Y.-Z. Tan¹

¹*Institute for Quantum Computing and Department of Physics and Astronomy,
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

²*The Center for Quantum Science and Technology, Department of Complex Systems,
Weizmann Institute of Science, Rehovot, Israel*

 (Received 26 October 2024; revised 1 May 2025; accepted 18 July 2025; published 28 October 2025)

The entropy accumulation theorem—and its subsequent generalized version—is a powerful tool in the security analysis of many device-dependent and device-independent cryptography protocols. However, it has the drawback that the finite-size bounds it yields are not necessarily optimal; furthermore, it relies on the construction of an affine min-tradeoff function, which can often be challenging to construct optimally in practice. In this work, we address both of these challenges simultaneously by deriving a new entropy accumulation bound. Our bound yields significantly better finite-size performance and can be computed as an intuitively interpretable convex optimization, without any specification of affine min-tradeoff functions. Furthermore, it can be applied directly at the level of Rényi entropies if desired, yielding fully-Rényi security proofs. Our proof techniques are based on elaborating on a connection between entropy accumulation and the frameworks of quantum probability estimation or f -weighted Rényi entropies; in the process, we obtain some new results with respect to those frameworks as well. In particular, those findings imply that our bounds apply to prepare-and-measure protocols without the virtual tomography procedures or repetition-rate restrictions previously required for entropy accumulation.

DOI: [10.1103/pgm-mz9j](https://doi.org/10.1103/pgm-mz9j)

Subject Areas: Quantum Physics, Quantum Information

I. INTRODUCTION

Many protocols in quantum cryptography consist of performing n rounds of some operations in order to generate a long string of raw data, which is then processed into the final secret key produced by the protocol. In security proofs of such protocols, it is often extremely useful to relate some operational “one-shot” quantity of the raw data string, such as smooth min-entropy, to simpler quantities that can be computed by just analyzing single rounds of the protocol. A powerful tool developed for this purpose is the entropy accumulation theorem (EAT) [1,2], which gives a relation that can be informally described as follows. Suppose the state ρ in the protocol can be produced by n channels acting “sequentially” in some sense, and denote the resulting “secret” raw data as S_1^n and some final side-information register as E_n . Then, letting Ω denote the event that the protocol accepts (based on some “test data” computed over the n rounds), the EAT states that as long as ρ satisfies some Markov conditions, its smooth

min-entropy conditioned on Ω satisfies a bound with the following form:

$$\text{(informal summary)} \\ H_{\min}^{\epsilon}(S_1^n | E_n)_{\rho_{|\Omega}} \geq n h_{vN} - O(\sqrt{n}), \quad (1)$$

where, loosely speaking, h_{vN} is a value slightly smaller than the minimum von Neumann entropy over all single-round states that are “compatible with” the accept condition. It suffices to yield a security proof since the $O(\sqrt{n})$ “finite-size correction” becomes negligible in comparison to the leading-order $n h_{vN}$ term at large n , so $(1/n) H_{\min}^{\epsilon}(S_1^n | E_n)_{\rho_{|\Omega}}$ converges asymptotically to h_{vN} . Subsequently, a generalized entropy accumulation theorem (GEAT) was developed [3,4], which relaxed the Markov conditions to a less-restrictive no-signalling condition, allowing a broader range of applications.

However, the existing EAT and GEAT results have some limitations. In particular, computing explicit values in their bounds requires specifying a technical object known as an affine min-tradeoff function, which affects both the h_{vN} term and the finite-size correction. The task of choosing and computing an affine min-tradeoff function that yields “good” finite-size bounds can be a very involved procedure in practice, as noted in, e.g., Ref. [5]. Furthermore, there is

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

the question of how tight the finite-size correction terms are since they are currently outperformed by approaches such as entropic uncertainty relations (EURs) for smooth entropies [6,7].

In this work, we address both of these challenges simultaneously. In particular, we present a bound that has no dependence on min-tradeoff functions at all, hence completely removing the issue of optimizing the choice of this function. Furthermore, the resulting finite-size bounds we obtain appear to be extremely tight. Our approach for achieving this result is to prove a bound somewhat similar to the above, specifically, a bound with the form

(informal summary)

$$H_{\alpha}^{\uparrow}(S_1^n|E_n)_{\rho_{\Omega}} \geq nh_{\hat{a}} - \frac{\alpha}{\alpha-1} \log \frac{1}{\Pr[\Omega]}, \quad (2)$$

where $H_{\alpha}^{\uparrow}$ is a (sandwiched) Rényi entropy with $\alpha > 1$ and $h_{\hat{a}}$ is a Rényi version of h_{vN} , i.e., loosely speaking, a value somewhat smaller than the minimum Rényi entropy over all single-round states that are “compatible with” the accept condition [8]. We also show that any “reasonable” protocol yields a strictly positive $h_{\hat{a}}$ value for classical S_1^n , as one would expect. Importantly, $h_{\hat{a}}$ can be computed as a convex optimization that does not involve any specification of an affine min-tradeoff function, removing the issue of choosing such a function. Our approach is based on techniques developed in Ref. [5], but we find that, by working directly with Rényi entropies, we obtain simpler final results.

This bound on the overall Rényi entropy has the appealing property of being a simple linear expression with only an $O(1)$ finite-size correction instead of $O(\sqrt{n})$ [9]. It is similar to bounds that were derived in Refs. [12–15] for min-entropy (the $\alpha \rightarrow \infty$ limit of $H_{\alpha}^{\uparrow}$) or collision entropy, but our result holds for *any* $\alpha > 1$ (under the original EAT conditions; for the GEAT conditions, it is restricted to $\alpha \in (1, 2)$, though this still suffices for most applications) [16]. In particular, similar to a recent work [17] (and an earlier work [18]), this work achieves the goal put forward in Ref. [10] of finding a “fully Rényi” approach for security proofs of many protocols by combining our bound with the Rényi privacy amplification theorem in that work. Our proof techniques also yield *upper* bounds on smooth max-entropy or $\alpha < 1$ Rényi entropies, if desired—such bounds can be useful for quantifying one-shot distillable entanglement [19].

While the entropy accumulation model is suitable for analyzing device-independent (DI) protocols and device-dependent entanglement-based (EB) protocols, it currently has limitations in device-dependent prepare-and-measure (PM) protocols, where one either has to introduce “virtual tomography” rounds [20] or impose a “single-signal interaction” condition that limits the repetition rate in the protocol [21]. Recently, in Ref. [17], a framework of f -weighted Rényi entropies was introduced, together with

an analysis of a suitable model for such protocols, which achieves the critical goal of overcoming this issue while simultaneously providing much tighter finite-size bounds. They also show that f -weighted Rényi entropies yield a very natural proof framework for protocols producing variable-length keys. Our results are closely connected to theirs, and we obtain very similar bounds, though since we mostly work in the EAT or GEAT models, our results are more suitable for DI or EB protocols than PM protocols.

Still, we contribute to slightly extending the results in Ref. [17] for PM protocols by providing some simplifications to their bounds for protocols producing fixed-length keys; in particular, we derive bounds of the form given in Eqs. (1) and (2) under the model they consider as well. Our techniques also provide an alternative approach for choosing tradeoff functions in their framework (the methods developed in Ref. [18] might also be relevant here), which we elaborate on in Sec. VIB. We thank the authors of that work for early presentations and discussions of their results to allow these comparisons.

More fundamentally, the proof techniques we used in this work expand on a connection between entropy accumulation and the concept of quantum probability estimation developed in Ref. [18], based on quantum estimation factors (QEFs). The latter was generally found to yield better finite-size key rates than the EAT in contexts such as DI randomness expansion (DIRE), though it has not yet been explicitly applied to DIQKD. We highlight that Ref. [18] described some connections between the EAT and their approach, including a conversion from min-tradeoff functions in the EAT to QEFs in their framework; however, the bounds that resulted from the latter conversion were quite suboptimal due to a sequence of conversions between von Neumann entropy and Rényi entropy. Our work shows that these conversions can be avoided by modifying some steps in the entropy accumulation proofs; in particular, under the Markov conditions of the original EAT, we can *exactly* reproduce the bounds that were obtained in the QEF framework. However, since we work in the general framework of entropy accumulation, this approach allowed us to obtain similar bounds under the GEAT conditions as well, which are less restrictive. In this sense, our results also serve to slightly generalize the QEF framework.

For ease of understanding, we now present an overview of the key results of our work, describing how they can be applied in security proofs.

A. Summary of key results for applications

While the main contribution of our work (based on the EAT or GEAT models) is best suited for DI protocols, for this overview, we focus on presenting the results we obtained in the context of device-dependent PM-QKD—the bounds we obtain in all of these cases have a very similar structure and can hence be discussed in similar

ways, but the channel structure for PM-QKD is easier to describe. To begin, we restate a standard result regarding how the state generated in a PM protocol can be reformulated as one generated by an EB protocol, which is the model used in Ref. [17] for analyzing such protocols. Specifically, by applying the source-replacement technique [22,23], one writes the state (before error correction and privacy amplification [6,24]) in the form

$$\rho_{S_1^n \hat{C}_1^n T_1^n \hat{E}} = \mathcal{M}^{\otimes n}[\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0], \quad (3)$$

where $\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0$ is the premeasurement quantum state between Alice, Bob, and Eve in the EB version of the protocol, and $\mathcal{M}: \tilde{A}\tilde{B} \rightarrow S\hat{C}T$ is simply a channel representing Alice's and Bob's single-round operations to produce the following registers: S is the secret data (after applying any required processing, such as sifting), and $\hat{C}T$ are public announcements, in which $\hat{C}$ denotes “test data” that Alice and Bob later use to decide whether to abort. (See Sec. VII B for an even more detailed description of these registers using the example of the BB84 protocol.) Furthermore, the source-replacement technique also has the property that Alice's registers $\tilde{A}_1^n$ are inaccessible to Eve even in the EB version, and hence the state $\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0$ satisfies $\omega_{\tilde{A}_1^n}^0 = \sigma_{\tilde{A}}^{\otimes n}$ for some known trusted state σ —note that this holds even though $\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0$ is the state after Eve has performed some *arbitrary* coherent attack.

Let us now focus on fixed-length protocols, i.e., protocols that always output a key of some specific *fixed* length whenever they accept. Furthermore, suppose that one step in deciding whether to accept consists of an “acceptance test” (sometimes also called “parameter estimation”) in which Alice and Bob compute the observed frequency distribution on the publicly announced registers $\hat{C}_1^n$ and accept if and only if it lies within some suitably chosen set S_Ω .

With this in mind, our main result for such protocols is the following, obtained by building on the work in Ref. [17] (which established a critical result regarding PM protocols; we present the details in Fact VI.1). It is a slightly restricted version of Theorem VI.1, which we present in full in Sec. VI B. (See Definition II.6 for the formal mathematical definition of the Rényi entropy $H_\alpha^\uparrow$; this technical aspect will not be critical to our discussion here. In addition, $D(\mathbf{q}||\mathbf{p})$ simply denotes the Kullback-Leibler divergence, which is a commonly used form of “distance” between any two probability distributions $\mathbf{q}$ and $\mathbf{p}$; see, e.g., Refs. [25,26] or Definition II.5 for details.)

Corollary I.1. Let $\rho_{S_1^n \hat{C}_1^n T_1^n \hat{E}}$ be a state of the form in Eq. (3), for an initial state $\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0$ satisfying $\omega_{\tilde{A}_1^n}^0 = \sigma_{\tilde{A}}^{\otimes n}$ for some state $\sigma_{\tilde{A}}$, and with all the $\hat{C}_j$ registers being classical. Let Ω denote the event that the frequency distribution on the classical registers $\hat{C}_1^n$ lies within some convex set S_Ω of

probability distributions, and let $\rho_{|\Omega}$ denote the state conditioned on Ω . Then, the following bound holds for any $\alpha \in (1, \infty]$:

$$H_\alpha^\uparrow(S_1^n | \hat{C}_1^n T_1^n \hat{E})_{\rho_{|\Omega}} \geq n h_\alpha^\uparrow - \frac{\alpha}{\alpha-1} \log \frac{1}{\Pr[\Omega]},$$

where

$$h_\alpha^\uparrow = \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} \left(\frac{\alpha}{\alpha-1} D(\mathbf{q}||\nu_{\hat{C}}) + \sum_{\hat{c}} q(\hat{c}) H_\alpha^\uparrow(S | T \tilde{E})_{\nu_{|\hat{c}}} \right), \quad (4)$$

where $\nu_{\hat{C}}$ denotes the probability distribution on the classical register $\hat{C}$ induced by the state $\nu_{\hat{C}}$, and Σ denotes the set of all states of the form $\mathcal{M}[\omega_{\tilde{A}\tilde{B}\tilde{E}}]$ for some initial state $\omega_{\tilde{A}\tilde{B}\tilde{E}}$ satisfying $\omega_{\tilde{A}} = \sigma_{\tilde{A}}$, with $\tilde{E}$ being any register of large enough dimension to purify $\tilde{A}\tilde{B}$.

To apply this result in a protocol, we can basically take Ω as the event that the protocol accepts during the acceptance test. Then, the above theorem lets us bound the Rényi entropy $H_\alpha^\uparrow(S_1^n | \hat{C}_1^n T_1^n \hat{E})_{\rho_{|\Omega}}$ of the overall state in terms of a quantity $h_\alpha^\uparrow$ that can be computed by only analyzing single rounds. Critically, this Rényi entropy of the overall state can be easily used to find the finite-size secret key length that can be obtained from the protocol, according to the Rényi privacy amplification theorem in Ref. [10]. (We give examples of such computations in Secs. VII B and VII C, together with more elaboration for conditioning on other possible protocol steps such as “error verification”).

Furthermore, the single-round quantity $h_\alpha^\uparrow$ can be given an intuitive interpretation. Specifically, let us compare it against a very “simplistic” scenario where the state across the n rounds is independent and identically distributed (IID). In that case, the overall entropy $H_\alpha^\uparrow(S_1^n | \hat{C}_1^n T_1^n \hat{E})$ (ignoring the conditioning on Ω for simplicity) would just be n times the entropy $H_\alpha^\uparrow(S | \hat{C} T \tilde{E})_\nu$ of a state ν in a single round. Furthermore, note that as long as the single-round probability distribution $\nu_{\hat{C}}$ lies in the acceptance set S_Ω , such an IID state would be accepted in the protocol with high probability asymptotically. Given these facts, we cannot expect to obtain a bound on the overall entropy that is much better than n times the value

$$\inf_{\nu \in \Sigma} H_\alpha^\uparrow(S | \hat{C} T \tilde{E})_\nu \quad \text{s.t. } \nu_{\hat{C}} \in S_\Omega, \quad (5)$$

i.e., the smallest single-round entropy over a set of states that would be accepted with high probability asymptotically.

Now, observe that the optimization in Eq. (5) for that “simplistic” scenario only differs from our actual formula

in Eq. (4) for $h_a^\uparrow$ in two ways. First, rather than the “hard” constraint $\nu_{\hat{c}} \in S_\Omega$ in Eq. (5), in the $h_a^\uparrow$ optimization in Eq. (4), we instead basically have a “soft” version of that constraint by allowing $\nu_{\hat{c}}$ to move outside of S_Ω but at the cost of a “penalty” as quantified by $D(\mathbf{q} \parallel \nu_{\hat{c}})$ (with $\mathbf{q} \in S_\Omega$). Second, we have replaced $H_a^\uparrow(S|\hat{C}\hat{T}\hat{E})_\nu$ with a particular linear combination $\sum_{\hat{c}} q(\hat{c})H_a^\uparrow(S|\hat{T}\hat{E})_{\nu_{|\hat{c}}}$, but this change is less important as these quantities are still essentially similar (the latter is just a “reweighted” average of the entropies conditioned on the $\hat{c}$ values).

Hence, $h_a^\uparrow$ can be intuitively understood as a relaxed version of the simplistic optimization in Eq. (5), so $h_a^\uparrow$ should have a somewhat lower value than the latter. Critically, however, Corollary I.1 tells us that this relaxation already *rigorously* accounts for all finite-size and non-IID effects in the protocol. Therefore, once the set S_Ω in the accept condition is specified, the QKD security proof basically only needs to focus on evaluating the specific relaxed optimization in $h_a^\uparrow$, without needing to further consider any statistical analysis or concentration inequalities as in many previous security proof techniques (or min-tradeoff functions, for entropy accumulation). This method is fairly intuitive to compute finite-size key rates (readers interested in applying this method can now skip directly to Sec. VB for more details regarding practical implementation). Furthermore, it appears to also generally yield better key rates in practice, as we demonstrate with explicit examples in Sec. VII B.

In addition, if there are situations where it is not easy to compute the single-round Rényi entropies, we note that they can be easily lower bounded in terms of the von Neumann entropy that has been extensively studied in previous QKD security proofs; see Eq. (86). Similarly, the overall Rényi entropy $H_a^\uparrow(S_1^n | \hat{C}_1^n T_1^n \hat{E})_{\rho_{|\Omega}}$ can be used to bound the overall smooth min-entropy if desired; see Eq. (87). Hence, our results can be easily reformulated to reproduce bounds similar to Eq. (1) while still entirely avoiding min-tradeoff functions. Note that this approach will introduce some suboptimality compared to using Corollary I.1 in a “fully Rényi” analysis. However, we find that the resulting bounds still appear to be significantly tighter in practice compared to previous entropy accumulation results—in fact, we still often obtain results roughly competitive with the smooth-entropy EUR approach in Refs. [6,7]; see Sec. VII B.

1. MDI and decoy-state protocols

We highlight that this model also suffices for measurement-device-independent (MDI) protocols [27], where Alice and Bob prepare states and send them to an *untrusted* third party Charlie, who measures the states and announces some values. Despite the fact that Charlie is untrusted, one can still apply the above model by observing that this

untrusted measurement can be *equivalently* described by an adversary performing some untrusted quantum operation followed by Charlie performing a completely trusted tensor-product measurement across some registers $\tilde{C}_1^n$; see, e.g., Ref. [28]. With this model, the state produced in the protocol would similarly have the form $\rho_{S_1^n \tilde{C}_1^n T_1^n \hat{E}} = \mathcal{M}^{\otimes n}[\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{C}_1^n \hat{E}}^0]$ for a channel $\mathcal{M}: \tilde{A} \tilde{B} \tilde{C} \rightarrow \hat{S} \hat{C} \hat{T}$ that incorporates Charlie’s (trusted) measurement in that model. Hence, this framework also suffices to analyze MDI protocols in nearly identical fashion to PM protocols. Furthermore, we note that the computation of $h_a^\uparrow$ for decoy-state protocols can be addressed using techniques developed in Sec. 7 of Ref. [11], which evaluated optimizations of a very similar form (just with a different objective function). However, as the implementation details of applying this method to MDI and decoy-state protocols are fairly lengthy, we perform these explicit computations in a separate work.

2. DI protocols

Turning to DI protocols, one cannot only consider states of the form in Eq. (3) since, for instance, the measurements may not be in a tensor product across rounds. However, the original EAT [1,29] and GEAT [4] studied more sophisticated channel structures that are suitable for analyzing a variety of protocols in the DI setting (for instance, QKD, randomness amplification, and randomness expansion, including “blind” protocols that prove security even against an untrusted Bob [4]). In this work, we show that the EAT and GEAT channel structures also suffice to yield bounds of a very similar form to those in Corollary I.1, which we show in detail in Theorem V.1 as well some simplifications in Lemmas V.1–V.2 (these results were obtained independently from Ref. [17]). Hence, these simpler and tighter bounds can be immediately applied to improve the key rates in all circumstances where the EAT and GEAT were previously used, including the aforementioned variety of DI protocols.

To summarize, readers interested in applying our results to fixed-length protocols may skip directly to one of the following key points, which are mostly self-contained apart from some references to background definitions in Sec. III:

- (i) For DI protocols, refer to Sec. VA, in which the “fully Rényi” bound we described above is presented as Theorem V.1, with simpler versions in Lemmas V.1–V.2. Then, in Sec. VB, we give many further details that are helpful for applications.
- (ii) For device-dependent protocols, refer instead to Theorem VI.1 (which is an extension of the core result of Ref. [17]), along with the qualitative discussions in Sec. VB.
- (iii) For explicit bounds of the form Eq. (1), relating smooth min-entropy to von Neumann entropy, refer

to the bounds in Eqs. (88) to (90) for the DI case, and Eq. (128) for the device-dependent case.

More elaborate results, which we do not attempt to summarize in this section, are given as follows: Note that under the GEAT or EAT model, we can also accommodate a form of “time-varying” behavior in fixed-length protocols (similar to Ref. [18]); refer to Corollary IV.1 and the discussion below it. In addition, as mentioned above, Ref. [17] developed a powerful proof framework for variable-length protocols; some steps in our analysis are sufficiently similar to theirs that we could extract analogous results, under the GEAT or EAT model rather than their model. We describe the background concepts for this in Sec. IV, with some key parts given in Theorem IV.1 and Sec. IV C.

B. Structure of the paper

This paper is structured as follows.

- (i) In Sec. II and III, we lay out various preliminary notations and concepts.
- (ii) In Sec. IV, we introduce the concept of a quantum estimation score (QES) system inspired by QEFs and f -weighted Rényi entropies, and present our analog of the QEF bounds under the conditions of the GEAT.
- (iii) In Sec. V, we further simplify these results for applications in fixed-length protocols, including the detailed versions of the bounds in Eqs. (1) and (2) sketched above. We also discuss many points relevant for practical applications.
- (iv) In Sec. VI, we give slightly better bounds under the original EAT Markov conditions or the model in Ref. [17], where the latter also has the advantage of being more suited for analyzing device-dependent PM protocols.
- (v) In Sec. VII, we analyze the tightness of our bounds, including key-rate computations for some example protocols.

- (vi) In Sec. VIII, we conclude by discussing prospects for future work.

Various technical details are deferred to the appendixes; however, we highlight Appendix E, in particular, in which we discuss how to modify these results to instead obtain upper bounds on the $\alpha < 1$ Rényi entropies, or smooth max-entropy.

II. PRELIMINARIES

We list some basic notation in Table I. In addition, we need to use some other concepts, which we define below and briefly elaborate on in some cases. In this work, we assume that all systems are finite dimensional, but we do not impose any bounds on the system dimensions unless otherwise specified. All entropies are defined in base 2. For a channel $\mathcal{E}$ from register Q to register Q' , we often write the abbreviated notation

$$\mathcal{E}: Q \rightarrow Q', \quad (6)$$

rather than writing out the formal statement of it being a completely positive trace preserving. linear map $\mathcal{E}: \text{End}(\mathcal{H}_Q) \rightarrow \text{End}(\mathcal{H}_{Q'})$ [where $\text{End}(\mathcal{H}_Q)$ is the set of linear operators on the Hilbert space $\mathcal{H}_Q$]. In addition, throughout this work, we often leave tensor products with identity channels implicit; e.g., given a channel $\mathcal{E}: Q \rightarrow Q'$, we often use the compact notation

$$\mathcal{E}[\rho_{QR}] := (\mathcal{E} \otimes \text{id}_R)[\rho_{QR}]. \quad (7)$$

Definition II.1. (Frequency distributions) For a string $z_1^n \in \mathcal{Z}^n$ on some alphabet $\mathcal{Z}$, $\text{freq}_{z_1^n}$ denotes the following probability distribution on $\mathcal{Z}$:

$$\text{freq}_{z_1^n}(z) := \frac{\text{number of occurrences of } z \text{ in } z_1^n}{n}. \quad (8)$$

TABLE I. List of notations.

Symbol	Definition
$\log$	Base-2 logarithm
H	Base-2 von Neumann entropy
h_{bin}	Binary entropy: $h_{\text{bin}} := -x \log x - (1-x) \log(1-x)$
$\mathbb{R} \cup \{-\infty, +\infty\}$	Extended real line
$\lfloor \cdot \rfloor$ (respectively, $\lceil \cdot \rceil$)	Floor (respectively, ceiling) function
$\ \cdot \ _p$	Schatten p -norm
$ \cdot $	Absolute value of operator; $ M = \sqrt{M^\dagger M}$.
$A \perp B$	A and B are orthogonal; $AB = BA = 0$.
$X \geq Y$ (respectively, $X > Y$)	$X - Y$ is positive semidefinite (respectively, positive definite).
$\text{Pos}(A)$	Set of positive-semidefinite operators on register A
$\mathbf{S}_=(A)$ [respectively, $\mathbf{S}_\leq(A)$]	Set of normalized (respectively, subnormalized) states on register A
$\mathbb{U}_A$	Maximally mixed state on register A
A_j^k	Registers $A_j \dots A_k$

Definition II.2. A state $\rho \in \mathcal{S}_{\leq}(CQ)$ is said to be classical on C (with respect to a specified basis on C) if it is in the form

$$\rho_{CQ} = \sum_c \lambda_c |c\rangle\langle c| \otimes \sigma_c, \quad (9)$$

for some normalized states $\sigma_c \in \mathcal{S}_{\leq}(Q)$ and weights $\lambda_c \geq 0$, with $|c\rangle$ being the specified basis states on C . In most circumstances, we will not explicitly specify this “classical basis” of C , leaving it to be implicitly defined by context. It may be convenient to absorb the weights λ_c into the states σ_c , writing them as subnormalized states $\omega_c = \lambda_c \sigma_c \in \mathcal{S}_{\leq}(Q)$ instead.

Definition II.3 (Conditioning on classical events) For a state $\rho \in \mathcal{S}_{\leq}(CQ)$ classical on C , written in the form $\rho_{CQ} = \sum_c |c\rangle\langle c| \otimes \omega_c$ for some $\omega_c \in \mathcal{S}_{\leq}(Q)$, and an event Ω defined on the register C , we will define a corresponding partial state and conditional state as, respectively,

$$\begin{aligned} \rho_{\wedge \Omega} &:= \sum_{c \in \Omega} |c\rangle\langle c| \otimes \omega_c, \\ \rho_{|\Omega} &:= \frac{\text{Tr}[\rho]}{\text{Tr}[\rho_{\wedge \Omega}]} \rho_{\wedge \Omega} = \frac{\sum_{c \in \Omega} \text{Tr}[\omega_c]}{\sum_{c \in \Omega} \text{Tr}[\omega_c]} \rho_{\wedge \Omega}. \end{aligned} \quad (10)$$

The process of taking partial states is commutative and “associative,” in the sense that for any events Ω, Ω' , we have $(\rho_{\wedge \Omega})_{\wedge \Omega'} = (\rho_{\wedge \Omega'})_{\wedge \Omega} = \rho_{\wedge (\Omega \wedge \Omega')}$; hence, for brevity, we denote all of these expressions as

$$\rho_{\wedge \Omega \wedge \Omega'} := (\rho_{\wedge \Omega})_{\wedge \Omega'} = (\rho_{\wedge \Omega'})_{\wedge \Omega} = \rho_{\wedge (\Omega \wedge \Omega')}. \quad (11)$$

On the other hand, some disambiguating parentheses are needed when combined with taking conditional states (due to the normalization factors).

In light of the preceding two definitions, for a normalized state $\rho \in \mathcal{S}_{\leq}(CQ)$ that is classical on C , it is reasonable to write it in the form

$$\rho_{CQ} = \sum_c \rho(c) |c\rangle\langle c| \otimes \rho_{Q|c}, \quad (12)$$

where $\rho(c)$ denotes the probability of $C = c$ according to ρ , and $\rho_{Q|c}$ can indeed be interpreted as the conditional state on Q corresponding to $C = c$, i.e., $\rho_{Q|c} = \text{Tr}_C[\rho_{|\Omega}]$, where Ω is the event $C = c$. We may sometimes denote the distribution on C induced by ρ as the tuple

$$\rho_C := (\rho(1), \rho(2), \dots). \quad (13)$$

Definition II.4. (Measure-and-prepare or read-and-prepare channels) A (projective) measure-and-prepare channel is a channel $\mathcal{E}: Q \rightarrow QQ'$ of the form

$$\mathcal{E}[\rho_Q] = \sum_j (P_j \rho_Q P_j) \otimes \sigma_{Q'|j}, \quad (14)$$

for some projective measurement $\{P_j\}$ on Q and some normalized states $\sigma_{Q'|j}$. If Q is classical and the measurement is

a projective measurement in its classical basis, we refer to it as a read-and-prepare channel. Note that a read-and-prepare channel always simply extends the state “without disturbing it”; i.e., tracing out Q' results in the original state again.

The following definitions of Rényi divergences and entropies are reproduced from Ref. [30] and coincide with those in Refs. [1,2,4] for normalized states.

Definition II.5. (Rényi divergence) For any $\rho, \sigma \in \text{Pos}(A)$ with $\text{Tr}[\rho] \neq 0$, and $\alpha \in (0, 1) \cup (1, \infty)$, the (sandwiched) Rényi divergence between ρ and σ is defined as

$$D_{\alpha}(\rho \| \sigma) = \frac{1}{\alpha - 1} \log \frac{\text{Tr}[(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha}]}{\text{Tr}[\rho]}, \quad (15)$$

for $(\alpha < 1 \wedge \rho \not\subseteq \sigma)$ or $(\text{supp}(\rho) \subseteq \text{supp}(\sigma))$. Otherwise, we set $D_{\alpha}(\rho \| \sigma) = \infty$. For $\alpha > 1$, the $\sigma^{\frac{1-\alpha}{2\alpha}}$ terms are defined via the Moore-Penrose pseudoinverse if σ is not full support [30]. The above definition is extended to $\alpha \in \{0, 1, \infty\}$ by taking the respective limits. For the $\alpha = 1$ case, it reduces to the Umegaki divergence:

$$D(\rho \| \sigma) = \begin{cases} \frac{\text{Tr}[\rho \log \rho - \rho \log \sigma]}{\text{Tr}[\rho]} & \text{supp}(\rho) \subseteq \text{supp}(\sigma) \\ +\infty & \text{otherwise.} \end{cases} \quad (16)$$

For any two classical probability distributions $\mathbf{p}$ and $\mathbf{q}$ on a common alphabet, we also define the Rényi divergence $D_{\alpha}(\mathbf{p} \| \mathbf{q})$ analogously, e.g., by viewing the distributions as diagonal density matrices in the above formulas; in the $\alpha = 1$ case, this gives the Kullback-Leibler (KL) divergence.

Definition II.6 (Rényi entropies) For any bipartite state $\rho \in \mathcal{S}_{\leq}(AB)$, and $\alpha \in [0, \infty]$, we define the following two (sandwiched) Rényi conditional entropies:

$$\begin{aligned} H_{\alpha}(A|B)_{\rho} &= -D_{\alpha}(\rho_{AB} \| \mathbb{I}_A \otimes \rho_B), \\ H_{\alpha}^{\uparrow}(A|B)_{\rho} &= \sup_{\sigma_B \in \mathcal{S}_{\leq}(B)} -D_{\alpha}(\rho_{AB} \| \mathbb{I}_A \otimes \sigma_B). \end{aligned} \quad (17)$$

For $\alpha = 1$, both the above values coincide and are equal to the von Neumann entropy.

While we will not explicitly use the following definitions of min- and max-entropies (for subnormalized states) anywhere in our proofs, we state them here to ensure consistency with previous work such as Ref. [1].

Definition II.7. For $\rho \in \mathcal{S}_{\leq}(AB)$ with $\text{Tr}[\rho] \neq 0$, the min- and max-entropies of A conditioned on B are

$$H_{\min}(A|B)_{\rho} := -\log \min_{\substack{\sigma \in \mathcal{S}_{\leq}(B) \text{ s.t.} \\ \ker(\rho_B) \subseteq \ker(\sigma_B)}} \|\rho_{AB}^{\frac{1}{2}} \sigma_B^{-\frac{1}{2}}\|_{\infty}^2, \quad (18)$$

$$H_{\max}(A|B)_{\rho} := \log \max_{\sigma \in \mathcal{S}_{\leq}(B)} \|\rho_{AB}^{\frac{1}{2}} \sigma_B^{\frac{1}{2}}\|_1^2, \quad (19)$$

where, in the first equation, the $\sigma_B^{-\frac{1}{2}}$ term should be understood in terms of the Moore-Penrose generalized

inverse. In both equations, the optimum is indeed attained (see, e.g., Secs. 6.1.2 and 6.1.3 of Ref. [30]), and it can be attained by a normalized state; thus, $S_{\leq}(B)$ can be replaced by $S_{=}(B)$ without loss of generality. When $\text{Tr}[\rho] = 1$, these definitions coincide with the Rényi entropies $H_{\infty}^{\dagger}$ and $H_{1/2}^{\dagger}$ defined above.

Additionally, for $\varepsilon \in [0, \sqrt{\text{Tr}[\rho_{AB}]})$, the ε -smoothed min- and max-entropies of A conditioned on B are

$$\begin{aligned} H_{\min}^{\varepsilon}(A|B)_{\rho} &:= \max_{\substack{\tilde{\rho} \in S_{\leq}(AB) \text{ s.t.} \\ P(\tilde{\rho}, \rho) \leq \varepsilon}} H_{\min}(A|B)_{\tilde{\rho}}, \\ H_{\max}^{\varepsilon}(A|B)_{\rho} &:= \min_{\substack{\tilde{\rho} \in S_{\leq}(AB) \text{ s.t.} \\ P(\tilde{\rho}, \rho) \leq \varepsilon}} H_{\max}(A|B)_{\tilde{\rho}}, \end{aligned} \quad (20)$$

where P denotes purified distance as defined in Ref. [30].

We now also list some useful properties we will use throughout our work.

Fact II.1 (Data processing, Theorem 1 of Ref. [31]; see also Refs. [30, 32–34]) For any $\alpha \in [1/2, \infty]$, any $\rho, \sigma \in \text{Pos}(Q)$ with $\text{Tr}[\rho] \neq 0$, and any channel $\mathcal{E}: Q \rightarrow Q'$, we have

$$D_{\alpha}(\rho||\sigma) \geq D_{\alpha}(\mathcal{E}[\rho]||\mathcal{E}[\sigma]), \quad (21)$$

and thus also for any $\rho \in S_{=}(Q''Q)$,

$$\begin{aligned} H_{\alpha}(Q''|Q)_{\rho} &\leq H_{\alpha}(Q''|Q')_{\mathcal{E}[\rho]}, \\ H_{\alpha}^{\dagger}(Q''|Q)_{\rho} &\leq H_{\alpha}^{\dagger}(Q''|Q')_{\mathcal{E}[\rho]}. \end{aligned} \quad (22)$$

If $\mathcal{E}$ is an isometry, all the above bounds hold with equality.

Fact II.2 (Conditioning on classical registers; see Sec. III. B. 2 and Proposition 9 of Ref. [32] or Eq. (5.32) and Proposition 5.1 of Ref. [30]) Let $\rho, \sigma \in S_{=}(CQ)$ be states classical on C . Then, for $\alpha \in (0, 1) \cup (1, \infty)$,

$$D_{\alpha}(\rho||\sigma) = \frac{1}{\alpha - 1} \log \left(\sum_c \rho(c)^{\alpha} \sigma(c)^{1-\alpha} 2^{(\alpha-1)D_{\alpha}(\rho_{Q|c}||\sigma_{Q|c})} \right), \quad (23)$$

and hence for a state $\rho \in S_{=}(CQQ')$ classical on C , and any $\alpha \in (0, 1) \cup (1, \infty)$,

$$H_{\alpha}(Q|CQ') = \frac{1}{1-\alpha} \log \left(\sum_c \rho(c) 2^{(1-\alpha)H_{\alpha}(Q|Q')_{\rho|c}} \right), \quad (24)$$

and for any $\alpha \in [1/2, 1) \cup (1, \infty)$,

$$H_{\alpha}^{\dagger}(Q|CQ') = \frac{\alpha}{1-\alpha} \log \left(\sum_c \rho(c) 2^{\frac{1-\alpha}{\alpha} H_{\alpha}^{\dagger}(Q|Q')_{\rho|c}} \right). \quad (25)$$

III. GEAT CHANNELS

In this section, we briefly introduce the sequences of channels that we will be focusing on in this work, essentially following the definitions in Ref. [4].

Definition III.1. $\{\mathcal{N}_j\}_{j=1}^n$ is called a sequence of GEAT channels if each $\mathcal{N}_j$ is a channel $R_{j-1}E_{j-1} \rightarrow S_j R_j E_j$ satisfying the following nonsignaling (NS) condition:

$$\begin{aligned} \exists \text{ a channel } \mathcal{R}_j: E_{j-1} &\rightarrow E_j \text{ such that} \\ \text{Tr}_{S_j R_j} \circ \mathcal{N}_j &= \mathcal{R}_j \circ \text{Tr}_{R_{j-1}}. \end{aligned} \quad (26)$$

If a state $\rho \in S_{=}(S_1^{\dagger} \tilde{C}_1^{\dagger} \hat{C}_1^{\dagger} E_n R_n)$ is of the form $\rho = \mathcal{N}_n \circ \dots \circ \mathcal{N}_1[\omega^0]$ (leaving some identity channels implicit) for some initial state $\omega^0 \in S_{=}(R_0 E_0)$, we say it is generated by the sequence of GEAT channels $\{\mathcal{N}_j\}_{j=1}^n$.

Qualitatively, S_j can be understood as (possibly quantum) registers that will be kept secret, E_j represents some side information that can be updated by each GEAT channel, and R_j represents memory passed between the channels without being available as side information. The NS condition serves to ensure that information is not “signaled” from the memory registers to the side information, in the sense that if we consider the term $\mathcal{R}_j \circ \text{Tr}_{R_{j-1}}$ on the right-hand side, it is a channel that outputs the “correct” reduced state on E_j (namely, the state produced by $\text{Tr}_{S_j R_j} \circ \mathcal{N}_j$) despite first tracing out R_{j-1} .

The above definition of GEAT channels is enough for entropy to “accumulate” in a certain sense; specifically, a key result of Ref. [4] is the following bound:

Fact III.1. (Reference [4]) Let ρ be a state generated by a sequence of GEAT channels $\{\mathcal{N}_j\}_{j=1}^n$ (Definition III.1). Take any $\alpha \in (1, 2)$, and let $\hat{\alpha} = 1/(2 - \alpha)$. Then, we have

$$H_{\alpha}(S_1^n | E_n)_{\rho} \geq \sum_j \inf_{\nu \in \Sigma_j} H_{\hat{\alpha}}(S_j | E_j \tilde{E})_{\nu}, \quad (27)$$

where Σ_j denotes the set of all states of the form $\mathcal{N}_j[\omega_{R_{j-1}E_{j-1}\tilde{E}}]$ for some initial state $\omega \in S_{=}(R_{j-1}E_{j-1}\tilde{E})$, with $\tilde{E}$ being a register of large enough dimension to serve as a purifying register for any of the $R_j E_j$ registers.

However, as mentioned in the Introduction, the main drawback of the above result is that there is no restriction on the set of states in the infimum (other than the fact that they are possible output states of $\mathcal{N}_j$), and hence it is not obvious how this result can be applied in security proofs. To overcome this drawback, one introduces a notion of GEAT with “testing”:

Definition III.2. $\{\mathcal{M}_j\}_{j=1}^n$ is called a sequence of GEAT-with-testing (GEATT) channels if each $\mathcal{M}_j$ is a channel $R_{j-1}E_{j-1} \rightarrow S_j R_j E_j \tilde{C}_j \hat{C}_j$ such that the output registers $\tilde{C}_j \hat{C}_j$ are always classical (for any input state), and it satisfies the following NS condition:

$$\begin{aligned} \exists \text{ a channel } \mathcal{R}_j: E_{j-1} &\rightarrow E_j \hat{C}_j \text{ such that} \\ \text{Tr}_{S_j \tilde{C}_j R_j} \circ \mathcal{M}_j &= \mathcal{R}_j \circ \text{Tr}_{R_{j-1}}. \end{aligned} \quad (28)$$

If a state $\rho \in S_=(S_1^n \bar{C}_1^n \hat{C}_1^n E_n R_n)$ is of the form $\rho = \mathcal{M}_n \circ \dots \circ \mathcal{M}_1[\omega^0]$ (leaving some identity channels implicit) for some initial state $\omega^0 \in S_=(R_0 E_0)$, we say it is generated by the sequence of GEATT channels $\{\mathcal{M}_j\}_{j=1}^n$.

Qualitatively, the classical registers $\bar{C}_j$ and $\hat{C}_j$, respectively, contain secret and public information that will be used to estimate the accumulated entropy. It was shown in Theorem 4.3 of Ref. [4] that this roughly allows one to restrict the states considered in the infimum, at the price of various $O(\sqrt{n})$ corrections—our goal in this work will be to obtain a similar result but with a simpler formulation and better finite-size performance. Note that, in many applications, it is possible to take one of the registers $\bar{C}_j$ and $\hat{C}_j$ to be trivial—for instance, in device-dependent security proofs as described in Ref. [21], it is usually possible to put all the “test-round data” in the public registers $\hat{C}_j$, so the secret registers $\bar{C}_j$ can be trivial [35]. On the other hand, for device-independent security proofs, the test-round data do not usually satisfy the NS conditions, and hence one has to model them first using the secret registers $\bar{C}_j$ instead and then use chain rules to “move” them into the conditioning registers in the case of DIQKD; see Refs. [29,36,37] (or Remark VIII.1). Note that the definition of GEATT channels we have presented here is subtly different from Ref. [4]; for readers already familiar with that work, we highlight the differences in Appendix A, though we believe there should be no significant differences in applications.

When studying GEAT or GEATT channels, one often has to consider purifications or extensions of the input states to the channels (for instance, the registers $\tilde{E}$ in Fact III.1). In much of our analysis, it will be convenient to have compact notation for taking some arbitrary purification of an input state to the channel. We therefore introduce the following terminology:

Definition III.3. For registers Q and Q' with $\dim(Q) \leq \dim(Q')$, a purifying function for Q onto Q' is a function $\text{Pur}: S_=(Q) \rightarrow S_=(QQ')$ such that, for any state ρ_Q , the state $\text{Pur}(\rho_Q)$ is a purification of ρ_Q onto the register Q' , i.e., a (possibly subnormalized) rank-1 operator such that $\text{Tr}_{Q'}[\text{Pur}(\rho_Q)] = \rho_Q$.

Note that a purifying function is *not* a channel (i.e., completely positive trace preserving. map), for instance, because it is necessarily nonlinear. As a concrete example, one can choose, for example, the function

$$\text{Pur}(\rho_Q) = \dim(Q)(\sqrt{\rho_Q} \otimes \mathbb{I}_{Q'})|\Phi^+\rangle\langle\Phi^+|(\sqrt{\rho_Q} \otimes \mathbb{I}_{Q'}), \quad (29)$$

where $|\Phi^+\rangle$ is some normalized maximally entangled state across QQ' (up to the support of Q) in some arbitrary basis. However, all results we present in this work should be basically independent of any choice of purifying function by exploiting the isometric equivalence of purifications.

IV. DERIVING QEF-TYPE BOUNDS FROM THE GEAT

In this section, we show how to derive bounds very similar to the QEF framework but under the conditions of the GEAT instead.

A. Quantum estimation score systems

We begin by presenting a slight variant of the QEF concept, which we refer to as a “quantum estimation score-system” (QES)—while this is nearly identical to a QEF, we find it convenient to formulate the definition in a slightly different way, hence we coin a similar but slightly different term for it to avoid ambiguity. QES-s are also closely connected to the concept of tradeoff functions defined in Ref. [17], where they use this concept to develop a notion of f -weighted Rényi entropies, which we base our following definition on. However, we choose to use H_α as the basis of our definition for most of our work due to some technical points; their definition uses $H_\alpha^\uparrow$, and our definition also slightly differs in some other respects. Moreover, there also exist potential generalizations of those concepts, e.g., to Petz entropies as noted in Ref. [18]. We defer further discussion of these points to Remark IV.1, after first establishing some helpful properties.

Definition IV.1. (H_α^f entropies) Let $\rho \in S_=(\bar{C} \hat{C} QQ')$ be a state where $\bar{C}$ and $\hat{C}$ are classical with alphabets $\bar{\mathcal{C}}$ and $\hat{\mathcal{C}}$, respectively. A QES on $\bar{C} \hat{C}$ is simply a function $f: \bar{\mathcal{C}} \times \hat{\mathcal{C}} \rightarrow \mathbb{R}$; equivalently, we may denote it as a real-valued tuple $\mathbf{f} \in \mathbb{R}^{|\bar{\mathcal{C}} \times \hat{\mathcal{C}}|}$, where each term in the tuple specifies the value $f(\bar{c} \hat{c})$. Given a QES f and a value [38] $\alpha \in (0, 1) \cup (1, \infty)$, we define

$$\begin{aligned} H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho &:= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c} \hat{c}} \rho(\bar{c} \hat{c})^\alpha \rho(\hat{c})^{1-\alpha} 2^{(1-\alpha)(-f(\bar{c} \hat{c}) - D_\alpha(\rho_{Q\bar{C}|\hat{c}} \|\mathbb{I}_Q \otimes \rho_{Q'|\hat{c}}))} \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c} \hat{c}} \rho(\bar{c} \hat{c}) 2^{(1-\alpha)(-f(\bar{c} \hat{c}) - D_\alpha(\rho_{Q\bar{C}|\hat{c}} \|\mathbb{I}_Q \otimes \rho_{Q'|\hat{c}}))} \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c} \hat{c}} 2^{-(1-\alpha)f(\bar{c} \hat{c})} \text{Tr}[(\rho_{Q'|\hat{c}})^{\frac{1-\alpha}{2\alpha}} \rho_{Q\bar{C}|\hat{c}} (\rho_{Q'|\hat{c}})^{\frac{1-\alpha}{2\alpha}}]^\alpha \right), \end{aligned} \quad (30)$$

where the sum is over all $\bar{c}\hat{c}$ values such that $\rho(\bar{c}\hat{c}) > 0$, and we leave some tensor factors of identity implicit in the last expression. We may variously refer to this quantity as a H_α^f entropy or (when there is no danger of confusion with the version in Definition VI.1) an f -weighted Rényi entropy, or simply an f -weighted entropy [39].

In the above, the restriction of the summation domain is just to avoid technical problems in defining the $D_\alpha(\rho_{Q\bar{Q}'\wedge\bar{c}\hat{c}}\|\mathbb{I}_Q \otimes \rho_{Q'\wedge\hat{c}})$ terms when $\rho(\bar{c}\hat{c}) = 0$. (In principle, we could assign arbitrary finite values to such terms without changing the value of the sum, but this approach introduces some technical complications in our Sec. V analysis; see Remark V.1.) With this convention, all terms that appear in the sum are well defined and finite because, for all such terms, we have $\text{Tr}[\rho_{Q\bar{Q}'\wedge\bar{c}\hat{c}}] > 0$ and

$$\text{supp}(\rho_{Q\bar{Q}'\wedge\bar{c}\hat{c}}) \subseteq \text{supp}(\rho_{Q\bar{Q}'\wedge\hat{c}}) \subseteq \text{supp}(\mathbb{I}_Q \otimes \rho_{Q'\wedge\hat{c}}), \quad (31)$$

and similarly for the normalized conditional states; hence, the condition for finiteness in Eq. (15) is satisfied.

To gain some intuition about the definition, note that if the $\bar{C}$ register is trivial, it reduces to

$$H_\alpha^f(Q|\hat{C}Q')_\rho = \frac{1}{1-\alpha} \log \left(\sum_{\hat{c}} \rho(\hat{c}) 2^{(1-\alpha)(H_\alpha(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{c}))} \right), \quad (32)$$

so it has almost the same form as the summations that appear in Fact II.2 regarding Rényi entropies, except that each $H_\alpha(Q|Q')_{\rho_{|\hat{c}}}$ term is shifted by the corresponding QES value $f(\hat{c})$. In particular, if we choose the QES to be simply the constant function $f(\hat{c}) = 0$, then $H_\alpha^f(Q|\hat{C}Q')_\rho$ is exactly equal to the standard Rényi entropy $H_\alpha(Q|\hat{C}Q')_\rho$. Apart from this “entropic” interpretation (which we expand on in Lemmas IV.1 and IV.2 below), we can also discuss a “statistical” interpretation. Suppose, loosely speaking, that we want the QES values $f(\hat{c})$ to be lower bounds on the entropies $H_\alpha(Q|Q')_{\rho_{|\hat{c}}}$ of the conditional states in some “averaged” sense over $\hat{c}$ [hence our choice of terminology: we want to view $f(\hat{c})$ as a “score” assigned to each $\hat{c}$ value, which bounds $H_\alpha(Q|Q')_{\rho_{|\hat{c}}}$ in some qualitative sense]. Most directly, we could impose such a condition by considering the usual notion of expected or mean value, $\mathbb{E}_{P_X}[g(X)] := \sum_x P_X(x)g(x)$ (for some function g of a random variable X with distribution P_X) and requiring that $\mathbb{E}_{\rho_{\hat{c}}}[H_\alpha(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{c})] \geq 0$. However, it turns out that the quantity $\mathbb{E}_{\rho_{\hat{c}}}[H_\alpha(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{c})]$ seems difficult to analyze with the techniques used in this work. Instead, suppose one modifies the usual notion of mean value to a notion of “log-mean-exponential” value, sometimes also known as the exponential mean [with respect to any base $b \in (0, \infty)$]:

$$\text{lme}_b[g(X)] := \log_b \left(\sum_x P_X(x) b^{g(x)} \right), \quad (33)$$

similarly to how the log-sum-exponential function (see, e.g., Ref. [26]) is a modified notion of a standard sum. Then, we see that Eq. (32) can be rewritten as

$$H_\alpha^f(Q|\hat{C}Q')_\rho = \text{lme}_{\rho_{\hat{c}}}[H_\alpha(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{C})], \quad (34)$$

where $b = 2^{1-\alpha} \in (0, \infty)$, which implies, for instance, that a statement such as $H_\alpha^f(Q|\hat{C}Q')_\rho \geq 0$ is precisely the statement that $\text{lme}_{\rho_{\hat{c}}}[H_\alpha(Q|Q')_{\rho_{|\hat{c}}} - f(\hat{C})] \geq 0$; i.e., $f(\hat{C})$ lower bounds the conditional entropies $H_\alpha(Q|Q')_{\rho_{|\hat{c}}}$ in a log-mean-exponential sense rather than the usual mean sense. Our approach in this work is to simultaneously exploit the “entropic” interpretation of $H_\alpha^f(Q|\hat{C}Q')_\rho$ to analyze such statements.

Thus, we see that imposing a condition $H_\alpha^f(Q|\hat{C}Q')_\rho \geq 0$ in single protocol rounds would be roughly a condition that the QES f defines a Rényi version of a min-tradeoff function as defined in the original EAT or GEAT, except that it involves a log-mean-exponential value instead of the usual mean—analogueous observations were made in Refs. [17,18]. We remark, however, that for the approach in this work, we find it is often more flexible to first analyze QESs without imposing the condition $H_\alpha^f(Q|\hat{C}Q')_\rho \geq 0$ and then perform a “normalization” argument at the end (see Lemma IV.7) to obtain that property. Analogously, a condition that $H_\alpha^f(Q|\hat{C}Q')_\rho \leq 0$ is basically the statement that $f(\hat{C})$ upper bounds the conditional entropies $H_\alpha(Q|Q')_{\rho_{|\hat{c}}}$ in a log-mean-exponential sense, so it is related to the notion of a max-tradeoff function in the original EAT.

Another way to gain some intuition is to use the following property (based on a construction in Refs. [1,2]): The idea is to construct a new register D that “encodes the value of $f(\bar{C}\hat{C})$ ” via its entropy, in some sense.

Lemma IV.1. Let f be a QES on some classical registers $\bar{C}\hat{C}$, let $M \in \mathbb{R}$ be any value such that $M - f(\bar{c}\hat{c}) > 0$ for all $\bar{c}\hat{c}$, and take any $\alpha \in (0, 1) \cup (1, \infty)$. Consider any read-and-prepare channel $\bar{C}\hat{C} \rightarrow \bar{C}\hat{C}D$ such that the state it prepares on D always satisfies

$$H_\alpha(D)_{\rho_{|\bar{c}\hat{c}}} = H_\alpha^\dagger(D)_{\rho_{|\bar{c}\hat{c}}} = M - f(\bar{c}\hat{c}). \quad (35)$$

(It is always possible to construct such a channel, and to construct it such that D is classical.) Then, for any $\rho \in \mathcal{S}_=(\bar{C}\hat{C}QQ')$ classical on $\bar{C}\hat{C}$, extending ρ with this channel yields [40]

$$H_\alpha(DQ\bar{C}|\hat{C}Q')_\rho = M + H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho. \quad (36)$$

Proof. First, we briefly verify that such channels can indeed be constructed: Note that for any $\alpha > 0$ and $h > 0$, given a register D with dimension of at least 2^h , one can straightforwardly construct a state on D with $H_\alpha(D) = H_\alpha^\uparrow(D) = h$ (the first equality holds simply because $H_\alpha = H_\alpha^\uparrow$ when there is no conditioning system), e.g., by taking a mixture between some pure state on D and the maximally mixed state; furthermore, this

result can clearly be achieved using a classical D . Therefore, to obtain a read-and-prepare channel satisfying Eq. (35), we simply need to read the classical value $\bar{c}\hat{c}$ and prepare a state on D with the corresponding desired entropy value.

We now show that such a read-and-prepare channel indeed achieves Eq. (36) (using $\mathbb{U}$ to denote maximally mixed states):

$$\begin{aligned}
H_\alpha(DQ\bar{C}|\hat{C}Q')_\rho &= \log(d_D d_Q d_{\bar{C}}) - D_\alpha(\rho_{DQ\bar{C}\hat{C}Q'} \| \mathbb{U}_{DQ\bar{C}} \otimes \rho_{\hat{C}Q'}) \\
&= \log(d_D d_Q d_{\bar{C}}) - D_\alpha\left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c}) |\bar{c}\hat{c}\rangle \langle \bar{c}\hat{c}|_{\bar{C}\hat{C}} \otimes \rho_{DQQ'|\bar{c}\hat{c}} \| \sum_{\bar{c}\hat{c}} \frac{\rho(\hat{c})}{d_{\bar{C}}} |\bar{c}\hat{c}\rangle \langle \bar{c}\hat{c}|_{\bar{C}\hat{C}} \otimes \mathbb{U}_{DQ} \otimes \sigma_{Q'|\hat{c}}\right) \\
&= \log(d_D d_Q d_{\bar{C}}) - \frac{1}{\alpha-1} \log\left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c})^\alpha \left(\frac{\rho(\hat{c})}{d_{\bar{C}}}\right)^{1-\alpha} 2^{(\alpha-1)D_\alpha(\rho_{DQQ'|\bar{c}\hat{c}} \| \mathbb{U}_{DQ} \otimes \rho_{Q'|\hat{c}})}\right) \\
&= \log(d_D d_Q d_{\bar{C}}) - \frac{1}{\alpha-1} \log\left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c})^\alpha \left(\frac{\rho(\hat{c})}{d_{\bar{C}}}\right)^{1-\alpha} 2^{(\alpha-1)(D_\alpha(\rho_{D|\bar{c}\hat{c}} \| \mathbb{U}_D) + D_\alpha(\rho_{QQ'|\bar{c}\hat{c}} \| \mathbb{U}_Q \otimes \rho_{Q'|\hat{c}}))}\right) \\
&= -\frac{1}{\alpha-1} \log\left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c})^\alpha \rho(\hat{c})^{1-\alpha} 2^{(\alpha-1)(-H_\alpha(D)_{\rho_{|\bar{c}\hat{c}}} + D_\alpha(\rho_{QQ'|\bar{c}\hat{c}} \| \mathbb{U}_Q \otimes \rho_{Q'|\hat{c}}))}\right) \\
&= \frac{1}{1-\alpha} \log\left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c})^\alpha \rho(\hat{c})^{1-\alpha} 2^{(1-\alpha)(M-f(\bar{c}\hat{c})-D_\alpha(\rho_{QQ'|\bar{c}\hat{c}} \| \mathbb{U}_Q \otimes \rho_{Q'|\hat{c}}))}\right) \\
&= M + \frac{1}{1-\alpha} \log\left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c})^\alpha \rho(\hat{c})^{1-\alpha} 2^{(1-\alpha)(-f(\bar{c}\hat{c})-D_\alpha(\rho_{QQ'|\bar{c}\hat{c}} \| \mathbb{U}_Q \otimes \rho_{Q'|\hat{c}}))}\right) \\
&= M + H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho,
\end{aligned} \tag{37}$$

where the third line holds by Fact II.2, the fourth holds because $\rho_{DQQ'|\bar{c}\hat{c}} = \rho_{D|\bar{c}\hat{c}} \otimes \rho_{QQ'|\bar{c}\hat{c}}$, and the sixth line follows by substitution from Eq. (35). ■

This lemma implies that an f -weighted entropy is in fact just the usual Rényi conditional entropy evaluated on some extension of the state (and the extension can be produced using the same channel for all states), apart from an additive term M that does not affect any important properties [41]. In particular, this implies that it immediately inherits many properties of the corresponding Rényi conditional entropy,

which we describe later. Before doing so, we present a minor variation of the above result, in which we obtain an approximate version of the relation in Eq. (36) for *all* Rényi parameters simultaneously:

Lemma IV.2. Let f be a QES on some classical registers $\bar{C}\hat{C}$, and let $M > 0$ be any value such that $M - f(\bar{c}\hat{c}) > M/2 > 0$ for all $\bar{c}\hat{c}$. Consider any read-and-prepare channel $\bar{C}\hat{C} \rightarrow \bar{C}\hat{C}D$ such that the state it prepares on D always satisfies

$$H_\alpha(D)_{\rho_{|\bar{c}\hat{c}}} = H_\alpha^\uparrow(D)_{\rho_{|\bar{c}\hat{c}}} \in [M - f(\bar{c}\hat{c}), M - f(\bar{c}\hat{c}) + 2^{-\frac{M}{2}} \log e] \tag{38}$$

for any $\alpha \in [0, \infty]$.

(It is always possible to construct such a channel, and to construct it such that D is classical.) Then, for any $\rho \in \mathcal{S}_=(\bar{C}\hat{C}Q\bar{C}Q')$ classical on $\bar{C}\hat{C}$, extending ρ with this channel yields

$$\begin{aligned}
\forall \alpha \in (0, 1) \cup (1, \infty), \\
M + H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho &\leq H_\alpha(DQ\bar{C}|\hat{C}Q')_\rho \\
&\leq M + 2^{-\frac{M}{2}} \log e + H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho.
\end{aligned} \tag{39}$$

Proof. To see that such channels indeed exist, simply consider a read-and-prepare channel that reads the classical value $\bar{c} \hat{c}$ and prepares a state on D that is a *uniform* mixture with support size $\lceil 2^{M-f(\bar{c} \hat{c})} \rceil$ (this is sometimes called a flat state); again, this result can clearly be achieved with D classical. Since all (unconditioned) Rényi entropies take the same value for a uniform distribution, we see that for *every* $\alpha \in [0, \infty]$, the state prepared on D has Rényi entropy

$$H_\alpha(D)_{\rho_{|\bar{c}\hat{c}}} = H_\alpha^\uparrow(D)_{\rho_{|\bar{c}\hat{c}}} = \log(\lceil 2^{M-f(\bar{c} \hat{c})} \rceil), \quad (40)$$

which lies within the interval described in Eq. (38)—the upper bound holds from observing that

$$\begin{aligned} & \log(\lceil 2^{M-f(\bar{c} \hat{c})} \rceil) \\ & \leq \log(2^{M-f(\bar{c} \hat{c})} + 1) \\ & = \log(2^{M-f(\bar{c} \hat{c})}) + \log(1 + 2^{f(\bar{c} \hat{c})-M}) \\ & \leq M - f(\bar{c} \hat{c}) + 2^{-\frac{M}{2}} \log e, \end{aligned} \quad (41)$$

where in the third line we simply factor out $2^{M-f(\bar{c} \hat{c})}$, and the fourth line follows from $\ln(1+x) \leq x$ along with the lemma condition $M - f(\bar{c} \hat{c}) > M/2 > 0$.

The remainder of the proof follows as in Lemma IV.1, except that we replace the sixth line with inequalities in either direction by bounding $H_\alpha(D)_{\rho_{|\bar{c}\hat{c}}}$ using the interval in Eq. (38) [together with the observation that the preceding line is monotonically increasing with respect to the $H_\alpha(D)_{\rho_{|\bar{c}\hat{c}}}$ terms; note that this is true in both the $\alpha < 1$ and $\alpha > 1$ regimes]. ■

The main difference between the above two lemmas is that Lemma IV.2 only achieves an “approximate” version of Lemma IV.1, but it does so using a single channel that works for all Rényi parameters simultaneously, which is

needed in some of our subsequent proofs. At large M , the gap between the upper and lower bounds in the above lemma shrinks to zero, so the approximation usually becomes sufficiently good for our analysis. We now use these two lemmas to “transfer” many properties of the standard Rényi entropy over to the f -weighted entropy.

Lemma IV.3. (Data processing) Let $\rho \in S_=(\bar{C} \hat{C} Q Q')$ be classical on $\bar{C} \hat{C}$, let f be a QES on $\bar{C} \hat{C}$, and take any $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty)$. Then, for any channel $\mathcal{E}: Q' \rightarrow Q''$,

$$H_\alpha^f(Q\bar{C}|\hat{C}Q'')_{\mathcal{E}[\rho]} \geq H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho. \quad (42)$$

If $\mathcal{E}$ is an isometry, then we have equality in the above bound.

Proof. Let $\mathcal{D}$ be a read-and-prepare channel as described in Lemma IV.1. Then, we have [here, for clarity, we explicitly write $\mathcal{D}$ in the formulas, instead of leaving it implicit in the state extension as in Eq. (36)]:

$$\begin{aligned} H_\alpha^f(Q\bar{C}|\hat{C}Q'')_{\mathcal{E}[\rho]} &= H_\alpha(DQ\bar{C}|\hat{C}Q'')_{\mathcal{D} \circ \mathcal{E}[\rho]} - M \\ &= H_\alpha(DQ\bar{C}|\hat{C}Q'')_{\mathcal{E} \circ \mathcal{D}[\rho]} - M \\ &\geq H_\alpha(DQ\bar{C}|\hat{C}Q'')_{\mathcal{D}[\rho]} - M \\ &= H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho, \end{aligned} \quad (43)$$

where the second line holds since $\mathcal{D}$ commutes with $\mathcal{E}$, and the third line is simply the usual data-processing inequality for Rényi conditional entropies in the range $\alpha \in [\frac{1}{2}, \infty)$ (Fact II.1). Similarly, the equality condition is simply inherited from that data-processing inequality.

Alternatively, we give a proof directly from the definition: First, considering $\alpha \in [\frac{1}{2}, 1)$, the data-processing inequality for sandwiched Rényi divergence itself gives

$$\begin{aligned} & D_\alpha(\mathcal{E}[\rho_{Q Q' \wedge \bar{c} \hat{c}}] \| \mathcal{E}[\mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}]) \leq D_\alpha(\rho_{Q Q' \wedge \bar{c} \hat{c}} \| \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}) \\ \iff & \rho(\bar{c} \hat{c}) 2^{(1-\alpha)(-f(\bar{c} \hat{c}) - D_\alpha(\mathcal{E}[\rho_{Q Q' \wedge \bar{c} \hat{c}}] \| \mathcal{E}[\mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}]))} \geq \rho(\bar{c} \hat{c}) 2^{(1-\alpha)(-f(\bar{c} \hat{c}) - D_\alpha(\rho_{Q Q' \wedge \bar{c} \hat{c}} \| \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}))}, \end{aligned} \quad (44)$$

where summing over all values of $\bar{c} \hat{c}$, taking the logarithm, and dividing by $1 - \alpha$ would prove the result. The proof for the case where $\alpha \in (1, \infty)$ follows from a similar argument. ■

Lemma IV.4. (Conditioning on classical registers) Let $\rho \in S_=(\bar{C} \hat{C} Q Q' Z)$ be classical on $\bar{C} \hat{C} Z$, let f be a QES on $\bar{C} \hat{C}$, and take any $\alpha \in (0, 1) \cup (1, \infty)$. Then,

$$H_\alpha^f(Q\bar{C}|\hat{C}Q'Z)_\rho = \frac{1}{1-\alpha} \log \left(\sum_z \rho(z) 2^{(1-\alpha)H_\alpha^f(Q\bar{C}|\hat{C}Q')_{\rho_{|z}}} \right). \quad (45)$$

Proof. Extend ρ with a read-and-prepare channel as described in Lemma IV.1. Then,

$$\begin{aligned} & H_\alpha^f(Q\bar{C}|\hat{C}Q'Z)_\rho \\ &= H_\alpha(DQ\bar{C}|\hat{C}Q'Z)_\rho - M \\ &= \frac{1}{1-\alpha} \log \left(\sum_z \rho(z) 2^{(1-\alpha)H_\alpha(DQ\bar{C}|\hat{C}Q')_{\rho_{|z}}} \right) - M \\ &= \frac{1}{1-\alpha} \log \left(\sum_z \rho(z) 2^{(1-\alpha)(M + H_\alpha^f(Q\bar{C}|\hat{C}Q')_{\rho_{|z}})} \right) - M \\ &= \frac{1}{1-\alpha} \log \left(\sum_z \rho(z) 2^{(1-\alpha)H_\alpha^f(Q\bar{C}|\hat{C}Q')_{\rho_{|z}}} \right), \end{aligned} \quad (46)$$

where in the third line we applied Fact II.2, and in the fourth line we implicitly exploited the fact that the

read-and-prepare channel in Lemma IV.1 achieves the relation in Eq. (36) for all states (in particular, also the conditional states $\rho_{|z}$).

Alternatively, we give a proof directly from the definition: Rewriting the formula for H_α^f entropy of the state in the lemma, we have

$$\begin{aligned} & H_\alpha^f(Q\bar{C}|\hat{C}Q'Z)_\rho \\ &= \frac{1}{1-\alpha} \log \left(\sum_z \sum_{\bar{c}\hat{c}} 2^{-(1-\alpha)f(\bar{c}\hat{c})} \right. \\ & \quad \left. \text{Tr}[(\rho_{Q' \wedge z \hat{c}})^{\frac{1-\alpha}{2\alpha}} \rho_{Q\bar{C}Q' \wedge z \bar{c} \hat{c}} (\rho_{Q' \wedge z \hat{c}})^{\frac{1-\alpha}{2\alpha}}]^\alpha \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_z \rho(z) \sum_{\bar{c}\hat{c}} 2^{-(1-\alpha)f(\bar{c}\hat{c})} \right. \\ & \quad \left. \text{Tr}[(\rho_{Q' \wedge \hat{c}|z})^{\frac{1-\alpha}{2\alpha}} \rho_{Q\bar{C}Q' \wedge \bar{c} \hat{c}|z} (\rho_{Q' \wedge \hat{c}|z})^{\frac{1-\alpha}{2\alpha}}]^\alpha \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_z \rho(z) 2^{(1-\alpha)H_\alpha^f(Q\bar{C}|\hat{C}Q')_{\rho_{|z}}} \right). \quad (47) \end{aligned}$$

Lemma IV.5. (Monotonicity in α) Let $\rho \in S_=(\bar{C}\hat{C}QQ')$ be classical on $\bar{C}\hat{C}$, let f be a QES on $\bar{C}\hat{C}$, and take any

$$\begin{aligned} H_\alpha^f(RQ\bar{C}|\hat{C}Q')_\rho &\leq H_{\alpha'}^f(Q\bar{C}|\hat{C}Q'R)_\rho + H_{\alpha''}(R|\hat{C}Q')_\rho \quad \text{if } (\alpha-1)(\alpha'-1)(\alpha''-1) < 0, \\ H_\alpha^f(RQ\bar{C}|\hat{C}Q')_\rho &\geq H_{\alpha'}^f(Q\bar{C}|\hat{C}Q'R)_\rho + H_{\alpha''}(R|\hat{C}Q')_\rho \quad \text{if } (\alpha-1)(\alpha'-1)(\alpha''-1) > 0. \end{aligned} \quad (50)$$

Furthermore, we also have, for any $\rho \in S_=(\bar{C}\hat{C}QQ')$,

$$\begin{aligned} H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho &\leq H_{\alpha'}^f(Q|\bar{C}\hat{C}Q')_\rho + H_{\alpha''}(\bar{C}|\hat{C}Q')_\rho \quad \text{if } (\alpha-1)(\alpha'-1)(\alpha''-1) < 0, \\ H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho &\geq H_{\alpha'}^f(Q|\bar{C}\hat{C}Q')_\rho + H_{\alpha''}(\bar{C}|\hat{C}Q')_\rho \quad \text{if } (\alpha-1)(\alpha'-1)(\alpha''-1) > 0, \end{aligned} \quad (51)$$

where by $H_\alpha^f(Q|\bar{C}\hat{C}Q')_\rho$ we mean

$$\begin{aligned} & H_\alpha^f(Q|\bar{C}\hat{C}Q')_\rho \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c}) 2^{(1-\alpha)(-f(\bar{c}\hat{c}) - D_\alpha(\rho_{Q\bar{C}Q' \wedge \bar{c}\hat{c}} \| \mathbb{I}_{Q\bar{C}} \otimes \rho_{Q' \wedge \bar{c}\hat{c}}))} \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c}) 2^{(1-\alpha)(-f(\bar{c}\hat{c}) + H_\alpha(Q|Q')_{\rho_{|\bar{c}\hat{c}}})} \right). \quad (52) \end{aligned}$$

Proof. We focus only on proving the bounds in Eq. (51); the bounds in Eq. (50) hold by precisely analogous arguments, but they are simpler since we do not need to consider the consistency of Eq. (52) with our preceding H_α^f -entropy properties.

$\alpha, \alpha' \in [\frac{1}{2}, 1) \cup (1, \infty)$ such that $\alpha \geq \alpha'$. Then,

$$H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho \leq H_{\alpha'}^f(Q\bar{C}|\hat{C}Q')_\rho. \quad (48)$$

Proof. Let $M > 0$ be any value such that $M - f(\bar{c}\hat{c}) > M/2 > 0$, and extend ρ with a read-and-prepare channel as described in Lemma IV.1. Then, we have

$$\begin{aligned} H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho &\leq H_\alpha(DQ\bar{C}|\hat{C}Q')_\rho - M \\ &\leq H_{\alpha'}(DQ\bar{C}|\hat{C}Q')_\rho - M \\ &\leq 2^{-\frac{M}{2}} \log e + H_{\alpha'}^f(Q\bar{C}|\hat{C}Q')_\rho, \end{aligned} \quad (49)$$

where the second line follows from the first inequality in Eq. (39), the third line follows from the monotonicity of sandwiched conditional entropies in α [32], and the last line follows from the second inequality in Eq. (39). Since this inequality holds for *arbitrary* (sufficiently large) M , we can take the $M \rightarrow \infty$ limit so that the $2^{-\frac{M}{2}}$ term vanishes, yielding the desired result. ■

Lemma IV.6. (Chain rules) Let f be a QES on classical registers $\bar{C}\hat{C}$, and take any $\alpha, \alpha', \alpha'' \in (\frac{1}{2}, 1) \cup (1, \infty)$ such that $[\alpha/(\alpha-1)] = [\alpha'/(\alpha'-1)] + [\alpha''/(\alpha''-1)]$. Then, we have, for any $\rho \in S_=(\bar{C}\hat{C}RQQ')$,

Take any $M > 0$ such that $M - f(\bar{c}\hat{c}) > (M/2) > 0$, and extend ρ with a read-and-prepare channel as described in Lemma IV.2. Then, as stated in the lemma, we have

$$\begin{aligned} & M + H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho \\ &\leq H_\alpha(DQ\bar{C}|\hat{C}Q')_\rho \\ &\leq M + 2^{-\frac{M}{2}} \log e + H_{\alpha'}^f(Q\bar{C}|\hat{C}Q')_\rho, \end{aligned} \quad (53)$$

and also [by viewing $H_\alpha^f(Q|\bar{C}\hat{C}Q')_\rho$ as an instance of H_α^f entropy where *both* the $\bar{C}$ and $\hat{C}$ registers are viewed as the “public” part, as is consistent with the formula in Eq. (52) above]

$$\begin{aligned}
& M + H_{\alpha'}^f(Q|\bar{C}\hat{C}Q')_{\rho} \\
& \leq H_{\alpha'}(DQ|\bar{C}\hat{C}Q')_{\rho} \\
& \leq M + 2^{-\frac{M}{2}} \log e + H_{\alpha'}^f(Q|\bar{C}\hat{C}Q')_{\rho}. \quad (54)
\end{aligned}$$

Then, we have the following chain of inequalities if $(\alpha - 1)(\alpha' - 1)(\alpha'' - 1) < 0$:

$$\begin{aligned}
& H_{\alpha}^f(Q\bar{C}|\hat{C}Q')_{\rho} \\
& \leq H_{\alpha}(DQ\bar{C}|\hat{C}Q')_{\rho} - M \\
& \leq H_{\alpha'}(DQ|\bar{C}\hat{C}Q')_{\rho} + H_{\alpha''}(\bar{C}|\hat{C}Q')_{\rho} - M \\
& \leq H_{\alpha}^f(Q|\bar{C}\hat{C}Q')_{\rho} + H_{\alpha''}(\bar{C}|\hat{C}Q')_{\rho} + 2^{-\frac{M}{2}} \log e, \quad (55)
\end{aligned}$$

where the second line follows from the first inequality in Eq. (53), the third line is a special case of Proposition 8 in Ref. [42], and the fourth line is a result of applying the second inequality in Eq. (54). Taking the $M \rightarrow \infty$ limit, we obtain the first bound in Eq. (51). The second bound [for $(\alpha - 1)(\alpha' - 1)(\alpha'' - 1) > 0$] holds by a similar argument, using Proposition 7 of Ref. [42] instead. ■

Arguably, the construction of the D register is not strictly necessary for our results; it should be possible, in principle, to prove these results directly from the definition of H_{α}^f entropies, and we indeed did so for Lemmas IV.3 and IV.4. However, the advantage of the D register construction is that more sophisticated results like the chain rule corresponding to Lemma IV.6 can be transferred to H_{α}^f entropies with equal ease, rather than having to rederive them “from base principles.” Similarly, in our subsequent results involving entropy accumulation, this D register construction will allow us to exploit advanced results such as the GEAT without explicitly rederiving them in the framework of H_{α}^f entropies.

Apart from the above, another convenient property is the following:

Lemma IV.7. (Normalization property) Let $\rho \in \mathcal{S}_{=}(\bar{C}\hat{C}Q'Q')$ be classical on $\bar{C}\hat{C}$, and let f be a QES on $\bar{C}\hat{C}$. Then, for any constant $\kappa \in \mathbb{R}$, we have

$$H_{\alpha}^{f+\kappa}(Q\bar{C}|\hat{C}Q')_{\rho} = H_{\alpha}^f(Q\bar{C}|\hat{C}Q')_{\rho} - \kappa, \quad (56)$$

where $f + \kappa$ simply denotes the QES with values $f(\bar{c}\hat{c}) + \kappa$.

Proof. This follows directly from the definition. ■

Remark IV.1. In the special case where Q is trivial (or in a certain sense, if Q is classical), [43] a QES is *exactly* equivalent to a QEF as defined in Ref. [18], except that, in this work, we take some logarithms or exponentials to make our results more “entropylike”—for instance, Ref. [18] mainly works directly with the trace terms in the last line of Eq. (30), which are referred to as Rényi powers in that work. (Strictly speaking, they also impose a condition that corresponds to requiring $H_{\alpha}^f(Q\bar{C}|\hat{C}Q')_{\rho} \geq 0$

over some class of states under consideration, but as noted in that work, this condition can be enforced using the normalization property in Lemma IV.7.) Similarly, in the case where $\bar{C}$ is trivial [so Eq. (32) holds], the definition of f -weighted entropy we gave above is extremely similar to the original definition that was introduced in Ref. [17] (which we restate in Definition VI.1), except we use H_{α} rather than $H_{\alpha}^{\uparrow}$ and the convex combination is adjusted accordingly (also, Ref. [17] uses the term “tradeoff function” rather than “QES” to refer to the function f , under the imposition of the aforementioned “normalization” condition that we have chosen not to include here).

Furthermore, as noted in Ref. [18], one can certainly consider using Petz entropies instead of sandwiched entropies when defining these concepts. However, that work was unable to prove a “QEF chaining” property for Petz entropies; similarly, we do not prove it here for the $\alpha > 1$ regime because we rely on various intermediate results in the GEAT proof that were only derived for sandwiched entropies. (On the other hand, our results for the $\alpha < 1$ regime involve Petz entropies; see Appendix E.) Another potential generalization to consider would be whether the original f -weighted entropy definition from Ref. [17] could be extended to the case where $\bar{C}$ is nontrivial; however, some technical care is necessary since it is less clear how to choose an analog of $H_{\alpha}^{\uparrow}$ to use in the divergence-based formulas we gave in Definition IV.1—we discuss this case in a follow-up work.

B. QES chaining or accumulation

We now present the first key result in this work, that H_{α}^f entropies “accumulate” in a simple fashion when considering a state generated by a sequence of GEATT channels. This result is almost identical to the “QEF chaining” property described in Ref. [18]. However, we have derived it using the conditions and framework of the GEAT instead; in particular, it holds under the more relaxed NS conditions of the GEAT, rather than the stricter Markov conditions of Ref. [18] or the original EAT [at the cost of a very slight “loss” in Rényi parameter; see Eq. (64)]. In Sec. VI A, we also show that we can exactly reproduce the bounds in Ref. [18] if we simply impose the same Markov conditions instead.

Theorem IV.1. (H_{α}^f -entropy accumulation) Let ρ be a state generated by a sequence of GEATT channels $\{\mathcal{M}_j\}_{j=1}^n$ (Definition III.2). For each j , suppose that for every value $\bar{c}_1^{j-1}\hat{c}_1^{j-1}$, we have a QES $f_{|\bar{c}_1^{j-1}\hat{c}_1^{j-1}}$ on registers $\bar{C}_j\hat{C}_j$ [44]. Define the following QES on $\bar{C}_1^n\hat{C}_1^n$:

$$f_{\text{full}}(\bar{c}_1^n\hat{c}_1^n) := \sum_{j=1}^n f_{|\bar{c}_1^{j-1}\hat{c}_1^{j-1}}(\bar{c}_j\hat{c}_j). \quad (57)$$

Take any $\alpha \in (1, 2)$, and let $\hat{\alpha} = 1/(2 - \alpha)$. Then, we have

$$H_{\alpha}^{f_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \geq \sum_j \min_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} \kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}},$$

$$\text{where } \kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} := \inf_{\nu \in \Sigma_j} H_{\hat{\alpha}}^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}}(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu}, \quad (58)$$

where Σ_j denotes the set of all states of the form $\mathcal{M}_j[\omega_{R_{j-1}E_{j-1}\tilde{E}}]$ for some initial state $\omega \in S = (R_{j-1}E_{j-1}\tilde{E})$, with $\tilde{E}$ being a register of large enough dimension to serve as a purifying register for any of the $R_j E_j$ registers.

Consequently, if we instead define the following “normalized” QES on $\bar{C}_1^n \hat{C}_1^n$,

$$\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) := \sum_{j=1}^n \hat{f}_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j),$$

$$\text{where } \hat{f}_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) := f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) + \kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}, \quad (59)$$

then

$$H_{\alpha}^{\hat{f}_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \geq 0. \quad (60)$$

As the full proof is somewhat lengthy, we defer it to Appendix B; however, the overall structure can be sketched

out as follows. The idea is to rely on the relations between H_{α}^f entropies and standard Rényi entropies that we described in the previous section, which are similar to some steps in the proofs of the (G)EAT-with-testing in Refs. [1,2,4]. For simplicity, let us focus on a case where all the QESs $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ are identical (assuming all the $\bar{C}_j$ registers have the same alphabet, and similarly for $\hat{C}_j$), so all of them are equal to a single QES f . Then, we basically define new channels $\mathcal{N}_j$ that extend the $\mathcal{M}_j$ channels by applying an additional read-and-prepare channel $\mathcal{D}_j: \bar{C}_j \hat{C}_j \rightarrow \bar{C}_j \hat{C}_j D_j$ of the form described in Lemma IV.2. Next, we could apply the Rényi chain rule of Lemma 3.6 of Ref. [4] (Fact III.1 stated above) to obtain a bound of the form

$$H_{\alpha}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \geq \sum_j \inf H_{\hat{\alpha}}(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu}, \quad (61)$$

with the infimum taking place over states ν that could be produced by $\mathcal{N}_j \otimes \text{id}_{\tilde{E}}$. (This bound is basically the same as some intermediate steps in Ref. [4].) Now, by analyzing these channels in a similar way to the Lemma IV.2 proof, one can show that the states they produce satisfy

$$H_{\alpha}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \leq nM + H_{\alpha}^{f_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} + n2^{-\frac{M}{2}} \log e,$$

$$H_{\hat{\alpha}}(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu} \geq M + H_{\hat{\alpha}}^f(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu}, \quad (62)$$

hence relating the terms in the bound in Eq. (61) to H_{α}^f entropies. Noting that the resulting nM terms simply cancel and recalling that we can choose arbitrarily large M so $2^{-\frac{M}{2}}$ becomes arbitrarily small, we obtain the desired result in Eq. (58). Essentially, our proof differs from Refs. [1,2,4] because those works applied a condition that f lower bounds the single-round von Neumann entropy in an “averaged” sense (i.e., defines a min-tradeoff function [1,2,4]), whereas we observe that, in fact, this was not necessary—we can just view f as an arbitrary “score” value. (However, as discussed below Eq. (33), in some situations we can view f as being a log-mean-exponential bound on Rényi entropy.)

The full proof essentially proceeds along the above lines, except that we need to define the input and output registers of the $\mathcal{N}_j$ channels differently, such that they preserve a copy of the “past” testing registers $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ at each step. This method is needed so that the read-and-prepare channels $\mathcal{D}_j$ can also take the values on these registers into account, which allows us to “encode” any QES value $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j)$ in the entropies of the D_j registers. We present these details in Appendix B.

Note that without further conditions on the channels or QES choices, the bound in the above result is almost tight

(for α close to 1) since it is almost saturated by an IID example. Specifically, if the action of each channel $\mathcal{M}_j$ is simply to independently generate a fresh copy of some fixed state σ on registers $S_j \bar{C}_j \hat{C}_j \tilde{E}_j$ and append $\tilde{E}_j$ to E_{j-1} , then the final state is an IID state $\rho = \sigma^{\otimes n}$. Hence, if all the QESs are identical to a single QES f , we immediately obtain

$$H_{\alpha}^{f_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} = nH_{\alpha}^f(S_1 \bar{C}_1 | \hat{C}_1 \tilde{E}_1)_{\sigma}$$

$$= \sum_j \inf_{\nu \in \Sigma_j} H_{\alpha}^f(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu}, \quad (63)$$

which only differs from the bound in Eq. (58) by having α in place of $\hat{\alpha}$. However, if we write $\alpha = 1 + \mu$ for some $\mu > 0$, then we see

$$\hat{\alpha} = \frac{1}{1 - \mu} = 1 + \frac{\mu}{1 - \mu} = 1 + \mu + O(\mu^2), \quad (64)$$

so it only differs from α by a second-order correction [which becomes a “third-order” correction for the purposes of finite-size analysis; see the later discussion in Sec. V leading up to Eq. (89)]. Hence, in an IID scenario,

Theorem IV.1 is tight up to the difference in Eq. (64). In fact, in Sec. VIA, we show that under the stricter Markov conditions in the original EAT, this change of Rényi parameter can be avoided entirely, hence producing a bound exactly identical to the QEF-chaining property in Ref. [18].

There might be some room for improvement in scenarios where the QESs are different in each round; for instance, at a glance, it perhaps seems a bit too pessimistic to take the worst-case value over $\tilde{c}_1^{j-1} \hat{c}_1^{j-1}$ in Eq. (58). However, inspecting our above proof shows that, while this minimum first appears in the bound in Eq. (B6), it is easy to construct an initial state ω that saturates that bound, using Eq. (B5). Hence, to improve it, one would have to restrict the infimum in the original “GEAT without testing” bound in Eq. (B3) from Ref. [4], which is a challenging prospect given the proof methods in that work (unless, perhaps, one could design the $\mathcal{N}_j$ channels in a different way such that the minimum over $\tilde{c}_1^{j-1} \hat{c}_1^{j-1}$ does not occur at all).

We highlight the fact that computation of the $\kappa_{\tilde{c}_1^{j-1} \hat{c}_1^{j-1}}$ values in practice might be aided by the following observation, which allows it to be rewritten as a convex optimization (and is in fact critical for our later proofs in Sec. V). In the following lemma, for flexibility in potential applications, we denote the input space for the channel as a register $\tilde{Q}$ that does not need to straightforwardly correspond to the input spaces of GEAT channels. We have also not included a “memory register” R in the output of the channel since it is not necessary for the lemma statement and our subsequent proofs.

Lemma IV.8. Let $\mathcal{M}$ be a channel $\tilde{Q} \rightarrow SE\tilde{C}\hat{C}$ where the output is always classical on $\tilde{C}\hat{C}$, and let f be a QES on $\tilde{C}\hat{C}$. Let $\tilde{E}$ be a register such that $\dim(\tilde{Q}) \leq \dim(\tilde{E})$, and let Pur be a purifying function for $\tilde{Q}$ onto $\tilde{E}$ (Definition III.3). Then, for any state $\omega_{\tilde{Q}\tilde{E}}$ and $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty)$,

$$H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\omega_{\tilde{Q}\tilde{E}}]} \geq H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\text{Pur}(\omega_{\tilde{Q}})]}, \quad (65)$$

with equality if $\omega_{\tilde{Q}\tilde{E}}$ is pure; furthermore, for $\alpha \in (1, \infty)$, the right-hand side is a convex function of $\omega_{\tilde{Q}}$.

Proof. If $\omega_{\tilde{Q}\tilde{E}}$ is pure, then by using the isometric equivalence of purifications along with the corresponding invariance of H_α^f entropies (one instance of an equality condition in Lemma IV.3), we conclude the equality condition in Eq. (65). If $\omega_{\tilde{Q}\tilde{E}}$ is not pure, then there exists a purification of it such that $\text{Tr}_{\tilde{E}'}[\omega_{\tilde{Q}\tilde{E}\tilde{E}'}] = \omega_{\tilde{Q}\tilde{E}}$. Thus, we have the following:

$$\begin{aligned} H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\omega_{\tilde{Q}\tilde{E}}]} &= H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M} \circ \text{Tr}_{\tilde{E}'}[\omega_{\tilde{Q}\tilde{E}\tilde{E}'}]} \\ &\geq H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E}\tilde{E}')_{\mathcal{M}[\omega_{\tilde{Q}\tilde{E}\tilde{E}'}]} \\ &= H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\text{Pur}(\omega_{\tilde{Q}})]}, \end{aligned} \quad (66)$$

where the second line holds by applying Lemma IV.3 and noting that the partial trace $\text{Tr}_{\tilde{E}'}[\cdot]$ and $\mathcal{M}$ commute; the last line follows by noting that purifications are isometrically equivalent and using the equality condition in Lemma IV.3.

To prove the convexity property, for any two states $\omega_{\tilde{Q}}^{(0)}$ and $\omega_{\tilde{Q}}^{(1)}$, and probability distribution $\{p(i)\}_{i=0}^1$, we construct the following state, which is easily verified to be an extension of the “averaged” state $\omega_{\tilde{Q}} := \sum_{i=0}^1 p(i) \omega_{\tilde{Q}}^{(i)}$:

$$\omega_{\tilde{Q}\tilde{E}\tilde{F}} := \sum_{i=0}^1 p(i) \text{Pur}(\omega_{\tilde{Q}}^{(i)}) \otimes |i\rangle\langle i|_{\tilde{F}}. \quad (67)$$

Now, consider the state $\text{Pur}(\omega_{\tilde{Q}})$. Since it is a purification of $\omega_{\tilde{Q}}$ onto $\tilde{E}$, there exists a channel $\mathcal{E}: \tilde{E} \rightarrow \tilde{E}\tilde{F}$ such that

$$\mathcal{E}[\text{Pur}(\omega_{\tilde{Q}})] = \omega_{\tilde{Q}\tilde{E}\tilde{F}}. \quad (68)$$

Therefore, we can bound the function value at the “averaged” state $\omega_{\tilde{Q}}$ via

$$\begin{aligned} H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\text{Pur}(\omega_{\tilde{Q}})]} &\leq H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E}\tilde{F})_{\mathcal{E} \circ \mathcal{M}[\text{Pur}(\omega_{\tilde{Q}})]} \\ &= H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E}\tilde{F})_{\mathcal{M} \circ \mathcal{E}[\text{Pur}(\omega_{\tilde{Q}})]} \\ &= \frac{1}{1-\alpha} \log \sum_{i=0}^1 p(i) 2^{(1-\alpha)(H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\text{Pur}(\omega_{\tilde{Q}}^{(i)})]})} \\ &\leq \sum_{i=0}^1 p(i) H_\alpha^f(S\tilde{C}|\hat{C}E\tilde{E})_{\mathcal{M}[\text{Pur}(\omega_{\tilde{Q}}^{(i)})]}, \end{aligned} \quad (69)$$

as desired, where the second line is due to the data-processing property in Lemma IV.3, the third line holds since $\mathcal{E}$ and $\mathcal{M}$ commute, the fourth line follows from Eqs. (67) and (68) and Lemma IV.4, and the last line follows by concavity of the log function and by noting $\alpha \in (1, \infty)$. ■

Remark IV.2. The only properties of H_α^f that were used in the above proof were data processing (Lemma IV.3) and the fact that for $\alpha > 1$ it is “convex when conditioned on a labeling register,” as in, for a state classical on Z , we have

$$H_\alpha^f(Q\tilde{C}|\hat{C}Q'Z)_\rho \leq \sum_z p(z) H_\alpha^f(Q\tilde{C}|\hat{C}Q')_{\rho_{|z}}, \quad (70)$$

which follows from the conditioning-on-classical-registers property (Lemma IV.4). Therefore, the proof immediately generalizes to any other entropy with the same properties, such as the Petz or sandwiched Rényi entropies for $\alpha \geq 1$ (as long as α is within the regime where data processing holds; see Refs. [30,31,45]), which includes the von Neumann entropy.

Note that including the “labeling” register Z in the conditioning is vital for Eq. (70) to hold. If it is omitted, then, e.g., for the case of von Neumann entropy, we know that $H(Q\bar{C}|\hat{C}Q')_\rho$ is a *concave* function of ρ , and hence the general inequality is instead the reverse direction $H(Q\bar{C}|\hat{C}Q')_\rho \geq \sum_z \rho(z)H(Q\bar{C}|\hat{C}Q')_{\rho|z}$; i.e., the only reason we have the bound in Eq. (70) for that case is that including Z in the conditioning makes it an equality.

C. Applications

We now describe some applications of Theorem IV.1 by itself [without yet reducing it to the simpler form Eq. (2) outlined previously]. Note that the key ideas in this section were already established in Refs. [17,18]; here, we just provide an exposition of the main steps for completeness.

1. Approach of Ref. [17] (variable-length protocols)

We first describe how Ref. [17] applies bounds of the form in Theorem IV.1 to protocols that produce an output key of variable length. The basic idea is that if the $\bar{C}_1^n$ registers are trivial and we have the “normalized QES” bound in Eq. (60) from Theorem IV.1 [i.e., we have $H_\alpha^{\hat{f}_{\text{full}}}(S_1^n|\hat{C}_1^n E_n)_\rho \geq 0$], then the analysis in that work shows that a variable-length secret key can usually be obtained by looking at the value $\hat{c}_1^n$ on the publicly announced registers $\hat{C}_1^n$, and then computing $\hat{f}_{\text{full}}(\hat{c}_1^n)$ and hashing to a key length determined by that value. (Strictly speaking, we need a relation between the $H_\alpha^{\hat{f}_{\text{full}}}$ entropy and its analog based on $H_\alpha^\uparrow$ that we describe later; see Lemma VI.2.) This case usually suffices for device-dependent security proofs. On the other hand, in DI security proofs, the $\bar{C}_1^n$ registers are usually not trivial [18,29,36,46]. In that case, if we only have a bound on $H_\alpha^{\hat{f}_{\text{full}}}(S_1^n|\bar{C}_1^n|\hat{C}_1^n E_n)_\rho$, then it does not seem straightforward to immediately apply their proof approach to obtain variable-length security.

Still, one of the results we derived above provides a possible solution—specifically, Lemma IV.6 lets us convert it to a lower bound on $H_\alpha^{\hat{f}_{\text{full}}}(S_1^n|\bar{C}_1^n|\hat{C}_1^n E_n)_\rho$ instead (see also Remark VIII.1), after which we can apply the preceding analysis [47]. Unfortunately, it may be somewhat suboptimal as the change in Rényi parameters here is potentially significant [see Eq. (85), although there may be some potential to carefully tune the α' and α'' choices to minimize this effect], unlike the change from α to $\hat{\alpha}$. It might potentially be better to find a more “direct” analysis that uses a bound on $H_\alpha^{\hat{f}_{\text{full}}}(S_1^n|\bar{C}_1^n|\hat{C}_1^n E_n)_\rho$ to produce a variable-length secret key. We leave this interesting question for future work, though one caveat is that for protocols such as DIQKD (though potentially not DIRE), the $\bar{C}_1^n$ registers have to be somehow communicated between Alice and Bob to perform parameter estimation; hence, it might be

necessary to “move” the $\bar{C}_1^n$ registers into the conditioning systems somewhere in the analysis.

Note that in the above procedure, it might appear that computing $\hat{f}_{\text{full}}(\hat{c}_1^n)$ [more generally $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$] could be challenging because, by the definition in Eq. (59), the function $\hat{f}_{\text{full}}$ depends on specifying all the QESs $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ across different rounds, and also all the $\kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ values (each of which is some minimization problem). However, Ref. [18] presented the following critical simplification (albeit for the purposes of applying their results for fixed-length protocols): When applying the above procedure in practice, one only needs to compute $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$ for the single value of $\bar{c}_1^n \hat{c}_1^n$ that actually occurred when the protocol was performed. Therefore, one can instead apply the following procedure:

- (1) First, implement the protocol without choosing any QESs beforehand. Look at the value $\bar{c}_1^n \hat{c}_1^n$ that actually occurred on the registers $\bar{C}_1^n \hat{C}_1^n$.
- (2) For each j , apply any arbitrary procedure that looks at the values $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$ that actually occurred, then (deterministically) returns a single choice of QES on $\bar{C}_j \hat{C}_j$. Denote this QES as $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$, and compute (or lower bound) the corresponding $\kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ value.
- (3) The values in the preceding step suffice to determine (or lower bound) $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$, so compute it and proceed with the privacy amplification.

With the above procedure, for each round, we only need to choose the *single* QES $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ (and compute $\kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$) corresponding to the value of $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$ that actually occurred in the protocol; i.e., we do not need to explicitly specify QESs $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ or compute $\kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ for all the other $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$ values. Note, however, that the Theorem IV.1 bound is entirely valid to apply in this context because this procedure indeed specifies, on an abstract level, a well-defined QES $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ and value $\kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ for every possible $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$ value, even if they did not actually occur in the protocol. [Qualitatively, we are exploiting the fact that while the abstract *function* $\hat{f}_{\text{full}}$ depends on all those quantities, in the physical protocol, we only need to evaluate the single value $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$, which only depends on a subset of those quantities.]

We have not yet specified how one should design a procedure that chooses the QESs $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ (while our above description is valid for any such procedure, we would of course want one that produces key rates that are as high as possible). In Ref. [18], some methods were developed for this purpose, including the option of “adaptively” choosing QESs $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ based on the past observations $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$ for each j , which may be useful for handling time-varying behavior. However, in this work, we describe an alternative procedure in Sec. V (see Remark V.5), which may be

simpler and easier to apply. In addition, note that if we ignore the option to have them depend on past observations $\tilde{c}_1^{j-1} \hat{c}_1^{j-1}$, so all of them are equal to a single QES f , then Ref. [17] also describes a procedure for choosing f . Still, we believe that the approach we present in Remark V.5 should perform better in the finite-size regime, though we do not analyze this rigorously; furthermore, our approach also gives the option for “adaptive” QES choices as mentioned above, at least in principle. We defer further discussion to that section.

2. Approach of Ref. [18] (fixed-length protocols)

Alternatively, Ref. [18] described how to apply bounds of the form in Theorem IV.1 while we are instead interested in entropy conditioned on an event, as is the case for protocols that simply make an accept or abort decision and produce a key of fixed length if they accept. (More precisely, their approach was based on QEFs; here, we verify that it generalizes to H_α^f entropies as well.)

To that end, we first state the following lemma, which is a slight generalization of Lemma 4.5 of Ref. [4].

Lemma IV.9. Consider any state $\rho \in \mathcal{S}_=(SED\tilde{C}\hat{C})$ that is classical on $\tilde{C}\hat{C}$ and has the form

$$\rho_{SED\tilde{C}\hat{C}} = \sum_{\tilde{c}\hat{c} \in \Omega} \rho(\tilde{c}\hat{c}) |\tilde{c}\hat{c}\rangle \langle \tilde{c}\hat{c}|_{\tilde{C}\hat{C}} \otimes \rho_{SE|\tilde{c}\hat{c}} \otimes \rho_{D|\tilde{c}\hat{c}}, \quad (71)$$

with Ω being a subset of the alphabet of registers $\tilde{C}\hat{C}$. Then, for any $\alpha \in (1, \infty)$, we have the following:

$$H_\alpha^\uparrow(DS\tilde{C}|\hat{C}E)_\rho \leq H_\alpha^\uparrow(S\tilde{C}|\hat{C}E)_\rho + \max_{\tilde{c}\hat{c} \in \Omega} H_\alpha(D)_{\rho|\tilde{c}\hat{c}}, \quad (72)$$

$$H_\alpha(DS\tilde{C}|\hat{C}E)_\rho \leq H_\alpha(S\tilde{C}|\hat{C}E)_\rho + \max_{\tilde{c}\hat{c} \in \Omega} H_\alpha(D)_{\rho|\tilde{c}\hat{c}}. \quad (73)$$

Proof. Let $\sigma_{\hat{C}E}$ be the optimizer in Definition II.6 for the conditional entropy in the lhs of Eq. (72), i.e.,

$$H_\alpha^\uparrow(DS\tilde{C}|\hat{C}E)_\rho = -D_\alpha(\rho_{DSE\tilde{C}\hat{C}} \| \mathbb{I}_{DS\tilde{C}} \otimes \sigma_{\hat{C}E}). \quad (74)$$

From Fact II.2, we have

$$\begin{aligned} H_\alpha^\uparrow(DS\tilde{C}|\hat{C}E)_\rho &= \frac{1}{1-\alpha} \log \left(\sum_{\tilde{c}\hat{c} \in \Omega} \rho(\tilde{c}\hat{c})^\alpha \sigma(\hat{c})^{1-\alpha} 2^{(\alpha-1)D_\alpha(\rho_{DSE|\tilde{c}\hat{c}} \| \mathbb{I}_{DS\tilde{C}} \otimes \sigma_{E|\hat{c}})} \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\tilde{c}\hat{c} \in \Omega} \rho(\tilde{c}\hat{c})^\alpha \sigma(\hat{c})^{1-\alpha} 2^{(\alpha-1)(D_\alpha(\rho_{D|\tilde{c}\hat{c}} \| \mathbb{I}_D) + D_\alpha(\rho_{SE|\tilde{c}\hat{c}} \| \mathbb{I}_S \otimes \sigma_{E|\hat{c}}))} \right) \\ &\leq \frac{1}{1-\alpha} \log \left(\min_{\tilde{c}\hat{c} \in \Omega} [2^{(\alpha-1)D_\alpha(\rho_{D|\tilde{c}\hat{c}} \| \mathbb{I}_D)}] \sum_{\tilde{c}\hat{c} \in \Omega} \rho(\tilde{c}\hat{c})^\alpha \sigma(\hat{c})^{1-\alpha} 2^{(\alpha-1)D_\alpha(\rho_{SE|\tilde{c}\hat{c}} \| \mathbb{I}_S \otimes \sigma_{E|\hat{c}})} \right) \\ &\leq \max_{\tilde{c}\hat{c} \in \Omega} H_\alpha(D)_{\rho|\tilde{c}\hat{c}} + H_\alpha^\uparrow(S\tilde{C}|\hat{C}E)_\rho, \end{aligned} \quad (75)$$

where the second line follows from the fact that $\rho_{DSE|\tilde{c}\hat{c}} = \rho_{D|\tilde{c}\hat{c}} \otimes \rho_{SE|\tilde{c}\hat{c}}$, and the last line follows from Definition II.6 and concavity of the log function. This formula yields the first bound in Eq. (72). To obtain the second bound in Eq. (73), simply repeat the above computations with σ replaced by ρ itself. ■

With the above lemma in hand, we have the following corollary.

Corollary IV.1. Consider the same conditions and notation as in Theorem IV.1. Suppose, furthermore, that the state ρ is of the form [48] $p_\Omega \rho_{|\Omega} + (1 - p_\Omega) \rho_{|\bar{\Omega}}$ for some $p_\Omega \in (0, 1]$ and normalized states $\rho_{|\Omega}$ and $\rho_{|\bar{\Omega}}$, and let $\tilde{\Omega}$ denote the set of all values $\tilde{c}_1^n \hat{c}_1^n$ that have nonzero probability in $\rho_{|\Omega}$. Then,

$$\begin{aligned} H_\alpha^\uparrow(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}} &\geq \min_{\tilde{c}_1^n \hat{c}_1^n \in \tilde{\Omega}} \hat{f}_{\text{full}}(\tilde{c}_1^n \hat{c}_1^n) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\ &\geq \left(\sum_j \min_{\tilde{c}_1^{j-1} \hat{c}_1^{j-1}} \kappa_{\tilde{c}_1^{j-1} \hat{c}_1^{j-1}} \right) + \min_{\tilde{c}_1^n \hat{c}_1^n \in \tilde{\Omega}} f_{\text{full}}(\tilde{c}_1^n \hat{c}_1^n) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega}. \end{aligned} \quad (76)$$

Proof. Let $\mathcal{D}: \tilde{C}_1^n \hat{C}_1^n \rightarrow \tilde{C}_1^n \hat{C}_1^n D$ be a read-and-prepare channel in the sense of Lemma IV.1 for the QES $\hat{f}_{\text{full}}(\tilde{c}_1^n \hat{c}_1^n)$ stated in the theorem conditions; i.e., it reads the registers $\tilde{C}_1^n \hat{C}_1^n$ and generates a corresponding state on register D . By linearity, we can write $\mathcal{D}[\rho] = p_\Omega \mathcal{D}[\rho_{|\Omega}] + (1 - p_\Omega) \mathcal{D}[\rho_{|\bar{\Omega}}]$ (in this proof, for clarity, we explicitly write out the $\mathcal{D}$ channel when extending the states with it). Note that, by construction of the $\mathcal{D}$ channel, the $\mathcal{D}[\rho_{|\Omega}]$ term is of the form of Eq. (71), with the sum over $\tilde{c}\hat{c}$ being restricted to $\tilde{\Omega}$ since that was the case in the original state $\rho_{|\Omega}$. Hence, we are allowed to apply Lemma IV.9, obtaining

$$\begin{aligned}
H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\mathcal{D}[\rho_\Omega]} &\geq H_\alpha^\dagger(DS_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\mathcal{D}[\rho_\Omega]} - \max_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} H_\alpha(D)_{\mathcal{D}[\rho]_{|\bar{c}_1^n \hat{c}_1^n}} \\
&\geq H_\alpha(DS_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\mathcal{D}[\rho]} - \max_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} H_\alpha(D)_{\mathcal{D}[\rho]_{|\bar{c}_1^n \hat{c}_1^n}} - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&= M + H_\alpha^{\hat{f}_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho - \max_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} H_\alpha(D)_{\mathcal{D}[\rho]_{|\bar{c}_1^n \hat{c}_1^n}} - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&= H_\alpha^{\hat{f}_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho + \min_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} \hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&\geq \min_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} \hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&= \min_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} \sum_{j=1}^n (f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) + \kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}}) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&\geq \left(\sum_{j=1}^n \min_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} \kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} \right) + \min_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} f_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega}, \tag{77}
\end{aligned}$$

where the first line follows from Lemma IV.9, the second line is from applying Lemma B.5 of Ref. [1] along with the fact that $H_\alpha^\dagger \geq H_\alpha$, the third line is due to Eq. (36), the fourth line is the result of Eq. (35), the fifth follows from Eq. (60), and the sixth line is just the substitution of $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$ from Eq. (59). ■

To apply the above corollary in practice, we can follow the approach presented in Ref. [18]: Compute $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$ in a protocol using the procedure described above in Sec. IV C 1, and define the conditioning event Ω to be that $\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) \geq K$ for some predetermined threshold value K . In that case, the above corollary tells us that $H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} \geq K - [\alpha/(\alpha-1)] \log(1/p_\Omega)$, so we have a lower bound on the Rényi entropy of the conditional state to use in subsequent proof steps (for example, showing we can produce a secret key of fixed length). The question of finding a “reasonable” choice of K (such that the protocol does not almost always abort, even under honest behavior) is somewhat subtle, and we defer to Ref. [18] for an in-depth discussion. Here, we simply note that the analysis in the next section suggests that, given a “good” choice of QESs, when the honest behavior is IID, we should pick K to be somewhat less than n times the honest single-round Rényi entropy; see the discussions in Secs. VA–VC.

Thus far, we have been deferring the discussion of how to choose “good” QESs. In the next section, we discuss this point in great detail, which is the next main contribution of our work. A remarkable consequence of our analysis, however, is that for some scenarios (where all the channels are “basically the same”), we can obtain an intuitive and very tight lower bound on $H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega}$ (namely, Theorem V.1 below) that does not involve any explicit choice of QES, in that the bound is already implicitly using

the best such choice. Note that even outside of those scenarios (e.g., if the channels have time-varying behavior, the optimal QES choice in each round might be different, as discussed previously), our methods may still be useful; see Remark V.5. We now present these results.

V. SIMPLIFIED VERSIONS

In some applications of the GEAT to fixed-length protocols, the channels in the sequence can be thought of as being basically the same in some sense (or at least they can be “relaxed” to a common channel). In such circumstances, we can greatly simplify Corollary IV.1, as we shall now describe. Furthermore, the overall approach we describe here should also yield some useful (albeit more elaborate) techniques to handle variable-length protocols and/or scenarios where the channels exhibit time-varying behavior by combining it with the results from the previous section—we give further details in Remark V.5.

Remark V.1. Within this section, we explicitly specify the domains of the summations over $\bar{c} \hat{c}$ to ensure that all terms in the calculations are well defined—in particular, note that all terms of the form $D_\alpha(\rho_{QQ' \wedge \bar{c} \hat{c}} \| \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}})$ that appear in our later formulas are well defined because we restrict the sums to terms where the first argument has nonzero trace. In principle, as noted below Definition IV.1, we could instead assign arbitrary (finite) values to all $D_\alpha(\rho_{QQ' \wedge \bar{c} \hat{c}} \| \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}})$ terms with $\rho(\bar{c} \hat{c}) = 0$ and still carry out basically the same calculations, which would yield similar results except with the summations over the whole of $\bar{\mathcal{C}} \times \hat{\mathcal{C}}$ instead—those results would still be valid due to other properties of the formulas; for instance, in Eq. (106), the $D(\lambda \| \rho_{\bar{c} \hat{c}})$ term ensures that the value of the sum over $\bar{c} \hat{c}$ only affects the value of $G_{\alpha, \rho}^*(\lambda)$ in cases where $\lambda(\bar{c} \hat{c}) = 0$ whenever $\rho(\bar{c} \hat{c}) = 0$. However, we find it

cleaner to simply restrict the summation domain rather than constantly clarify these technicalities.

We first focus on presenting our main results in Sec. VA and discussing their applications in Sec. VB, with the proofs being deferred to Sec. VC and Appendix B.

A. Main results

To begin, we note that in the subsequent discussions, we will often discuss the set of all *mixtures* of possible output states from some set of channels, rather than just the output states of any individual channel. It is hence convenient to introduce a concise term for this concept, as follows. Note that the embedding condition is mainly just a technicality to ensure there is a well-defined notion of taking mixtures of output states from different channels.

Definition V.1. (Convex range) Let $\{\mathcal{E}_j\}_{j=1}^n$ be any set of channels $\mathcal{E}_j: \tilde{Q}_j \rightarrow Q'_j Q''_j \dots$ (for some finite set of output registers $Q'_j, Q''_j, \dots$), such that the registers Q'_j (respectively, $Q''_j, \dots$) can all be embedded in a common register Q' (respectively, $Q'', \dots$). The convex range of these channels [49] simply refers to the set of all mixtures of states of the form $\mathcal{E}_j[\omega]$ for some j and some $\omega \in S_=(\tilde{Q}_j)$, interpreting the mixtures as taking place in the embedding spaces.

In scenarios where all the channels $\mathcal{E}_j$ are isomorphic to each other (for instance, as was the case for the channels used to describe device-dependent EB-QKD in Ref. [1]), the convex range of the channels can simply be taken to be the range of any one of the channels and is hence simple to describe. More generally, in many applications of entropy accumulation results, the single-round analysis is often “indifferent” to which specific channel in the sequence is being considered, treating them all in basically the same way [50]. In many such cases, the single-round analysis already implicitly analyzes the convex range of all the channels since in each round an adversary could be applying some mixture of attack strategies. Hence, most existing methods for analyzing single rounds in a protocol should also immediately generalize to the convex range; for instance, this is indeed the case for the analysis of device-dependent PM-QKD and EB-QKD using the GEAT in Ref. [21], as well as the analysis of device-independent QKD in Ref. [29]. (Previous versions of this work were based on the concept of a “rate-bounding channel,” which is arguably slightly more flexible but a bit more technical—for completeness, we discuss this case further in Appendix D, together with a technical error in a claim regarding such channels in a previous version.)

We now turn to the main result of this section. Note that from a technical standpoint, our current proof of this result explicitly relies on our background assumption in this work that all registers are finite dimensional [51] (in particular, $\tilde{Q}$), but for completeness, in Remark C.1 of Appendix C, we also discuss an alternative formulation that removes this assumption in part of the proof by imposing additional

conditions on S_Ω (which should be easily satisfied in practice).

Theorem V.1. Let ρ be a state generated by a sequence of GEATT channels $\{\mathcal{M}_j\}_{j=1}^n$ (Definition III.2). Take any $\alpha \in (1, 2)$, and let $\hat{\alpha} = 1/(2 - \alpha)$. Furthermore, suppose that $\rho = p_\Omega \rho|_\Omega + (1 - p_\Omega) \rho|_{\bar{\Omega}}$ for some $p_\Omega \in (0, 1]$ and normalized states $\rho|_\Omega, \rho|_{\bar{\Omega}}$. Let S_Ω be a convex set of probability distributions on the alphabet $\bar{C} \times \hat{C}$, such that for all $\bar{c}_1^n \hat{c}_1^n$ with nonzero probability in $\rho|_\Omega$, the frequency distribution $\text{freq}_{\bar{c}_1^n \hat{c}_1^n}$ lies in S_Ω . Then, letting $\sigma_{\bar{C}\hat{C}}$ denote the distribution on $\bar{C}\hat{C}$ induced by any state $\sigma_{\bar{C}\hat{C}}$, we have

$$\begin{aligned} & H_\alpha^\dagger(S_\Omega^n | \bar{C}_1^n \hat{C}_1^n E_n)_{\rho|_\Omega} \\ & \geq n h_{\hat{\alpha}} - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_\Omega}, \end{aligned}$$

where

$$\begin{aligned} h_{\hat{\alpha}} = & \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}) \right. \\ & \left. - \sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{C}\hat{C}})} q(\bar{c}\hat{c}) D_{\hat{\alpha}}(\nu_{SE\bar{E}\wedge\bar{c}\hat{c}} \| \mathbb{I}_S \otimes \nu_{E\bar{E}\wedge\hat{c}}) \right), \end{aligned} \quad (78)$$

where Σ denotes the convex range (Definition V.1) of the channels $\{\mathcal{M}_j \otimes \text{id}_{\bar{E}}\}_{j=1}^n$, with $\bar{E}$ being a register of large enough dimension to serve as a purifying register for any of the $R_j E_j$ registers.

Furthermore, if there exists some channel $\mathcal{M}: \tilde{Q} \rightarrow SE\bar{C}\hat{C}$ such that Σ is equal to the set of output states of $\mathcal{M} \otimes \text{id}_{\bar{E}}$ (i.e., $\{\mathcal{M}[\omega_{\tilde{Q}\bar{E}}] | \omega \in S_=(\tilde{Q}\bar{E})\}$), then for any purifying function Pur for $\tilde{Q}$ onto $\bar{E}$ (Definition III.3), we have

$$\begin{aligned} h_{\hat{\alpha}} = & \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\tilde{Q})} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}^\omega) \right. \\ & \left. - \sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{C}\hat{C}}^\omega)} q(\bar{c}\hat{c}) D_{\hat{\alpha}}(\nu_{SE\bar{E}\wedge\bar{c}\hat{c}}^\omega \| \mathbb{I}_S \otimes \nu_{E\bar{E}\wedge\hat{c}}^\omega) \right), \end{aligned}$$

where $\nu^\omega := \mathcal{M}[\text{Pur}(\omega_{\tilde{Q}})]$, (79)

and the objective function in the above infimum is jointly convex in ω and $\mathbf{q}$.

Note that the condition on S_Ω is basically just the simple statement that S_Ω contains all frequency distributions on $\bar{C}_1^n \hat{C}_1^n$ “compatible with” Ω (viewing Ω as an event, e.g., by extending the state ρ with a register on which Ω is defined, if necessary). While it is true that the convexity requirement is not necessarily fulfilled “by default” in various applications, in many circumstances we can reasonably choose S_Ω such that it holds (e.g., by taking the convex hull). Still, if this choice is not possible, then one can use Corollary V.1 (combined with Lemma V.4 and the discussion below it) as

an alternative to Theorem V.1, albeit a more complicated one. We also note that it is indeed always possible, in principle, to construct a valid channel $\mathcal{M}$ for the bound in Eq. (79); we defer this explicit construction to Lemma D.1 in Appendix D.

As discussed in the Introduction, the bound in Eq. (78) means that, for any $\alpha \in (1, 2)$, we have obtained a simple $\Theta(n)$ lower bound on $H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}}$, with an explicit first-order constant $h_{\hat{\alpha}}$ that can be computed as a convex optimization via Eq. (79). To obtain an intuitive interpretation of this constant $h_{\hat{\alpha}}$, as we discuss in the next section, we can consider either of the following simplified lower bounds (proven in Appendix B), which replace the Rényi divergences with some Rényi conditional entropies:

Lemma V.1. In Theorem V.1, the following bound holds on $h_{\hat{\alpha}}$:

$$\begin{aligned} h_{\hat{\alpha}} &\geq \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}) \right. \\ &\quad \left. + \sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{C}\hat{C}})} q(\bar{c}\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{|\bar{c}\hat{c}}} \right) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\bar{Q})} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}^\omega) \right. \\ &\quad \left. + \sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{C}\hat{C}}^\omega)} q(\bar{c}\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{|\bar{c}\hat{c}}^\omega} \right), \end{aligned} \quad (80)$$

and the objective function in the second line is jointly convex in ω and $\mathbf{q}$. If the $\bar{C}$ register is trivial, then the above bound becomes an equality; i.e., we have

$$\begin{aligned} h_{\hat{\alpha}} &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\hat{C}}) \right. \\ &\quad \left. + \sum_{\hat{c} \in \text{supp}(\nu_{\hat{C}})} q(\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{|\hat{c}}} \right) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\bar{Q})} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\hat{C}}^\omega) \right. \\ &\quad \left. + \sum_{\hat{c} \in \text{supp}(\nu_{\hat{C}}^\omega)} q(\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{|\hat{c}}^\omega} \right). \end{aligned} \quad (81)$$

Lemma V.2. In Theorem V.1, the following bound holds on $h_{\hat{\alpha}}$, for any $\alpha', \alpha'' \in (1, \infty)$ such that $[\hat{\alpha}/(\hat{\alpha} - 1)] = [\alpha'/(\alpha' - 1)] + [\alpha''/(\alpha'' - 1)]$:

$$\begin{aligned} h_{\hat{\alpha}} &\geq \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} \left(\frac{\alpha''}{\alpha'' - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}) + H_{\alpha'}(S\bar{C} | \hat{C}E\tilde{E})_\nu \right) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\bar{Q})} \left(\frac{\alpha''}{\alpha'' - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}^\omega) + H_{\alpha'}(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega} \right), \end{aligned} \quad (82)$$

and the objective function in the second line is jointly convex in ω and $\mathbf{q}$.

B. Understanding and applying the bounds

We now present some intuitive interpretations of the bounds on the single-round term $h_{\hat{\alpha}}$ in Lemmas V.1 and V.2 (or the term $h_\alpha^\dagger$ in Corollary I.1 or Theorem VI.1), along with many details relevant for applications. The bound in Lemma V.2 has a slightly simpler form, so we shall discuss it first to gain the desired intuition (however, it has worse Rényi parameters—we stress that it would likely be better to instead use Lemma V.1 or Theorem VI.1 for device-dependent protocols, but we defer a discussion of this point until after we have explained the basic intuition).

To begin, first recall that, as discussed in the Introduction, we can interpret the optimization in Eq. (82) for $h_{\hat{\alpha}}$ in Lemma V.2 as just a relaxation of the “simplistic” optimization

$$\begin{aligned} &\inf_{\omega \in S_=(\bar{Q})} H_{\alpha'}(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega} \\ &\text{s.t. } \nu_{\bar{C}\hat{C}}^\omega \in S_\Omega, \end{aligned} \quad (83)$$

i.e., computing the worst-case entropy $H_{\alpha'}(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega}$ over *exactly* the states ω that produce a distribution contained in S_Ω . Hence, the value of $h_{\hat{\alpha}}$ would be lower than this “simplistic” optimization; however, it has already rigorously accounted for finite-size and non-IID effects.

We remark that for a theoretical analysis, it may also be convenient to rewrite $h_{\hat{\alpha}}$ as follows:

$$\inf_{\omega \in S_=(\bar{Q})} \left(H_{\alpha'}(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega} + \inf_{\mathbf{q} \in S_\Omega} \frac{\alpha''}{\alpha'' - 1} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}^\omega) \right), \quad (84)$$

since the $\inf_{\mathbf{q} \in S_\Omega} [\alpha''/(\alpha'' - 1)] D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}^\omega)$ term may have some useful properties—for instance, the optimizer $\mathbf{q}^*$ (if attained) is sometimes termed the information projection of $\nu_{\bar{C}\hat{C}}^\omega$ onto S_Ω , and it satisfies a form of triangle inequality. However, when applying computational methods such as those in Ref. [52], it should be easier to solve the joint optimization in Eq. (82) rather than the nested-optimization formulation in Eq. (84).

Comparing our results to the previous GEAT, our bound in Lemma V.2 should be much easier to evaluate in practice—the previous GEAT requires a technical construction of an *affine* “entropy-bounding function” (the min-tradeoff function [4]) on the space of probability distributions on $\bar{C}\hat{C}$, and optimizing the choice of min-tradeoff function while ensuring it is affine is often a challenging task [5]. In contrast, our bound only requires changing the objective function by an additional term $D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}^\omega)$, which is just a classical KL divergence and hence convex and

differentiable on the domain interior. Finally, we observe that one can straightforwardly avoid considering the full “fine-grained” distributions $\mathbf{q}, \nu_{\hat{C}\hat{C}}^\omega$ if they are too complicated—since the KL divergence satisfies data processing, *any* “coarse graining” of those distributions (formally, a stochastic map $\mathcal{E}$ on probability distributions on $\hat{C}\hat{C}$) still yields valid lower bounds by replacing $D(\mathbf{q} \parallel \nu_{\hat{C}\hat{C}}^\omega)$ with $D(\mathcal{E}[\mathbf{q}] \parallel \mathcal{E}[\nu_{\hat{C}\hat{C}}^\omega])$.

Remark V.2. We can also verify that $h_{\hat{a}}$ should be strictly positive in any “reasonable” protocol (with classical S , so all entropies of interest are non-negative), as follows. First, observe that any “reasonable” choice of S_Ω should be such that at least the “simplistic” optimization in Eq. (83) evaluates to some strictly positive value $h_\star > 0$ since otherwise we cannot expect a nontrivial rate [53]. In that case, the lower bound on $h_{\hat{a}}$ given by Eq. (82) would be strictly positive because, for any feasible point $(\mathbf{q}, \omega)$, we either have $\nu_{\hat{C}\hat{C}}^\omega \in S_\Omega$ and so $H_{\alpha'}(S\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} \geq h_\star > 0$ or $\nu_{\hat{C}\hat{C}}^\omega \notin S_\Omega$ and so $D(\mathbf{q} \parallel \nu_{\hat{C}\hat{C}}^\omega) > 0$ [54].

Another convenient property of the Lemma V.2 bound is that, with it, we can make use of single-round analysis methods that bound *any* particular Rényi entropy $H_{\alpha'}(S\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega}$, instead of having to focus on von Neumann entropy as in the original GEAT. For instance, we can straightforwardly “accumulate” min-entropy or collision entropy, as studied in, e.g., Refs. [15,56,57] (or Ref. [58] for the IID case). Hence, we obtain a variety of “fully Rényi” approaches for security proofs, at least as a proof of concept. However, note that, in practice, even if the single-round analysis only yields bounds for a specific Rényi parameter rather than arbitrary ones, one should usually still tune the choice of Rényi parameter when applying our results to obtain the best key rates—we defer a discussion of this point to Sec. VII C.

On that note though, it is not necessary to explicitly have single-round bounds on arbitrary Rényi entropies to apply our methods—it suffices to consider the usual von Neumann entropy, if desired. To see this case (and also verify that our bounds scale as expected at large n), first note that, if we write $\alpha' = 1 + \mu'$, $\alpha'' = 1 + \mu''$ in Lemma V.2 (for some $\mu', \mu'' > 0$), then we have

$$\begin{aligned}\hat{\alpha} &= 1 + \frac{1}{1 + \frac{1}{\mu'} + \frac{1}{\mu''}} = 1 + \frac{\mu'\mu''}{\mu'\mu'' + \mu' + \mu''}, \\ \alpha &= 1 + \frac{1}{2 + \frac{1}{\mu'} + \frac{1}{\mu''}} = 1 + \frac{\mu'\mu''}{2\mu'\mu'' + \mu' + \mu''},\end{aligned}\quad (85)$$

recalling that $\hat{\alpha} = 1/(2 - \alpha)$. In particular, if we take $\alpha', \alpha'' \rightarrow 1$, then $\hat{\alpha}, \alpha \rightarrow 1$ as well. Thus, we can describe our results in terms of more well-known entropies (von Neumann entropy and smooth min-entropy) using the same approach as Ref. [1], as follows.

Remark V.3. We highlight that for applications, since the subsequent bounds in Eqs. (86) and (87) are inequalities rather than equalities, it should be advantageous to avoid their use whenever possible (though in Sec. VII B, we show that we can still obtain rather good results even when using those bounds). In particular, it may be possible to use just one bound rather than both; for instance, Eq. (86) can be avoided if one can bound the single-round Rényi entropy directly, and Eq. (87) can be avoided if the security proof can use the recent Rényi privacy amplification theorem of Ref. [10] (which typically gives better finite-size key rates; see Ref. [5] or Sec. VII B for comparisons).

First, we can relate the single-round terms to von Neumann entropy via continuity bounds in α of the form

$$H_\alpha(S\bar{C}|\hat{C}E\tilde{E}) \geq H(S\bar{C}|\hat{C}E\tilde{E}) - g_{\text{cont}}(\alpha), \quad (86)$$

where $g_{\text{cont}}(\alpha)$ is a function that goes to 0 as $\alpha \rightarrow 1$. In a separate work (Appendix B of Ref. [11]), we derive explicit bounds on $g_{\text{cont}}(\alpha)$ that dramatically improve over previous such bounds in the context of optical QKD protocols. For this work, we just note that Lemma B.9 of Ref. [1] gives the somewhat loose bounds $g_{\text{cont}}(\alpha) \leq (\alpha - 1) \log^2(1 + 2 \dim(S\bar{C}))$ or, in some cases, [59] $g_{\text{cont}}(\alpha) \leq (\alpha - 1) \log^2(1 + 2 \dim(S))$, for α sufficiently close to 1. [Alternatively, Corollary IV.2 of Ref. [2] gives bounds of the form $(\alpha - 1)[(\ln 2)/2] \log^2(1 + 2 \dim(S\bar{C})) + O((\alpha - 1)^2)$ or $(\alpha - 1)[(\ln 2)/2] \log^2(1 + 2 \dim(S)) + O((\alpha - 1)^2)$ for classical S ; these bounds are tighter than Lemma B.9 of Ref. [1] for α close to 1. See Appendix B of Ref. [11] for further discussion.] Moreover, for the overall entropy, we can write Lemma B.10 of Ref. [1],

$$\begin{aligned}H_{\min}^\varepsilon(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n) &\geq H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n) - \frac{\vartheta_\varepsilon}{\alpha - 1}, \\ \text{where } \vartheta_\varepsilon &:= \log\left(\frac{1}{1 - \sqrt{1 - \varepsilon^2}}\right) \leq \log \frac{2}{\varepsilon^2},\end{aligned}\quad (87)$$

for any $\alpha \in (1, 2]$ and $\varepsilon \in (0, 1)$.

Substituting these two bounds in Eqs. (86) and (87) into Theorem V.1 with the Lemma V.2 bound, we obtain (for α', α'' sufficiently close to 1 to apply those two bounds)

$$\begin{aligned}H_{\min}^\varepsilon(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} &\geq \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_{\hat{C}}(\bar{Q})} \left(\frac{\alpha''}{\alpha'' - 1} D(\mathbf{q} \parallel \nu_{\hat{C}\hat{C}}^\omega) + H(S\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} \right) n \\ &\quad - g_{\text{cont}}(\alpha') n - \frac{\vartheta_\varepsilon}{\alpha - 1} - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_\Omega},\end{aligned}\quad (88)$$

where g_{cont} can be explicitly bounded as described below Eq. (86).

The above bound is the desired reformulation of our results in terms of the single-round von Neumann entropy and the n -round smooth min-entropy. If we choose [60] $\alpha', \alpha'' = 1 + \Theta(1/\sqrt{n})$, then we see from Eq. (85) that we have $\hat{\alpha}, \alpha = 1 + \Theta(1/\sqrt{n})$ as well, so the above bound simplifies [recalling $g_{\text{cont}}(\alpha) \leq \Theta(\alpha - 1)$] to

$$\begin{aligned} & H_{\min}^{\varepsilon}(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho_{\Omega}} \\ & \geq \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{-}(\tilde{Q})} (\Theta(\sqrt{n}) D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}^{\omega}) \\ & \quad + H(S\tilde{C} | \hat{C}E\tilde{E})_{\nu^{\omega}})n - \Theta(\sqrt{n}). \end{aligned} \quad (89)$$

Here, the $\Theta(\sqrt{n})$ finite-size correction term is the same scaling as we would obtain from the AEP in the IID case, and the first-order term is a relaxed optimization of the form we considered above (and it will again be nonzero for “reasonable” S_{Ω} , by the same arguments). Furthermore, since the “soft penalty term” $D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}^{\omega})$ has a prefactor of order $\Theta(\sqrt{n})$, we see that at large n , the optimization approaches what we would obtain by simply imposing the “hard constraint” $\nu_{\tilde{C}\hat{C}}^{\omega} \in S_{\Omega}$, so the bound in Eq. (89) asymptotically converges to what we expect.

A drawback of the Lemma V.2 bound is the change in Rényi parameters; specifically, if, for simplicity, [61] we set α' and α'' both equal to $1 + \mu$ for some small $\mu > 0$, then from Eq. (85) we find that $\hat{\alpha}, \alpha = 1 + \mu/2 + O(\mu^2)$ —i.e., the “distance from 1” for α and α' is roughly twice that of the original Rényi parameters $\hat{\alpha}$ and α . Loosely speaking, this “distance from 1” is one of the major contributions to losses from finite-size effects, so Lemma V.2 roughly doubles the effect of some such losses [for instance, it effectively halves the prefactor on the $D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}^{\omega})$ “penalty term,” and from Eq. (86) with Lemma B.9 of Ref. [1], we loosely expect it to double the distance from the von Neumann entropy, even if the bound in Eq. (86) is not explicitly used].

This issue can be avoided by using Lemma V.1 instead: In that bound, we preserve the Rényi parameter $\hat{\alpha}$ [which matches α up to order $O((\alpha - 1)^2)$, as discussed in Eq. (64)], at the price of a slightly more elaborate form for the conditional-entropy term, which instead takes the form of a linear combination $\sum_{\tilde{c}\hat{c}} q(\tilde{c}\hat{c}) H_{\hat{\alpha}}(S | E\tilde{E})$. Note that, as stated in the lemma, there is no loss of tightness when using this bound in applications where the $\tilde{C}$ register is trivial, which is the case for many device-dependent protocols [21]. While this linear combination might be slightly harder to handle than the single $H_{\alpha'}(S\tilde{C} | \hat{C}E\tilde{E})_{\nu^{\omega}}$ term, we note, for instance, that if S_{Ω} is such that it implies entrywise constraints $\mathbf{q} \geq \mathbf{q}^{\min}$ for some tuple $\mathbf{q}^{\min}$, then we could replace each $q(\tilde{c}\hat{c})$ factor in the linear combination (though not in the KL divergence term) with a constant

lower bound $q^{\min}(\tilde{c}\hat{c})$, which might be simpler to handle. As above, we also have the option of reformulating the bounds using either or both Eqs. (86) and (87) if desired, at the cost of the same potential suboptimality, yielding bounds such as

$$\begin{aligned} & H_{\min}^{\varepsilon}(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho_{\Omega}} \\ & \geq \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{-}(\tilde{Q})} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}^{\omega}) \right. \\ & \quad \left. + \sum_{\tilde{c}\hat{c} \in \text{supp}(\nu_{\tilde{C}\hat{C}}^{\omega})} q(\tilde{c}\hat{c}) H(S | E\tilde{E})_{\nu_{\tilde{c}\hat{c}}^{\omega}} \right) n \\ & \quad - g_{\text{cont}}(\hat{\alpha})n - \frac{\vartheta_{\varepsilon}}{\alpha - 1} - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_{\Omega}}, \end{aligned} \quad (90)$$

where g_{cont} can be explicitly bounded as described below Eq. (86). Note, however, that the objective function in this version potentially might not be jointly convex; see Sec. VB 2.

However, for device-independent protocols (where $\tilde{C}$ is usually not trivial), it is less clear whether Lemma V.1 or V.2 is better (of course, ideally one would obtain the tightest bound by directly computing the divergence-based formula in Theorem V.1, but that expression is more complicated). We discuss this point further in the next section, after first explaining the concept of infrequent-sampling channels.

Remark V.4. When using the above bounds (especially Lemma V.2), a point to keep in mind is that unlike the von Neumann entropy, the Rényi entropy for $\alpha > 1$ is not concave. Hence, for a state of the form $\nu = \sum_z p(z) \nu_{|z}$, in general, we would have $H_{\alpha}(S\tilde{C} | \hat{C}E\tilde{E})_{\nu} \not\geq \sum_z p(z) H_{\alpha}(S\tilde{C} | \hat{C}E\tilde{E})_{\nu_{|z}}$, and in fact, we cannot even say that it is lower bounded by $p(z) H_{\alpha}(S\tilde{C} | \hat{C}E\tilde{E})_{\nu_{|z}}$ for arbitrary z (unless we have additional properties of that z value). In particular, this result creates some inconveniences in analyzing infrequent-sampling channels (defined below) since it is harder to break up the entropy into test and generation “contributions.” However, in some situations, Fact II.2 can be used to work around this issue, possibly by introducing a conditioning register, if necessary, that “labels” the states in the mixture [note, however, that the resulting lower bounds would not simply be “linear” expressions like $\sum_z p(z) H_{\alpha}(S\tilde{C} | \hat{C}E\tilde{E})_{\nu_{|z}}$].

We now elaborate further on two other topics of importance for applications, namely, how to handle protocols with “infrequent sampling” and a caveat regarding the convexity of the various relaxed lower bounds we presented.

1. Infrequent-sampling channels

In most applications of entropy accumulation, $\mathcal{M}$ has the structure of an “infrequent-sampling channel” as defined in Ref. [2]:

Definition V.2. A channel $\mathcal{M}$ with some classical registers $\bar{C}\hat{C}$ in its output is said to be an infrequent-sampling channel if there is a constant test probability value $\gamma \in (0, 1)$ such that

$$\mathcal{M} = (1 - \gamma)\mathcal{M}^{\text{gen}} + \gamma\mathcal{M}^{\text{test}}, \quad (91)$$

for some generation and test channels $\mathcal{M}^{\text{gen}}$ and $\mathcal{M}^{\text{test}}$, where $\mathcal{M}^{\text{gen}}$ satisfies the property that it always sets $(\bar{C}, \hat{C}) = (\perp, \perp)$ for some special symbol $\perp$, while $\mathcal{M}^{\text{test}}$ never sets $(\bar{C}, \hat{C}) = (\perp, \perp)$.

Note that this channel structure is equivalent to saying that $\mathcal{M}^{\text{gen}}$ is implemented with probability $1 - \gamma$ and $\mathcal{M}^{\text{test}}$ with probability γ . With this interpretation, the term generation rounds (respectively, test rounds) is often used to refer to the rounds in which $\mathcal{M}_j^{\text{gen}}$ (respectively, $\mathcal{M}_j^{\text{test}}$) was implemented. We highlight that in Theorem V.1, if all the GEATT channels $\mathcal{M}_j$ are infrequent-sampling channels with the same γ , then their convex range also retains that structure, in the sense that every state in it has the form $(1 - \gamma)\nu^{\text{gen}} + \gamma\nu^{\text{test}}$, where $\nu_{\bar{C}\hat{C}}^{\text{gen}}(\perp, \perp) = 1$ and $\nu_{\bar{C}\hat{C}}^{\text{test}}(\perp, \perp) = 0$. In addition, we can always construct the channel $\mathcal{M}$ in that theorem such that it is an infrequent-sampling channel with the same γ , for instance, via Lemma D.1.

For infrequent-sampling channels, if we only keep the “generation component” in the linear combination of entropies, we obtain a simple lower bound whenever S is classical (so that the entropies are non-negative):

$$\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{C}\hat{C}}^\omega)} q(\bar{c}\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega} \geq q(\perp\perp) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\perp\perp}^\omega}. \quad (92)$$

Importantly, the above bound is an equality for any protocol in which S is set to some fixed trivial value in test rounds, or any protocol in which $\bar{C}$ or $\hat{C}$ contains a copy of S in test rounds (e.g., if the test-round data include the raw “fine-grained” data, instead of a “coarse-grained” version such as phase error rate or Clauser-Horne-Shimony-Holt (CHSH) winning frequency) since for such protocols we have $H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega} = 0$ for any $\bar{c}\hat{c}$ values other than $\perp\perp$. In particular, this is often the case in device-dependent protocols of practical interest [11], in order to simplify the public announcement structure. Recalling also that for such protocols the $\bar{C}$ register can usually be taken to be trivial [21]—so the Lemma V.1 bound is tight as well—we can conclude that, in such scenarios, we have the simpler formulation

$$h_{\hat{\alpha}} = \inf_{\mathbf{q} \in S_{\Omega} \omega \in S_{-}(\bar{Q})} \inf_{\omega \in S_{-}(\bar{Q})} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \parallel \nu_{\bar{C}\hat{C}}^\omega) + q(\perp) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\perp\perp}^\omega} \right), \quad (93)$$

with the objective function being jointly convex in $\mathbf{q}$ and ω . If needed, we could even further simplify it with the methods discussed above by replacing the $q(\perp)$ factor with some lower bound $q^{\min}(\perp)$ induced by S_{Ω} or converting to von Neumann entropy with Eq. (86).

A drawback of the Lemma V.1 bound is that for device-independent security proofs, the $\bar{C}$ register is usually not trivial [18,29,36,46]. Then, as mentioned above, if $\bar{C}$ contains a copy of S in test rounds, then Eq. (92) becomes an equality, which implies that in such scenarios, the Lemma V.1 bound loses all the “test-round entropy contributions” [62]. In DI security proofs, preserving these contributions in the entropy-accumulation part of the security proof usually yields slight improvements in the finite-size key rates [29,36], so the Lemma V.1 bound is suboptimal in that respect. One could retain these contributions by using Lemma V.2 instead, but as discussed above, the resulting loss in the Rényi parameters is non-trivial, roughly doubling some finite-size effects. The question of which lemma yields better results in a given scenario may have to be resolved on a case-by-case basis (as an initial impression, it seems likely that Lemma V.1 will be better in many cases due to the better Rényi parameters, *except* that if the test probability γ is large, it could be worse because the “lost” test-round contribution is larger in that case). We discuss this slightly further in Sec. VII C.

In summary, if we are considering a security proof where the $\bar{C}$ registers are trivial, then the Lemma V.1 bound is tight and should be simpler to analyze than Theorem V.1. Otherwise, in principle, one should use the divergence-based formulas in Theorem V.1 itself to obtain the best finite-size key rates, while Lemmas V.1 and V.2 should be considered as simpler but slightly suboptimal alternatives. In a companion work [63], we show that directly tackling the Theorem V.1 formula is possible in theory for some DI scenarios, by applying recently developed variational formulas for Rényi divergence (though the resulting SDPs become very large if we keep all the terms in the sum over $\bar{c}\hat{c}$).

For infrequent-sampling channels, we can also rewrite the $D(\mathbf{q} \parallel \nu_{\bar{C}\hat{C}}^\omega)$ term in various ways to more clearly highlight its dependencies on γ and improve numerical stability at small γ . In the first approach, ordering the distributions $\mathbf{q}$ and $\nu_{\bar{C}\hat{C}}^\omega$ such that the first component is the $\perp\perp$ probability, note that they can always be expressed in the form

$$\mathbf{q} = \begin{pmatrix} 1 - \gamma_q \\ \gamma_q \check{\mathbf{q}} \end{pmatrix}, \quad \nu_{\bar{C}\hat{C}}^\omega = \begin{pmatrix} 1 - \gamma \\ \gamma \check{\nu}_{\bar{C}\hat{C}}^\omega \end{pmatrix}, \quad (94)$$

where $\gamma_q := 1 - q(\perp\perp)$, and $\check{\mathbf{q}}$ and $\check{\nu}_{\bar{C}\hat{C}}^\omega$ are normalized distributions (computed by dropping the first components from $\mathbf{q}$ and $\nu_{\bar{C}\hat{C}}^\omega$ and then dividing by γ_q and γ , respectively).

Then, we can write an expression in which the dependency on γ_q and γ is made more explicit:

$$\begin{aligned}
D(\mathbf{q} \parallel \nu_{\bar{c}\hat{c}}^\omega) &= (1 - \gamma_q) \log \frac{1 - \gamma_q}{1 - \gamma} + \sum_{\bar{c}\hat{c} \neq \perp \perp} \gamma_q \check{q}(\bar{c}\hat{c}) \log \frac{\gamma_q \check{q}(\bar{c}\hat{c})}{\gamma \check{\nu}^\omega(\bar{c}\hat{c})} \\
&= (1 - \gamma_q) \log \frac{1 - \gamma_q}{1 - \gamma} + \gamma_q \log \frac{\gamma_q}{\gamma} + \gamma_q D(\check{\mathbf{q}} \parallel \check{\nu}_{\bar{c}\hat{c}}^\omega) \\
&= D(\mathbf{r} \parallel \mathbf{s}) + \gamma_q D(\check{\mathbf{q}} \parallel \check{\nu}_{\bar{c}\hat{c}}^\omega)
\end{aligned}$$

where $\mathbf{r} = \begin{pmatrix} 1 - \gamma_q \\ \gamma_q \end{pmatrix}$, $\mathbf{s} = \begin{pmatrix} 1 - \gamma \\ \gamma \end{pmatrix}$. (95)

However, this expression may still be inconvenient for numerical work because the relation between $\mathbf{q}$ and $\check{\mathbf{q}}$ is nonlinear, making it harder to convert the constraint $\mathbf{q} \in S_\Omega$ to a constraint on $\check{\mathbf{q}}$. For such applications, we instead recommend the following approach: Consider a new variable

$$\mathbf{t} := \begin{pmatrix} q(\perp \perp) \\ \frac{1}{\gamma} \mathbf{q}_{\setminus \perp \perp} \end{pmatrix}, \quad (96)$$

where $\mathbf{q}_{\setminus \perp \perp}$ simply means $\mathbf{q}$ with the $q(\perp \perp)$ component dropped. Thus, we can reparametrize $D(\mathbf{q} \parallel \nu_{\bar{c}\hat{c}}^\omega)$ in terms of $\mathbf{t}$ and the normalized distribution $\check{\nu}_{\bar{c}\hat{c}}^\omega$ from above:

$$\begin{aligned}
D(\mathbf{q} \parallel \nu_{\bar{c}\hat{c}}^\omega) &= t(\perp \perp) \log \frac{t(\perp \perp)}{1 - \gamma} + \gamma \sum_{\bar{c}\hat{c} \neq \perp \perp} t(\bar{c}\hat{c}) \log \frac{t(\bar{c}\hat{c})}{\check{\nu}^\omega(\bar{c}\hat{c})}. \quad (97)
\end{aligned}$$

Since $\mathbf{t}$ [respectively, $\check{\nu}^\omega(\bar{c}\hat{c})$] is an affine function of $\mathbf{q}$ [respectively, $\nu^\omega(\bar{c}\hat{c})$], this formulation automatically preserves all convexity properties, [64] and it is easy to convert the constraint $\mathbf{q} \in S_\Omega$ to a constraint that $\mathbf{t}$ is in some other convex set S'_Ω (basically, S_Ω with some components “rescaled”). This approach yields reparametrizations such as

$$\begin{aligned}
&\inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\bar{Q})} \left(\frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \parallel \nu_{\bar{c}\hat{c}}^\omega) + \sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} q(\bar{c}\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega} \right) \\
&= \inf_{\mathbf{t} \in S'_\Omega} \inf_{\omega \in S_=(\bar{Q})} \left(\frac{t(\perp \perp)}{\hat{\alpha} - 1} \log \frac{t(\perp \perp)}{1 - \gamma} + \frac{\gamma}{\hat{\alpha} - 1} \sum_{\bar{c}\hat{c} \neq \perp \perp} t(\bar{c}\hat{c}) \log \frac{t(\bar{c}\hat{c})}{\check{\nu}^\omega(\bar{c}\hat{c})} \right. \\
&\quad \left. + t(\perp \perp) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\perp \perp}^\omega} + \gamma \sum_{\bar{c}\hat{c} \neq \perp \perp} t(\bar{c}\hat{c}) H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega} \right). \quad (98)
\end{aligned}$$

This convex optimization should be more numerically stable at small γ because all components in $\mathbf{t}$ and $\check{\nu}^\omega(\bar{c}\hat{c})$ have comparable orders of magnitude, independent of γ (apart from an “indirect” dependency in that their optimal values change as γ changes).

The first expression in Eq. (95) has the advantage of being more intuitive for theoretical analysis; for instance, it lets us verify that we can choose γ to scale the same way as described in Ref. [2]. Specifically, suppose, for simplicity, that $\mathbf{q} \in S_\Omega$ implies that $\gamma - \delta_\gamma \leq \gamma_q \leq \gamma + \delta'_\gamma$ and $\check{\mathbf{q}} \in \check{S}_\Omega$ for some constants δ_γ and δ'_γ and some set $\check{S}_\Omega$, so we can relax the infimum over $\mathbf{q} \in S_\Omega$ to an infimum over γ_q and $\check{\mathbf{q}}$ satisfying those constraints. In addition, we can drop the $D(\mathbf{r} \parallel \mathbf{s})$ term as it is non-negative. Then, we obtain bounds on smooth min-entropy of the form

$$\begin{aligned}
&H_{\min}^e(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}} \\
&\geq \inf_{\check{\mathbf{q}} \in \check{S}_\Omega} \inf_{\omega \in S_=(\bar{Q})} \left(\frac{\gamma - \delta_\gamma}{\hat{\alpha} - 1} D(\check{\mathbf{q}} \parallel \check{\nu}_{\bar{c}\hat{c}}^\omega) \right. \\
&\quad \left. + (1 - \gamma - \delta'_\gamma) H(S|E\tilde{E})_{\nu_{\perp \perp}^\omega} \right) n - (\hat{\alpha} - 1) \\
&\log^2(1 + 2 \dim(S\bar{C})) n - \frac{\theta_\epsilon}{\alpha - 1} - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_\Omega}. \quad (99)
\end{aligned}$$

If we now pick $\alpha = 1 + \Theta(\sqrt{\gamma/n})$ where the implied constants depend only on $\dim(S\bar{C})$, ϵ , and p_Ω , then we have $\hat{\alpha} = 1 + \Theta(\sqrt{\gamma/n})$ as well. Let us also suppose, for simplicity, that δ_γ and δ'_γ can be chosen such that [65] they become smaller than, say, $\gamma/2$ at sufficiently large n . Then, the above bound simplifies to

$$\begin{aligned}
& H_{\min}^e(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} \\
& \geq \inf_{\tilde{\mathbf{q}} \in \tilde{S}_\Omega} \inf_{\omega \in S_=(\tilde{Q})} \left((\gamma - \delta_\gamma) \Theta \left(\sqrt{\frac{n}{\gamma}} \right) D(\tilde{\mathbf{q}} \| \tilde{\nu}_{\tilde{C}\hat{C}}^\omega) \right. \\
& \quad \left. + (1 - \gamma - \delta'_\gamma) H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega} \right) n - \Theta(\sqrt{\gamma n}) - \Theta \left(\sqrt{\frac{n}{\gamma}} \right) \\
& \geq \inf_{\tilde{\mathbf{q}} \in \tilde{S}_\Omega} \inf_{\omega \in S_=(\tilde{Q})} (\Theta(\sqrt{\gamma n}) D(\tilde{\mathbf{q}} \| \tilde{\nu}_{\tilde{C}\hat{C}}^\omega) \\
& \quad + (1 - 1.5\gamma) H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega}) n - \Theta \left(\sqrt{\frac{n}{\gamma}} \right), \quad (100)
\end{aligned}$$

where the second inequality holds at sufficiently large n such that $\delta_\gamma, \delta'_\gamma < \gamma/2$, and we trivially upper bounded the $\Theta(\sqrt{\gamma n})$ term by $\Theta(\sqrt{n/\gamma})$. Thus, similarly to Ref. [2] we observe that if we pick the scaling of γ with n to be any function that goes to zero more slowly than $1/n$, then the $\Theta(\sqrt{n/\gamma})$ term grows more slowly than $\Theta(n)$; furthermore, the $\Theta(\sqrt{\gamma n})$ prefactor on the KL divergence “penalty” term will increase with n . Hence, for any such scaling of γ with n , we would have the same limiting behavior as the IID case:

$$\lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^e(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} \geq \inf_{\substack{\omega \in S_=(\tilde{Q}) \\ \text{s.t. } \tilde{\nu}^\omega \in \tilde{S}_\Omega}} H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega}. \quad (101)$$

Note that just as in Ref. [2], there are some technical issues if we take *exactly* $\gamma = k/n$ for some constant k (basically, the expected number of test rounds). In particular, this approach causes some difficulties with the assumption that $\delta_\gamma, \delta'_\gamma < \gamma/2$ at large n ; furthermore, even if that issue were resolved, we would end up with a slightly but strictly worse bound, similar to that observed in Ref. [2]:

$$\begin{aligned}
& \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^e(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} \\
& \geq \inf_{\tilde{\mathbf{q}} \in \tilde{S}_\Omega} \inf_{\omega \in S_=(\tilde{Q})} \left(\Theta(\sqrt{k}) D(\tilde{\mathbf{q}} \| \tilde{\nu}_{\tilde{C}\hat{C}}^\omega) + H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega} \right. \\
& \quad \left. - \Theta \left(\frac{1}{\sqrt{k}} \right) \right), \quad (102)
\end{aligned}$$

which could be arbitrarily close to Eq. (101) by picking large enough k but will not be equal to it.

2. Convexity of relaxed lower bounds

Note that while we have proven the convexity of various expressions in Theorem V.1 and Lemmas V.1 and V.2, these convexity properties might not be preserved when applying the lower bounds we described above. If such properties are required for numerical techniques to tackle the resulting optimizations, one would need to separately prove that

they hold, which may or may not be straightforward (while, in many cases, the objective functions are clearly convex in the individual variables, showing that *joint* convexity holds is more subtle). For instance, if we convert the Lemma V.1 bound to von Neumann entropy with Eq. (86) and keep only the “generation component” as in Eq. (92), we would need to consider the convexity of $q(\perp\perp)H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega}$ [66]. Note that the $H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega}$ term by itself is convex in ω by Remark IV.2 applied to the $\mathcal{M}^{\text{gen}}$ channel in Eq. (91) [a subtlety is that we need to use the fact that the test probability γ is a *fixed* constant in Eq. (91)], so if, e.g., we replace the $q(\perp\perp)$ term with some fixed lower bound $q^{\min}(\perp\perp)$ induced by S_Ω , we obtain a convex optimization.

However, the last replacement can potentially be avoided by a somewhat subtle argument. First, following the techniques in Ref. [52] for device-dependent QKD, one can construct CP linear maps $\mathcal{Z}$ and $\mathcal{G}$ determined by $\mathcal{M}^{\text{gen}}$, such that $H(S|E\tilde{E})_{\nu_{|\perp\perp}^\omega} = D(\mathcal{G}[\omega] \| \mathcal{Z} \circ \mathcal{G}[\omega])$ [67]. This is convex on the set of positive semidefinite (not necessarily normalized) ω by the convexity of Umegaki divergence under the definition in Eq. (16) we used—see Chapter 4.1.2, Property (IXb) in Ref. [30]. In addition, under that definition, we see that a “scale-invariance” property $D(\mathcal{G}[\omega/t] \| \mathcal{Z} \circ \mathcal{G}[\omega/t]) = D(\mathcal{G}[\omega] \| \mathcal{Z} \circ \mathcal{G}[\omega])$ holds for any $t > 0$ (recalling that $\mathcal{Z}$ and $\mathcal{G}$ are linear). We now use the fact that for any convex function $f(\omega)$, its perspective function $g(\omega, t) := tf(\omega/t)$ (for $t > 0$) is jointly convex in ω and t (see Chapter 3.2.6 of Ref. [26]). Therefore, if f is any convex function with a scale-invariance property $f(\omega/t) = f(\omega)$, we can see that $tf(\omega) = tf(\omega/t) = g(\omega, t)$ is jointly convex in ω and t . Hence, we conclude that $q(\perp\perp)D(\mathcal{G}[\omega] \| \mathcal{Z} \circ \mathcal{G}[\omega])$ is, in fact, jointly convex in $q(\perp\perp)$ and ω . On the other hand, it is less clear how to generalize this argument to a linear combination such as $\sum_{\tilde{c} \in \tilde{C}} q(\tilde{c} \hat{c}) H(S|E\tilde{E})_{\nu_{|\tilde{c}\hat{c}}^\omega}$; we leave this issue to be resolved in future work if necessary.

Similar considerations apply to the formula in Eq. (95) for the KL divergence term $D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}^\omega)$. However, as noted there, we again recommend that numerical work should be based on the formula in Eq. (97) instead, which automatically preserves all convexity properties.

C. Proof of Theorem V.1

We first derive a straightforward consequence of Corollary IV.1. This result may be of some use in its own right (note that it does not require the convexity condition on S_Ω in Theorem V.1), though it is more or less just a specialization of the Corollary IV.1 bound.

Corollary V.1. Consider the same conditions and notation as in Theorem V.1, except without requiring that S_Ω is convex. Then, for any QES f on $\tilde{C}\hat{C}$, we have

$$\begin{aligned}
H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} &\geq \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} (H_\alpha^f(S\bar{C} | \hat{C}E\tilde{E})_\nu + \mathbf{f} \cdot \mathbf{q})n - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&= \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\bar{Q})} (H_\alpha^f(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega} + \mathbf{f} \cdot \mathbf{q})n - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega},
\end{aligned} \tag{103}$$

where $\mathbf{f}$ denotes the function f viewed equivalently as a tuple in $\mathbb{R}^{|\bar{C} \times \hat{C}|}$. Furthermore, in the second line, $H_\alpha^f(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega}$ is convex in ω , and hence the objective function in the infimum is jointly convex in ω and $\mathbf{q}$.

Proof. Simply set all the QESs $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ in the Corollary IV.1 statement to be equal to f . Then, the bound in Eq. (76) becomes

$$\begin{aligned}
H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} &\geq \min_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} \sum_{j=1}^n (f(\bar{c}_j \hat{c}_j) + \inf_{\nu \in \Sigma_j} H_\alpha^f(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu) - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&= \min_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} \sum_{\bar{c} \hat{c} \in \bar{C} \times \hat{C}} f(\bar{c} \hat{c}) \text{freq}_{\bar{c}_1^n \hat{c}_1^n}(\bar{c} \hat{c})n + \sum_{j=1}^n \inf_{\nu \in \Sigma_j} H_\alpha^f(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&\geq \inf_{\mathbf{q} \in S_\Omega} \mathbf{f} \cdot \mathbf{q}n + \sum_{j=1}^n \inf_{\nu \in \Sigma_j} H_\alpha^f(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega} \\
&\geq \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} (H_\alpha^f(S\bar{C} | \hat{C}E\tilde{E})_\nu + \mathbf{f} \cdot \mathbf{q})n - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega},
\end{aligned} \tag{104}$$

where in the second line we rewrite the sum of $f(\bar{c}_j \hat{c}_j)$ values in terms of the frequency distribution $\text{freq}_{\bar{c}_1^n \hat{c}_1^n}$, the third line holds by expressing the minimization over $\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}$ as an minimization over its induced frequency distributions and then relaxing the domain to S_Ω (using the first condition on S_Ω), and the fourth line follows simply from the fact that every state $\nu \in \Sigma_j$ also lies in the convex range Σ by definition. (It may be worth noting that the third line is a valid bound even without introducing the convex range, so it may be of some potential use in contexts where the channels are not all basically the same, though, in that case, it also seems suboptimal to choose all the QESs equal.)

The second line in Eq. (103) follows straightforwardly from Lemma IV.8; from that lemma, we also know that $H_\alpha^f(S\bar{C} | \hat{C}E\tilde{E})_{\nu^\omega}$ is convex in ω as claimed since $\hat{\alpha} > 1$ given $\alpha > 1$. ■

Next, we derive a lemma that is an essential tool in the subsequent calculations. It is based on the concept of (Legendre-Fenchel) convex conjugates [26]:

Definition V.3. (Convex conjugate) For a function $F: D \rightarrow \mathbb{R} \cup \{-\infty, +\infty\}$ where D is a convex subset of $\mathbb{R}^k$, its convex conjugate is the function $F^*: \mathbb{R}^k \rightarrow \mathbb{R} \cup \{-\infty, +\infty\}$ given by

$$F^*(\mathbf{y}) := \sup_{\mathbf{x} \in D} (\mathbf{x} \cdot \mathbf{y} - F(\mathbf{x})). \tag{105}$$

Under this definition, we show the following result. The proof is a routine but somewhat lengthy calculation; we hence defer it to Appendix B.

Lemma V.3. Consider any $\alpha \in (1, \infty)$ and any $\rho \in S_=(Q Q' \bar{C} \hat{C})$ such that $\bar{C}$ and $\hat{C}$ are classical with alphabets $\bar{C}$ and $\hat{C}$. Then, letting $\mathbb{P}_{\bar{C} \hat{C}}$ denote the set of probability distributions on $\bar{C} \times \hat{C}$, the pair of functions $(G_{\alpha, \rho}, G_{\alpha, \rho}^*)$ on $\mathbb{R}^{|\bar{C} \times \hat{C}|}$ defined as

$$\begin{aligned}
G_{\alpha, \rho}(\mathbf{f}) &:= -H_\alpha^f(Q\bar{C} | \hat{C}Q')_\rho, \\
G_{\alpha, \rho}^*(\lambda) &:= \begin{cases} \frac{1}{\alpha-1} D(\lambda \| \rho_{\bar{C} \hat{C}}) - \sum_{\bar{c} \hat{c} \in \text{supp}(\rho_{\bar{C} \hat{C}})} \lambda(\bar{c} \hat{c}) D_\alpha(\rho_{Q Q' \wedge \bar{c} \hat{c}} \| \mathbb{I}_Q \otimes \rho_{Q' \wedge \bar{c} \hat{c}}) & \text{if } \lambda \in \mathbb{P}_{\bar{C} \hat{C}} \\ +\infty & \text{otherwise,} \end{cases}
\end{aligned} \tag{106}$$

are convex functions that are convex conjugates to each other, where in the $G_{\alpha, \rho}$ formula we recall that any tuple $\mathbf{f} \in \mathbb{R}^{|\bar{C} \times \hat{C}|}$ is equivalent to a QES on $\bar{C} \hat{C}$, and in the $G_{\alpha, \rho}^*$ formula, we recall that $\rho_{\bar{C} \hat{C}}$ denotes the distribution induced by ρ on $\bar{C} \hat{C}$ [68].

We now have the tools required to obtain Theorem V.1 by proving this final key lemma. Note that for this lemma to be nonvacuous, it is important that there indeed exists a channel $\mathcal{M}$ satisfying the required conditions so that we can define ν^ω as in Eq. (79). Hence, we again highlight that we can indeed give an explicit construction of this channel; see Lemma D.1.

Lemma V.4. Consider the same conditions and notation as in Corollary V.1. Let $r_{\hat{a}}(\mathbf{f})$ denote the value of the infimum in the second line of Eq. (103) as a function of the QES $\mathbf{f}$, i.e.,

$$r_{\hat{a}}(\mathbf{f}) := \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{-}(\tilde{Q})} (H_{\hat{a}}^f(S\tilde{C}|\hat{C}E\tilde{E})_{\nu^{\omega}} + \mathbf{f} \cdot \mathbf{q}). \quad (107)$$

Then, the optimization problem

$$\sup_{\mathbf{f}} r_{\hat{a}}(\mathbf{f}) \quad (108)$$

is the Lagrange dual problem [69] of the constrained optimization

$$\begin{aligned} & \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\lambda \in \mathbb{P}_{\tilde{C}\hat{C}}} \inf_{\omega \in S_{-}(\tilde{Q})} \left(\frac{1}{\hat{a} - 1} D(\lambda \| \nu_{\tilde{C}\hat{C}}^{\omega}) \right. \\ & \quad \left. - \sum_{\tilde{c}\hat{c} \in \text{supp}(\nu_{\tilde{C}\hat{C}}^{\omega})} \lambda(\tilde{c}\hat{c}) D_{\hat{a}}(\nu_{SE\tilde{E}\wedge\tilde{c}\hat{c}}^{\omega} \| \mathbb{I}_S \otimes \nu_{E\tilde{E}\wedge\hat{c}}^{\omega}) \right) \\ \text{s.t. } & \mathbf{q} - \lambda = \mathbf{0}, \end{aligned} \quad (109)$$

in which the objective function is jointly convex in λ and ω (and $\mathbf{q}$, trivially), with $\mathbb{P}_{\tilde{C}\hat{C}}$ denoting the set of probability distributions on $\tilde{C}\hat{C}$.

Furthermore, if S_{Ω} is convex, the values of Eqs. (108) and (109) are equal.

Before giving its proof, we present two critical consequences of this lemma. First, observe that the [70] best choice of f in Corollary V.1 is exactly the same thing as the optimal $\mathbf{f}$ in the optimization in Eq. (108). The above lemma gives us a method to find this $\mathbf{f}$, even in situations where S_{Ω} does not satisfy the convexity condition in Theorem V.1, by computing or approximating the optimal dual solution to Eq. (109) (see Refs. [5,11] for possible numerical approaches)—this approach can be used as a substitute for Theorem V.1 in such circumstances. [In addition, if the Rényi divergence terms in Eq. (109) are difficult to handle, then we can slightly relax the optimization using the steps in the subsequent Lemma V.1 and V.2 proofs to obtain versions with only Rényi conditional entropies; it seems reasonable to assume the dual solutions for such versions will not be far from the optimal f .] However, we must stress that in such a scenario, we do not have a guarantee that the values of the optimizations in Eqs. (108) and (109) are equal. Hence, it would be important to actually substitute the final choice of f into Corollary V.1 and compute the resulting value; it is *not* safe to assume we can obtain a valid lower bound simply by evaluating the optimization in Eq. (109) on its own. [Note that while weak duality [26] always holds for Lagrange dual problems, it would be the statement that Eq. (108) is a lower bound on Eq. (109), which is the wrong inequality direction for trying to lower bound $H_{\hat{a}}^{\uparrow}(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho_{\Omega}}$.]

The second important consequence is for the case where S_{Ω} is indeed convex because, in that case, it immediately yields the desired proof of Theorem V.1. Specifically, we simply need to optimize the Corollary V.1V.1 bound over all f , which gives

$$H_{\hat{a}}^{\uparrow}(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho_{\Omega}} \geq (\sup_{\mathbf{f}} r_{\hat{a}}(\mathbf{f}))n - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_{\Omega}}, \quad (110)$$

and set $h_{\hat{a}}$ equal to the value of the supremum over $\mathbf{f}$, i.e., precisely the value of the optimization in Eq. (108). Then, given S_{Ω} is convex, Lemma V.4 tells us that $h_{\hat{a}}$ is also equal to the value of the optimization in Eq. (109), i.e., basically that strong duality [26] holds (in the sense that the dual problems have the same value, though not necessarily in the sense that the optimum in either problem is obtained; we discuss this later at the end of the Lemma V.4 proof). By simply substituting the constraint in Eq. (109) into the objective, we see that it simplifies to the desired expression in Eq. (79) for $h_{\hat{a}}$, with the claimed convexity properties.

Technically, to complete the proof of Theorem V.1, there is one last step: showing that Eq. (79) matches the preceding expression in Eq. (78). This step is a straightforward data-processing argument, albeit slightly tedious. First, clearly the former is lower bounded by the latter since (for each $\mathbf{q}$) every feasible point $\omega_{\tilde{Q}}$ of the former yields a feasible point of the latter by setting $\nu = \nu^{\omega}$. For the reverse bound, take any feasible point $\nu \in \Sigma$ in Eq. (78), i.e., $\nu = \mathcal{M}[\omega_{\tilde{Q}\tilde{E}}]$ for some $\omega_{\tilde{Q}\tilde{E}}$. Then, the reduced state $\omega_{\tilde{Q}}$ is a feasible point of Eq. (79) with an objective value that is no larger, by a standard data-processing argument, as follows. Since $\text{Pur}(\omega_{\tilde{Q}})$ is a purification of $\omega_{\tilde{Q}}$, there exists some channel $\mathcal{E}$ on $\tilde{E}$ such that $\omega_{\tilde{Q}\tilde{E}} = \mathcal{E}[\text{Pur}(\omega_{\tilde{Q}})]$. This channel $\mathcal{E}$ commutes with $\mathcal{M}$, so by applying $\mathcal{M}$ on both sides, we see that $\nu = \mathcal{E}[\nu^{\omega}]$. Since $\mathcal{E}$ does not act on $\tilde{C}\hat{C}$, from this relation, we obtain $\nu_{\tilde{C}\hat{C}} = \nu_{\tilde{C}\hat{C}}^{\omega}$ (by tracing out everything other than $\tilde{C}\hat{C}$) and also $\nu_{\wedge\tilde{c}\hat{c}} = \mathcal{E}[\nu_{\wedge\tilde{c}\hat{c}}^{\omega}]$ (i.e., $\mathcal{E}$ commutes with taking partial trace on the $\tilde{C}\hat{C}$ registers). Therefore, we have $D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}) = D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}^{\omega})$, and also for any $\tilde{c}\hat{c} \in \text{supp}(\nu_{\tilde{C}\hat{C}})$, we have

$$\begin{aligned} & -D_{\hat{a}}(\nu_{SE\tilde{E}\wedge\tilde{c}\hat{c}} \| \mathbb{I}_S \otimes \nu_{E\tilde{E}\wedge\hat{c}}) \\ & = -D_{\hat{a}}(\mathcal{E}[\nu_{SE\tilde{E}\wedge\tilde{c}\hat{c}}^{\omega}] \| \mathbb{I}_S \otimes \mathcal{E}[\nu_{E\tilde{E}\wedge\hat{c}}^{\omega}]) \\ & \geq -D_{\hat{a}}(\nu_{SE\tilde{E}\wedge\tilde{c}\hat{c}}^{\omega} \| \mathbb{I}_S \otimes \nu_{E\tilde{E}\wedge\hat{c}}^{\omega}), \end{aligned} \quad (111)$$

by the data-processing property for Rényi divergences (Fact II.1), which yields the desired result.

We highlight that, in our above analysis proving Theorem V.1 from Corollary V.1 and Lemma V.4, everything is an *equality*; i.e., there is no loss of tightness in using Theorem V.1 (when S_{Ω} is convex) as compared to the Corollary V.1 bound optimized over all choices of f . Hence, there seems to be few remaining ways in which

Theorem V.1 could be sharpened; we return to this point in more detail in Sec. VII.

Remark V.5. Lemma V.4 also suggests heuristic procedures for choosing QESs to use in variable-length protocols as described in Sec. IV C. For instance, if we simply want to use the same QES f for every round, then it seems likely that the optimal dual solution to Eq. (109) (with S_Ω being a singleton set containing only the honest behavior or perhaps some δ neighborhood of it) should yield a good choice of f , though we do not attempt to prove this here. It also suggests an approach for the broader possibility of adaptive choices of QESs $f_{|\mathcal{C}_1^{j-1} \mathcal{C}_1^{j-1}}$ in the manner described in Sec. IV C. Specifically, for each j at which we want to “update” the QES choice, we could consider the preceding rounds and use them to compute a loose estimate $\mathbf{q}^{\text{est}}$ of the upcoming behavior of the device (via any suitable physical and/or statistical model); then, we could take $f_{|\mathcal{C}_1^{j-1} \mathcal{C}_1^{j-1}}$ to be the dual solution of the constrained optimization in Eq. (109), with S_Ω being the singleton set $\{\mathbf{q}^{\text{est}}\}$ (or some small δ neighborhood around it, perhaps chosen according to the number of remaining rounds). This idea is currently highly heuristic, and we do not have an analysis of whether it gives reasonable performance; however, it seems like a plausible approach in light of the properties we have derived above.

We now conclude by presenting the proof of Lemma V.4, which basically consists of a sequence of convex-analysis transformations.

Proof. Following Lemma V.3, we write $H_\alpha^f(S\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} = -G_{\alpha,\nu^\omega}(\mathbf{f})$ (identifying the registers Q and Q' in that lemma with S and $E\tilde{E}$ here, respectively). We can now rewrite $r_\alpha(\mathbf{f})$ as follows:

$$\begin{aligned} r_\alpha(\mathbf{f}) &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\tilde{Q})} (-G_{\alpha,\nu^\omega}(\mathbf{f}) + \mathbf{f} \cdot \mathbf{q}) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\omega \in S_=(\tilde{Q})} (-\sup_{\lambda \in \mathbb{P}_{\bar{C}\hat{C}}} (\lambda \cdot \mathbf{f} - G_{\alpha,\nu^\omega}^*(\lambda)) + \mathbf{f} \cdot \mathbf{q}) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\lambda \in \mathbb{P}_{\bar{C}\hat{C}}} \inf_{\omega \in S_=(\tilde{Q})} (G_{\alpha,\nu^\omega}^*(\lambda) + (\mathbf{q} - \lambda) \cdot \mathbf{f}), \quad (112) \end{aligned}$$

where in the second line we invoked Lemma V.3—specifically, the fact that G_{α,ν^ω} is itself the convex conjugate of G_{α,ν^ω}^* and the fact that G_{α,ν^ω}^* is infinite outside of $\mathbb{P}_{\bar{C}\hat{C}}$. Now, with the last line in this formula for $r_\alpha(\mathbf{f})$, by noting that the $G_{\alpha,\nu^\omega}^*(\lambda)$ term is entirely independent of $\mathbf{f}$ and filling in its definition in Eq. (106), we see that the maximization problem in Eq. (108) is precisely the Lagrange dual problem of the constrained optimization in Eq. (109), as claimed.

Turning to the case where S_Ω is convex, we basically want to prove that strong duality holds under that condition. First, recall that, as mentioned in Corollary V.1, the quantity $H_\alpha^f(S\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} = -G_{\alpha,\nu^\omega}(\mathbf{f})$ is convex in ω . Combined with the Legendre-conjugate formula in Eq. (B14),

this finding implies that $G_{\alpha,\nu^\omega}^*(\lambda)$ is jointly convex in λ and ω since it is a supremum over a family of functions $\lambda \cdot \mathbf{f} - G_{\alpha,\nu^\omega}(\mathbf{f})$ that are each jointly convex in λ and ω . Thus, the objective function in Eq. (109) is jointly convex in λ and ω (and $\mathbf{q}$, trivially), and the constraints are affine; therefore, we can apply strong duality theorems from convex optimization theory.

However, the well-known Slater condition does not exactly yield the result we claim here because it would require some strict-feasibility conditions on S_Ω [and there are further subtleties because the $D(\mathbf{q}||\nu_{\bar{C}\hat{C}}^\omega)$ term is sometimes infinite, which affects the definition of strict feasibility for ω]. To avoid this issue, we instead use the Clark-Duffin condition [55], which states that strong duality holds when the objective and constraints are continuous convex functions on a closed convex domain (in a normed [71] space) and the feasible set is bounded.

We first note that we can take the purifying function PUR to be continuous without loss of generality, [72] which implies that the mapping $\omega \rightarrow \nu^\omega$ is continuous since $\mathcal{M}$ is just a linear map. In turn, this implies $G_{\alpha,\nu^\omega}^*(\lambda)$ is continuous with respect to (λ, ω) [in an extended-real sense, accounting for the $D(\lambda||\nu_{\bar{C}\hat{C}}^\omega)$ term]. There is a subtlety regarding the $\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{C}\hat{C}}^\omega)} \lambda(\bar{c}\hat{c}) D_\alpha(\nu_{SE\tilde{E}\wedge\bar{c}\hat{c}}^\omega || \mathbb{I}_S \otimes \nu_{E\tilde{E}\wedge\bar{c}\hat{c}}^\omega)$ term: While we have previously shown that all terms in the sum are finite [which ensures each individual term is continuous in (λ, ω)], there might appear to be issues caused by the change of summation domain whenever $\text{supp}(\nu_{\bar{C}\hat{C}}^\omega)$ changes. To address this problem, we note that this change of support can only happen at points with $\nu_{\bar{C}\hat{C}}^\omega(\bar{c}\hat{c}) = 0$ for one or more $\bar{c}\hat{c}$; however, for such points, we either have that the corresponding $\lambda(\bar{c}\hat{c})$ terms are also zero (which ensures that the sum changes “continuously” at such points), or we have $D(\lambda||\nu_{\bar{C}\hat{C}}^\omega) = +\infty$ and thus $G_{\alpha,\nu^\omega}^*(\lambda) = +\infty$ (which suffices to ensure continuity in an extended-real sense) [73]. Now, since $G_{\alpha,\nu^\omega}^*(\lambda)$ is independent of $\mathbf{q}$, we trivially obtain continuity over all $(\mathbf{q}, \lambda, \omega) \in \mathbb{P}_{\bar{C}\hat{C}} \times \mathbb{P}_{\bar{C}\hat{C}} \times S_=(\tilde{Q})$ as well.

With this result in mind, we suppose S_Ω is closed, without loss of generality, because the objective and constraints in Eq. (109) [and similarly, the objective in the last line of Eq. (112)] are continuous over all $(\mathbf{q}, \lambda, \omega) \in \mathbb{P}_{\bar{C}\hat{C}} \times \mathbb{P}_{\bar{C}\hat{C}} \times S_=(\tilde{Q})$, which allows us to freely switch between an infimum over S_Ω and an infimum over its closure without changing any optimal values. Then, the optimization domain $S_\Omega \times \mathbb{P}_{\bar{C}\hat{C}} \times S_=(\tilde{Q})$ is a compact convex set (under the finite-dimensionality assumption), and the feasible set in Eq. (109) is certainly a bounded set as well since it is a subset of the domain. Now, we can finally apply the Clark-Duffin condition to state that strong duality holds, yielding the desired result.

In closing, we first note that instead of the Clark-Duffin condition, our above arguments could also allow us to apply Sion’s minimax theorem to exchange the optimizations in the last line of Eq. (112) (since the minimization

domain is compact, not just the feasible set), which yields the same final result. In fact, Sion's minimax theorem gives us a slightly more “direct” alternative proof that Eqs. (108) and (109) are equal (though this would forgo the claims regarding Lagrange duality, which might be useful for numerical algorithms):

$$\begin{aligned} \sup_{\mathbf{f}} r_{\hat{\alpha}}(\mathbf{f}) &= \sup_{\mathbf{f}} \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{=}(\hat{Q})} (-G_{\hat{\alpha}, \nu^{\omega}}(\mathbf{f}) + \mathbf{f} \cdot \mathbf{q}) \\ &= \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{=}(\hat{Q})} \sup_{\mathbf{f}} (-G_{\hat{\alpha}, \nu^{\omega}}(\mathbf{f}) + \mathbf{f} \cdot \mathbf{q}) \\ &= \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{=}(\hat{Q})} G_{\hat{\alpha}, \nu^{\omega}}^*(\mathbf{q}), \end{aligned} \quad (113)$$

where the second line follows from Sion's minimax theorem and the last line holds by the definition of convex conjugates. In addition, we highlight the fact that, while we have proven strong duality between the optimizations in Eqs. (108) and (109) in the sense that they have the same value, our above proof does not immediately yield more stringent versions of strong duality such as dual attainment because the Clark-Duffin condition (unlike Slater's condition) does not ensure dual attainment. In fact, from the geometric interpretation of Slater's condition [26], we can see that the dual might not genuinely be attained in some “boundary” scenarios. For instance, in the BB84 protocol we discuss later in Sec. VII B, if we choose the “threshold value” Q_{thresh} to be *exactly* zero when defining S_{Ω} in Eq. (132) (ignoring the practical issues with such an accept condition since, in that case, S_{Ω} consists only of a single point), then from the fact that the “rate bound” in Eq. (135) has an infinite derivative at $\nu_{\hat{C}}(1) = 0$, it can be argued that the corresponding dual is not attained. We leave a more extensive analysis of such aspects for future work, if it should become important.

Furthermore, while it is true that in our above proof we relied on the finite-dimensionality assumption (to claim that the domain is compact), we believe that this should be removable in at least some situations. In Appendix C, we present a modification of the above proof that “isolates” these dependencies to improve the prospect of removing them, as well as an alternative proof based on Slater's condition that does not require the finite-dimensionality assumption but instead requires additional (though easily satisfied) conditions on S_{Ω} . ■

The proofs of the simplified bounds in Lemmas V.1 and V.2 are very similar, except with some looser inequalities to obtain simpler results; we defer them to Appendix B.

VI. VARIANTS

A. Original EAT

In this section, we show that if we impose the Markov conditions from the original EAT in Ref. [1], we can (as expected) avoid the change of Rényi parameters $\alpha \rightarrow \hat{\alpha}$ arising from the GEAT, resulting in a bound that is

genuinely identical in form to the QEF chaining property in Ref. [18] (albeit still slightly generalized to allow an S register as discussed in Remark IV.1). Because of the relation in Eq. (64), this improvement in Rényi parameters is unlikely to make much difference if α is close to 1; however, it might perhaps be useful if for some reason the security proof necessarily involves α far from 1.

Strictly speaking, the original EAT, the QEF analysis, and the GEAT differ in a subtle technical fashion regarding the scope of their constraints: The original EAT imposes the Markov condition only on the final state, the QEF analysis imposes it over a class of models, and the GEAT imposes the NS condition at the level of the channels. Thus, it is slightly difficult to make a strict comparison between their conditions; however, it seems likely that the GEAT conditions are still the least restrictive in most applications. In presenting the following lemma, we simply use the original EAT and impose the Markov condition on the state rather than the channels.

Lemma VI.1. Let $\rho_{S_1^n T_1^n \bar{C}_1^n \hat{C}_1^n \hat{E}}$ be a state of the form $\rho = \mathcal{M}_n \circ \dots \circ \mathcal{M}_1[\omega_{R_0 \hat{E}}^0]$ for some initial state $\omega^0 \in S_{=}(R_0 \hat{E})$ and some channels $\mathcal{M}_j: R_{j-1} \rightarrow S_j T_j R_j \bar{C}_j \hat{C}_j$ such that the output registers $\bar{C}_j \hat{C}_j$ are always classical (for any input state). Suppose that for each j , ρ satisfies the Markov condition

$$I(S_1^{j-1} \bar{C}_1^{j-1}: T_j \hat{C}_j | T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_{\rho} = 0, \quad (114)$$

i.e., $S_1^{j-1} \bar{C}_1^{j-1} \leftrightarrow T_1^{j-1} \hat{C}_1^{j-1} \hat{E} \leftrightarrow T_j \hat{C}_j$ forms a Markov chain. Then, Theorems IV.1 and V.1, Corollaries IV.1 and V.1, and Lemmas V.1–V.4 all hold with the following minor modifications:

- (i) Replace $\hat{\alpha}$ with α throughout, and allow $\alpha \in (1, \infty)$ instead of $\alpha \in (1, 2)$.
- (ii) Omit the condition that $\{\mathcal{M}_j\}_{j=1}^n$ are GEAT channels.
- (iii) Replace the registers with suitable counterparts, e.g., $\mathbb{H}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n) \rightarrow \mathbb{H}(S_1^n \bar{C}_1^n | \hat{C}_1^n T_1^n \hat{E})$, $\mathbb{H}(S_j \bar{C}_j | \hat{C}_j E_j \hat{E}) \rightarrow \mathbb{H}(S_j \bar{C}_j | \hat{C}_j T_j \hat{E})$, $\mathbb{H}(S \bar{C} | \hat{C} E \hat{E}) \rightarrow \mathbb{H}(S \bar{C} | \hat{C} T \hat{E})$, and so on, where $\mathbb{H}$ denotes any type of entropy.

Proof. We construct new channels $\mathcal{N}_j$ the same way as the Theorem IV.1 proof, except that we also have them output an extra copy of $\hat{C}_j$ in a register $\hat{\hat{C}}_j$. Since the channels $\mathcal{M}_j$ in this case have the form $\mathcal{M}_j: R_{j-1} \rightarrow S_j T_j R_j \bar{C}_j \hat{C}_j$, we end up with channels $\mathcal{N}_j: R_{j-1} \bar{C}_1^{j-1} \hat{C}_1^{j-1} \rightarrow D_j \bar{C}_j S_j T_j \hat{\hat{C}}_j R_j \hat{C}_j \bar{C}_1^j$. Again writing $\rho = \mathcal{N}_n \circ \dots \circ \mathcal{N}_1[\omega^0]$, this is a state on registers $D_1^n S_1^n T_1^n \bar{C}_1^n \hat{\hat{C}}_1^n \bar{C}_1^n \hat{C}_1^n \hat{E}$ that is an extension of the state ρ in this lemma statement. We now show that the state produced by each channel $\mathcal{N}_j$ satisfies the following Markov condition:

$$I(S_1^{j-1} \bar{C}_1^{j-1} D_1^{j-1} : T_j \hat{C}_j | T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_\rho = 0. \quad (115)$$

For this purpose, we first use the chain rule for conditional mutual information (Proposition 7.7 of Ref. [74]) to obtain

$$\begin{aligned} & I(S_1^{j-1} \bar{C}_1^{j-1} D_1^{j-1} : T_j \hat{C}_j | T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_\rho \\ &= I(S_1^{j-1} \bar{C}_1^{j-1} D_1^{j-1} : T_j \hat{C}_j | T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_\rho \\ &= I(S_1^{j-1} \bar{C}_1^{j-1} : T_j \hat{C}_j | T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_\rho \\ &\quad + I(D_1^{j-1} : T_j \hat{C}_j | S_1^{j-1} \bar{C}_1^{j-1} T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_\rho \\ &= I(D_1^{j-1} : T_j \hat{C}_j | S_1^{j-1} \bar{C}_1^{j-1} T_1^{j-1} \hat{C}_1^{j-1} \hat{E})_\rho \\ &= 0, \end{aligned} \quad (116)$$

where the second line holds since $\bar{C}_1^{j-1} = \bar{C}_1^{j-1}$ and $\hat{C}_1^{j-1} = \hat{C}_1^{j-1}$. The third line is due to the chain rule for conditional mutual information, the fourth line follows from the Markov condition in Eq. (114), and the last line holds by noting that D_1^{j-1} is produced from $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$. Thus, we conclude that this extended ρ satisfies the Markov condition. We now apply Corollary 3.5 of Ref. [1] by identifying the registers $A_1 A_2 B_1 B_2 R$ in that corollary with the registers here as follows:

- (i) $A_1 \leftrightarrow D_1^{j-1} \bar{C}_1^{j-1} S_1^{j-1}$.
- (ii) $A_2 \leftrightarrow D_j \bar{C}_j S_j$.
- (iii) $B_1 \leftrightarrow \hat{C}_1^{j-1} T_1^{j-1} \hat{E}$.
- (iv) $B_2 \leftrightarrow \hat{C}_j T_j$.
- (v) $R \leftrightarrow R_{j-1} \bar{C}_1^j \hat{C}_1^j$.

With this identification, for each j , we obtain

$$\begin{aligned} & H_\alpha(D_1^j S_1^j \bar{C}_1^j | \hat{C}_1^j T_1^j \hat{E})_\rho \\ & \geq H_\alpha(D_1^{j-1} S_1^{j-1} \bar{C}_1^{j-1} | \hat{C}_1^{j-1} T_1^{j-1} \hat{E})_\rho \\ & \quad + \inf_{\nu' \in \Sigma_j'} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j T_j \hat{E})_{\nu'}. \end{aligned} \quad (117)$$

Applying this formula for every j , we obtain

$$\begin{aligned} & H_\alpha(D_1^j S_1^j \bar{C}_1^j | \hat{C}_1^j T_1^j \hat{E})_\rho \\ & \geq \sum_j \inf_{\nu' \in \Sigma_j'} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j T_j \hat{E})_{\nu'}. \end{aligned} \quad (118)$$

Recall that, by definition of $\mathcal{N}_j$, the state ν' contains registers $\bar{C}_1^j \hat{C}_1^j$ even though they do not appear in entropies in the above expression. Therefore, we can apply the same argument as the bound in Eq. (B6) in the Theorem IV.1 proof, lower bounding the $H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j T_j \hat{E})_{\nu'}$ term by conditioning on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ and taking the worst-case value. Moreover, since $\bar{C}_j$ and $\hat{C}_j$ are just copies of $\bar{C}_j$ and $\hat{C}_j$, respectively (in particular, $\bar{C}_1^n = \bar{C}_1^n$ and $\hat{C}_1^n = \hat{C}_1^n$), we arrive at

$$\begin{aligned} & H_\alpha(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n T_1^n \hat{E})_\rho \\ & \geq \sum_j \inf_{\nu' \in \Sigma_j'} \min_{\bar{C}_1^{j-1} \hat{C}_1^{j-1}} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j T_j \hat{E})_{\nu'_{|\bar{C}_1^{j-1} \hat{C}_1^{j-1}}}. \end{aligned} \quad (119)$$

Thus, we carry out the remainder of all the proofs in the same way since none of the subsequent steps requires the NS condition of GEATT channels. ■

B. Tensor-power channels

Here, we briefly summarize some results from Ref. [17] and then explain how our methods can be applied to their results. We begin by summarizing the original definition of f -weighted Rényi entropies, which were introduced in that work, based on $H_\alpha^\uparrow$ rather than H_α . (As mentioned in Remark IV.1, a QES is basically the same as what Ref. [17] calls a “tradeoff function,” up to a technicality about a “normalization” condition. We highlight that a tradeoff function in their terminology is not the same as a min-tradeoff function in the original EAT or GEAT, so those terms should not be conflated, though there are some analogies that can be drawn between them.) We also remark that, here, we extend the definition to cover the $\alpha = \infty$ case because, unlike the case of H_α^f entropies, this α value might potentially be useful in the following results, as they would then involve $H_\infty^\uparrow$ rather than H_∞ (the former is usually more well behaved).

Definition VI.1. ($H_\alpha^{\uparrow,f}$ entropies) Let $\rho \in \mathcal{S}_=(\hat{C} Q Q')$ be a state where $\hat{C}$ is classical with alphabet $\hat{C}$, and consider a QES on $\hat{C}$ as in Definition IV.1 (taking the $\bar{C}$ register in that definition to be trivial). Given such a QES f and a value $\alpha \in (0, 1) \cup (1, \infty)$, we define

$$H_\alpha^{\uparrow,f}(Q | \hat{C} Q')_\rho := \frac{\alpha}{1-\alpha} \log \left(\sum_{\hat{c}} \rho(\hat{c}) 2^{\frac{1-\alpha}{\alpha}(-f(\hat{c}) + H_\alpha^\uparrow(Q | Q')_{\rho_{|\hat{c}}})} \right), \quad (120)$$

where the sum is over all $\hat{c}$ values such that $\rho(\hat{c}) > 0$. We extend this definition to $\alpha = \infty$ by taking the $\alpha \rightarrow \infty$ limit, yielding

$$H_\infty^{\uparrow,f}(Q | \hat{C} Q')_\rho := -\log \left(\sum_{\hat{c}} \rho(\hat{c}) 2^{f(\hat{c}) - H_\infty^\uparrow(Q | Q')_{\rho_{|\hat{c}}}} \right). \quad (121)$$

Since for trivial $\bar{C}$ this solution matches our definition of H_α^f entropies, except based on $H_\alpha^\uparrow$ instead of H_α , we intuitively have the following straightforward relation, which may be of use in some situations (e.g., the applications of H_α^f entropies discussed in Sec. IV C 1):

Lemma VI.2. Let $\rho \in \mathcal{S}_=(\hat{C} Q Q')$ be a state where $\hat{C}$ is classical with alphabet $\hat{C}$, and take any $\alpha \in (0, 1) \cup (1, \infty)$. Then,

$$H_\alpha^{\uparrow,f}(Q | \hat{C} Q')_\rho \geq H_\alpha^f(Q | \hat{C} Q')_\rho. \quad (122)$$

Proof. Extend the state with a read-and-prepare channel as described in Lemma IV.1. Then, by analogous calculations [though simpler since we can just use Eq. (25) rather than Eq. (23); note also that we exploit the fact that $H_\alpha(D)_{\rho_{|\hat{c}}}} = H_\alpha^\dagger(D)_{\rho_{|\hat{c}}}]$, we obtain

$$H_\alpha^\dagger(DQ|\hat{C}Q')_\rho = M + H_\alpha^{\dagger,f}(Q|\hat{C}Q')_\rho. \quad (123)$$

Combining this solution with the existing result in Eq. (36) in that lemma and the general relation $H_\alpha^\dagger(DQ|\hat{C}Q')_\rho \geq H_\alpha(DQ|\hat{C}Q')_\rho$, we obtain the desired result. ■

As discussed in Eq. (3), for device-dependent PM-QKD or EB-QKD, we usually consider states of the form $\rho = \mathcal{M}^{\otimes n}[\omega^0]$ for some suitable channel $\mathcal{M}$, and the results in Ref. [17] were hence tailored towards such states. With this in mind, a key finding of Ref. [17] is the following critical result (basically, Theorem IV.1 in this work is a version of this result under the conditions of the GEAT instead), which can be viewed as an “exact reduction to IID.” We highlight that to obtain tight key-rate bounds from the source-replacement technique for generic PM protocols, one usually needs to impose a constraint on Alice’s reduced state in the resulting EB protocol (see, e.g., Refs. [5,20,21] for further discussion), which is why the results in Ref. [17] and our subsequent theorems involve statements regarding such constraints [75]—note that one can always obtain a statement without reduced-state constraints as a special case of these results, simply by setting $\tilde{A}$ to be trivial.

Fact VI.1. (Reference [17]) Consider any state of the form $\rho_{S_1^n \hat{C}_1^n T_1^n \hat{E}} = \mathcal{M}^{\otimes n}[\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0]$, for some channel $\mathcal{M}: \tilde{A}\tilde{B} \rightarrow S\hat{C}\hat{T}$ with classical $\hat{C}$ and some state $\omega^0 \in S_=(\tilde{A}_1^n \tilde{B}_1^n \tilde{E})$ satisfying $\omega_{\tilde{A}_1^n}^0 = \sigma_{\tilde{A}}^{\otimes n}$ for some fixed state $\sigma_{\tilde{A}}$. Let Σ denote the set of all states of the form $\mathcal{M}[\omega_{\tilde{A}\tilde{B}\tilde{E}}]$ for some initial state $\omega \in S_=(\tilde{A}\tilde{B}\tilde{E})$ satisfying $\omega_{\tilde{A}} = \sigma_{\tilde{A}}$, with $\tilde{E}$ being a purifying register for $\tilde{A}\tilde{B}$. Let f be any QES on $\hat{C}$ (Definition VI.1), and define the following QES on $\hat{C}_1^n$:

$$f_{\text{full}}(\hat{C}_1^n) := \sum_{j=1}^n f(\hat{c}_j). \quad (124)$$

Then, for any $\alpha \in (1, \infty]$, we have

$$H_\alpha^{\dagger,f_{\text{full}}}(S_1^n|\hat{C}_1^n T_1^n \hat{E})_\rho \geq n \inf_{\nu \in \Sigma} H_\alpha^{\dagger,f}(S|\hat{C}\tilde{T}\tilde{E})_\nu. \quad (125)$$

We now note that given the above fact, we can build on it using the methods in this work to obtain the following result:

Theorem VI.1. Consider any state of the form $\rho_{S_1^n \hat{C}_1^n T_1^n \hat{E}} = \mathcal{M}^{\otimes n}[\omega_{\tilde{A}_1^n \tilde{B}_1^n \tilde{E}}^0]$, for some channel $\mathcal{M}: \tilde{A}\tilde{B} \rightarrow S\hat{C}\hat{T}$ with classical $\hat{C}$ and some state $\omega^0 \in S_=(\tilde{A}_1^n \tilde{B}_1^n \tilde{E})$

satisfying $\omega_{\tilde{A}_1^n}^0 = \sigma_{\tilde{A}}^{\otimes n}$ for some fixed state $\sigma_{\tilde{A}}$. Let Σ denote the set of all states of the form $\mathcal{M}[\omega_{\tilde{A}\tilde{B}\tilde{E}}]$ for some initial state $\omega \in S_=(\tilde{A}\tilde{B}\tilde{E})$ satisfying $\omega_{\tilde{A}} = \sigma_{\tilde{A}}$, with $\tilde{E}$ being a purifying register for $\tilde{A}\tilde{B}$. Suppose, furthermore, that ρ is of the form $p_\Omega \rho_{|\Omega} + (1 - p_\Omega) \rho_{|\bar{\Omega}}$ for some $p_\Omega \in (0, 1]$ and normalized states $\rho_{|\Omega}, \rho_{|\bar{\Omega}}$, and let S_Ω be a convex set of probability distributions on the alphabet $\hat{C}$, such that for all $\hat{c}_1^n$ with nonzero probability in $\rho_{|\Omega}$, the frequency distribution $\text{freq}_{\hat{c}_1^n}$ lies in S_Ω . Let Pur be any purifying function for $\tilde{A}\tilde{B}$ onto $\tilde{E}$ (Definition III.3) and write $\nu^\omega := \mathcal{M}[\text{Pur}(\omega_{\tilde{A}\tilde{B}})]$ for any $\omega \in S_=(\tilde{A}\tilde{B})$. Then, the following bound holds for any $\alpha \in (1, \infty]$:

$$\begin{aligned} H_\alpha^\dagger(S_1^n|\hat{C}_1^n T_1^n \hat{E})_{\rho_\Omega} &\geq n h_\alpha^\dagger - \frac{\alpha}{\alpha-1} \log \frac{1}{p_\Omega}, \\ \text{where } h_\alpha^\dagger &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\nu \in \Sigma} \left(\frac{\alpha}{\alpha-1} D(\mathbf{q} \parallel \nu_{\hat{C}}) \right. \\ &\quad \left. + \sum_{\hat{c} \in \text{supp}(\nu_{\hat{C}})} q(\hat{c}) H_\alpha^\dagger(S|\tilde{T}\tilde{E})_{\nu_{|\hat{c}}} \right) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\substack{\omega \in S_=(\tilde{A}\tilde{B}) \\ \text{s.t. } \omega_{\tilde{A}} = \sigma_{\tilde{A}}}} \left(\frac{\alpha}{\alpha-1} D(\mathbf{q} \parallel \nu_{\hat{C}}^\omega) \right. \\ &\quad \left. + \sum_{\hat{c} \in \text{supp}(\nu_{\hat{C}}^\omega)} q(\hat{c}) H_\alpha^\dagger(S|\tilde{T}\tilde{E})_{\nu_{|\hat{c}}^\omega} \right), \end{aligned} \quad (126)$$

and the objective function in the last line is jointly convex in ω and $\mathbf{q}$. In the above, $\nu_{\hat{C}}$ and $\nu_{\hat{C}}^\omega$ denote the distributions on $\hat{C}$ induced by the states $\nu_{\hat{C}}$ and $\nu_{\hat{C}}^\omega$ [see Eq. (13)].

Just as in Theorem V.1, the set S_Ω in the above theorem is just a set containing all frequency distributions on $\hat{C}_1^n$ “compatible with” Ω , and the qualitative discussions in Sec. VB are applicable for understanding and computing the first-order term $h_\alpha^\dagger$ in the above bound.

Proof. Given that Fact VI.1 holds, the proof of Theorem VI.1 follows by exactly the same chain of arguments as the previous sections: By suitably extending the state with a read-and-prepare channel, from Fact VI.1, we obtain analogs of Corollary IV.1 and Corollary V.1 (except with $H_\alpha^{\dagger,f}$ rather than H_α^f in the single-round terms); then, we apply the convex-analysis transformations described in Sec. VC [except that, since now we work with $H_\alpha^{\dagger,f}$ entropies rather than H_α^f entropies, the “weights” in the log-mean-exponential follow Eq. (120) rather than Eq. (30), and hence we arrive at a prefactor of $[\alpha/(\alpha-1)]$ rather than $[1/(\alpha-1)]$ on the “penalty term” in $h_\alpha^\dagger$]. ■

Note that by similar reasoning as in Remark V.5, the dual of the optimization problem

$$\begin{aligned}
& \inf_{\mathbf{q} \in S_\Omega} \inf_{\lambda \in \mathbb{P}_{\hat{c}}} \inf_{\substack{\omega \in S_{\omega}(\hat{A} \hat{B}) \\ \text{s.t. } \omega_{\hat{A}} = \sigma_{\hat{A}}}} \left(\frac{\alpha}{\alpha - 1} D(\lambda \| \nu_{\hat{c}}^\omega) \right) \\
& + \sum_{\hat{c} \in \text{supp}(\nu_{\hat{c}}^\omega)} \lambda(\hat{c}) H_\alpha^\uparrow(S|T\tilde{E})_{\nu_{\hat{c}}^\omega} \\
& \text{s.t. } \mathbf{q} - \lambda = \mathbf{0},
\end{aligned} \tag{127}$$

for some suitable choice of S_Ω , should provide a good choice of QES in Fact VI.1 for variable-length protocols.

We can again reformulate the bounds using either or both Eqs. (86) and (87) if desired, at the cost of the same potential suboptimality discussed in Remark V.3. This process yields bounds such as

$$\begin{aligned}
& H_{\min}^e(S_1^n | \hat{C}_1^n T_1^n E_n)_{\rho_{|\Omega}} \\
& \geq \inf_{\mathbf{q} \in S_\Omega} \inf_{\substack{\omega \in S_{\omega}(\hat{A} \hat{B}) \\ \text{s.t. } \omega_{\hat{A}} = \sigma_{\hat{A}}}} \left(\frac{\alpha}{\alpha - 1} D(\mathbf{q} \| \nu_{\hat{c}}^\omega) \right) \\
& + \sum_{\hat{c} \in \text{supp}(\nu_{\hat{c}}^\omega)} q(\hat{c}) H(S|T\tilde{E})_{\nu_{\hat{c}}^\omega} n - g_{\text{cont}}(\alpha) n \\
& - \frac{\partial_\varepsilon}{\alpha - 1} - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_\Omega},
\end{aligned} \tag{128}$$

where g_{cont} can be explicitly bounded as described below Eq. (86), and we again have the same caveats regarding convexity as in Sec. V B 2. We also note that if (starting from Fact VI.1) instead of following the proof steps described above, we follow the proof steps in one of the various existing (G)EAT-with-testing proofs such as in Refs. [1,2,4,46], then we would obtain exactly the same formulas in the final bounds on $H_\alpha^\uparrow(S_1^n | \hat{C}_1^n T_1^n \hat{E})_{\rho_{|\Omega}}$ as those works. Thus, all (achievable) finite-size key rates computed using the previous GEAT or EAT bounds are, in fact, also valid under the Ref. [17] model, i.e., without the “single-signal interaction” structure previously required for the GEAT analysis.

One limitation of the results described in this section is that they require the same measurement channel $\mathcal{M}$ and reduced state $\sigma_{\hat{A}}$ in each round—a concern might be that, in practical implementations, the measurements could differ across rounds due to slight imperfections. To resolve this issue, we would like to generalize Fact VI.1 to a bound of the form

$$\begin{aligned}
& H_\alpha^{\uparrow, \text{full}}(S_1^n | \hat{C}_1^n T_1^n \hat{E})_{\mathcal{M}_1 \otimes \mathcal{M}_2 \otimes \dots \mathcal{M}_n [\omega^0]} \\
& \geq \sum_j \inf_{\nu \in \Sigma_j} H_\alpha^{\uparrow, \text{f}}(S_j | \hat{C}_j T_j \tilde{E})_\nu,
\end{aligned} \tag{129}$$

analogous to Theorem IV.1 but with reduced-state constraints. We address this possibility in a follow-up work, showing that such a bound indeed holds. It also allows us

to obtain better key rates in situations where we have *a priori* knowledge of how the behavior differs across rounds; moreover, via a further generalization to channels applied in sequence (rather than tensor products), we can even apply the various “adaptive” approaches described in Sec. IV C.

VII. TIGHTNESS OF BOUNDS AND NUMERICAL EXAMPLES

In this section, we only use heuristic numerical methods when evaluating the various minimizations that appear in, e.g., our lower bounds on $h_{\hat{a}}$. Thus, strictly speaking, our numerical results are not guaranteed to be certified lower bounds on the key rates. However, in all examples in this section, the minimizations we evaluate can be written using at most three optimization variables, and they are convex in all the individual variables; hence, we believe it is unlikely that we have significantly overestimated the true key rates.

A. Remaining steps for improvement

An interesting feature of our Theorem V.1 proof is that for S_Ω satisfying the theorem conditions and α close to 1, it seems there are not many steps that could be improved—almost all the bounds are nearly saturated (simultaneously) by IID states, except for the Lemma IV.9 bound and a “relaxation” from $\tilde{\Omega}$ to S_Ω . We explicitly list them in order: First, Theorem IV.1 is basically tight for IID states up to the “higher-order” change $\alpha \rightarrow \hat{\alpha}$, as discussed below the theorem statement (moreover, this change is, in fact, entirely avoided in all the variants presented in Sec. VI). Next, to obtain Corollary IV.1, the only important bounds we apply are [76] $H_\alpha^\uparrow \geq H_\alpha$ and Lemma IV.9; however, by a converse bound $H_{2-\frac{1}{\alpha}} \geq H_\alpha^\uparrow$ (Corollary 4 in Ref. [77]), we can conclude that the former is again basically tight up to a higher-order change in Rényi parameters [since $2 - (1/\alpha) = 1 + \mu + O(\mu^2)$ for $\alpha = 1 + \mu$]. We then simplified this to the Corollary V.1 bound by focusing on the special case where all QESs are the same in each round and relaxing the minimization over $\tilde{\Omega}$ to one over S_Ω ; there is perhaps some possibility that the former choice is not optimal, but there do not seem to be obviously better options for scenarios where all rounds are basically the same. Finally, recall that in proceeding from Corollary V.1 (optimized over f) to Theorem V.1, all the remaining steps hold with *equality* by Lemma V.4, so there is no loss of tightness there. (Though when applying our result in a security proof, perhaps there remains a question of how tight the Rényi privacy amplification theorem is. Still, this seems to be something of a distinct consideration, and we leave it for separate work.)

Hence, it seems the largest potential source of suboptimality might be Lemma IV.9 and possibly the relaxation from $\tilde{\Omega}$ to S_Ω . This finding is consistent with some

numerical observations we make in Remark VII.1, where it seems one obtains significantly better bounds when choosing the conditioning event to mostly only contain “typical sequences” produced in the IID case rather than a more coarse-grained version that includes other sequences [and hence worsens the value of $\max_{\tilde{c}_1^n \hat{c}_1^n \in \tilde{\Omega}} H_\alpha(D)_{\rho_{|\tilde{c}_1^n \hat{c}_1^n}}$]. However, we highlight that, for such a choice of conditioning event, Lemma IV.9 would only be “loose up to typicality” (in that it takes the worst-case value over the typical set rather than some sort of average-case value), which is still a fairly sharp bound, and it seems difficult to improve it much further in the presence of finite-size effects.

In light of this finding, we expect that Theorem V.1 should yield strictly better bounds than previous GEAT or EAT results, which can be more rigorously formalized with the following argument. First, note that if in Corollary V.1 we extend $\mathcal{M}$ with a read-and-prepare channel as described in Lemma IV.1 (for Rényi parameter $\hat{\alpha}$), we have

$$\begin{aligned} H_{\hat{\alpha}}^f(\bar{S}\bar{C}|\hat{C}\bar{E}\tilde{E})_\nu + \mathbf{f} \cdot \mathbf{q} \\ &= H_{\hat{\alpha}}(D\bar{S}\bar{C}|\hat{C}\bar{E}\tilde{E})_\nu - M + \mathbf{f} \cdot \mathbf{q} \\ &= H_{\hat{\alpha}}(D\bar{S}\bar{C}|\hat{C}\bar{E}\tilde{E})_\nu - \sum_{\bar{c}\hat{c} \in \bar{C} \times \hat{C}} H_{\hat{\alpha}}(D)_{\nu_{|\bar{c}\hat{c}}} q(\bar{c}\hat{c}) \\ &\geq H_{\hat{\alpha}}(D\bar{S}\bar{C}|\hat{C}\bar{E}\tilde{E})_\nu - \sum_{\bar{c}\hat{c} \in \bar{C} \times \hat{C}} H_{\hat{\alpha}}(D)_{\nu_{|\bar{c}\hat{c}}} q(\bar{c}\hat{c}), \end{aligned} \quad (130)$$

so the bound in that corollary is at least as good as

$$\begin{aligned} H_{\hat{\alpha}}^{\uparrow}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}} \\ &\geq \inf_{\mathbf{q} \in \mathcal{S}_{\Omega}} \inf_{\nu \in \Sigma} \left(H_{\hat{\alpha}}(D\bar{S}\bar{C}|\hat{C}\bar{E}\tilde{E})_\nu \right. \\ &\quad \left. - \sum_{\bar{c}\hat{c} \in \bar{C} \times \hat{C}} H_{\hat{\alpha}}(D)_{\nu_{|\bar{c}\hat{c}}} q(\bar{c}\hat{c}) \right) n - \frac{\alpha}{\alpha-1} \log \frac{1}{p_{\Omega}}. \end{aligned} \quad (131)$$

This bound is the same as a bound that appears in the middle of the GEAT-with-testing proof of Ref. [4] [specifically, Eq. (4.7) combined with the first two inequalities in step (iii) on the following page; here, we present the optimization domain with $\mathcal{S}_{\Omega}$ instead of an event Ω on $\bar{C}_1^n \hat{C}_1^n$, but this is just a slight generalization], apart from a technical issue that we have chosen the D register entropies in a slightly different fashion, which should not make a significant difference. However, recall that, in our proof of Theorem V.1, we showed that the bound in that theorem is *exactly equal* to the Corollary V.1 bound [which is slightly tighter than Eq. (131)] with the best choice of f . Therefore, the results in Ref. [4], which were obtained by proceeding onwards from Eq. (131) but with some further relaxations, should not yield a better bound than Theorem V.1. Analogous results hold for the EAT bounds derived in, e.g., Refs. [1,2,46].

B. BB84

As a preliminary example, we apply Theorem V.1 to derive key rates for an entanglement-based implementation of the BB84 protocol, as follows. In this protocol, the registers S_j store Alice’s “secret” data, and the registers $\hat{C}_j$ store “public” data from test rounds, similar to our above formulations; we design the protocol such that the $\bar{C}_j$ registers are trivial. Note that this is a “fully qubit” version of the BB84 protocol (in order to compare to Refs. [6,7], which studied the same protocol); i.e., Alice prepares single-qubit states in each round, and Bob performs single-qubit Pauli measurements—there are no photon losses or dark counts. We address more realistic optical BB84 protocols in a separate work, using techniques developed in Ref. [11].

Protocol 1. EB-BB84 protocol outline.

1. For each round $j \in \{1, 2, \dots, n\}$, perform the following steps:
 - 1.1 Alice and Bob each receive a qubit register. Then, via public communication, with probability $1 - \gamma$ (independently in each round), they jointly declare that the round is a generation round; otherwise, it is a test round. Alice also independently generates a uniformly random “symmetrization bit” $F_j \in \{0, 1\}$ and publicly announces it.
 - 1.2 If it is a generation round, they both measure in the Z basis, XOR their outcomes with F_j , and store the resulting values in registers S_j and $\tilde{S}_j$ for Alice and Bob, respectively. In addition, they jointly set $\hat{C}_j = \perp$.
 - 1.3 If it is a test round, they both measure in the X basis, XOR their outcomes with F_j and publicly announce the resulting values, and then jointly set $\hat{C}_j = 0$ if their outcomes matched and $\hat{C}_j = 1$ otherwise. In addition, Alice sets $S_j = 0$ and Bob sets $\tilde{S}_j = \text{test}$.
2. Perform an acceptance test, in which Alice and Bob abort if $\text{freq}_{\hat{C}_1^n}$ lies outside some predetermined set $\mathcal{S}_{\Omega}$.
3. Perform one-way error correction in which Alice sends Bob a bitstring of length λ_{EC} , which he uses, together with $\tilde{S}_1^n$, to produce a guess $\mathbf{S}^{\text{guess}}$ for Alice’s string S_1^n . Then, perform error verification, in which Alice sends Bob a 2-universal hash of S_1^n (together with the choice of hash function), who compares it with the hash of $\mathbf{S}^{\text{guess}}$ and aborts if they do not match.
4. If neither of the above steps aborted, produce final keys of length ℓ_{key} by performing privacy amplification, in which Alice chooses a 2-universal function $\{0, 1\}^n \rightarrow \{0, 1\}^{\ell_{\text{key}}}$ and publicly announces it, and then Alice and Bob apply it to S_1^n and $\mathbf{S}^{\text{guess}}$, respectively.

We defer to Refs. [6,21] for details on the error correction and privacy amplification steps. There are many modifications that can be made to the above outline (e.g., here, we have followed Sec. 3 of Ref. [6] and Protocol I of Ref. [7] and allowed Alice and Bob to jointly decide the

basis to measure in; however, for practical protocols, the parties may need to *independently* choose measurement bases, so the test or generation labeling is different; see Refs. [5,11]), but we do not pursue these details further for this example.

As our goal in this example is to provide some comparison to the results in Ref. [6] (and an improved finite-size analysis subsequently derived in Ref. [7]), we proceed in analogy to those works and choose some “QBER threshold” value Q_{thresh} ; then, we define the set S_Ω to be [78]

$$S_\Omega = \{\mathbf{q} \in \mathbb{P}_{\hat{c}} | q_{\hat{c}}(1) \leq \gamma Q_{\text{thresh}}\}. \quad (132)$$

Following those works, we do not include an in-depth analysis of the required honest QBER value such that the honest protocol accepts with high probability; we note, however, in Remark VII.1 that a careful analysis of this aspect can improve the key rates from our formulas for actual protocol implementations. Furthermore, following Refs. [6,7], we note that (without affecting any security properties of the protocol, only the probability that it aborts in the honest case), in the error-correction step, we can plausibly use the choice

$$\lambda_{\text{EC}} = \xi_{\text{EC}}(1 - \gamma)h_{\text{bin}}(Q_{\text{thresh}})n, \quad (133)$$

where $\xi_{\text{EC}} > 1$ is a heuristically chosen value (see Figs. 1 and 2 for specific choices) that describes the finite-size efficiency of the error-correction procedure, and the factor of $1 - \gamma$ accounts for the generation-round probability. [Strictly speaking, one could, in fact, use the better value $\lambda_{\text{EC}} = \xi_{\text{EC}}H(S_j|\tilde{S}_j)_{\text{hon}}n = \xi_{\text{EC}}(1 - \gamma)h_{\text{bin}}(Q_{\text{hon}})n$, where $H(S_j|\tilde{S}_j)_{\text{hon}}$ denotes the value in the *honest* implementation, rather than the threshold accept value; we avoid doing so for a fairer comparison to Refs. [6,7]. We also gloss over the subtlety that, here, $\tilde{S}_j$ is not a binary random variable since it is set to test with probability γ , so existing results for LDPCs may not immediately apply; besides, the above formula is an approximate heuristic.]

Remark VII.1. Some numerical experimenting indicates that if we consider that there should be some honest IID behavior of the protocol and S_Ω must be chosen to accept it with high probability, then we find a rough trend that Theorem V.1 seems to yield much tighter bounds if S_Ω is instead chosen to constrain *all* the entries of $\mathbf{q}$ in a small neighborhood of the honest behavior, i.e.,

$$S_\Omega = \{\mathbf{q} \in \mathbb{P}_{\hat{c}} | q_{\hat{c}}(\hat{c}) \in I_{\hat{c}} \ \forall \ \hat{c} \in \hat{\mathcal{C}}\}, \quad (134)$$

for some small intervals $I_{\hat{c}}$ [even after accounting for the fact that the resulting upper bound on $q_{\hat{c}}(1)$ must be looser than the single-term version in Eq. (132) to achieve the same bound on honest abort probability]. This finding seems related to the observation that Lemma IV.9 is

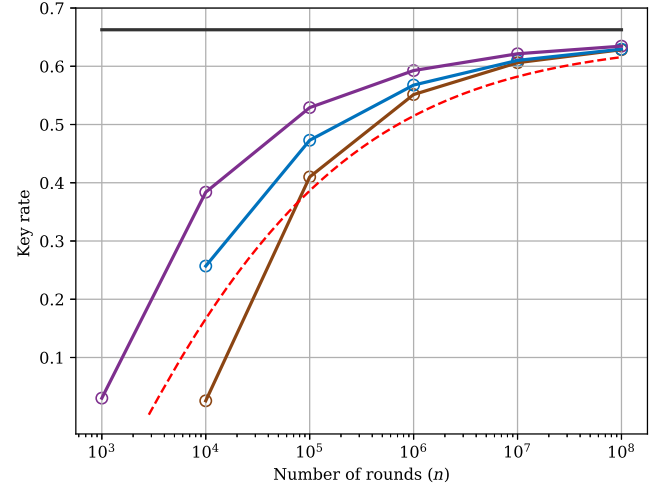


FIG. 1. Key rates for EB-BB84 from our approach, for an example with QBER threshold $Q_{\text{thresh}} = 0.025$, error-correction efficiency $\xi_{\text{EC}} = 1.1$, and security parameter $\epsilon^{\text{secure}} = 10^{-10}$. The brown, blue, and purple curves correspond to the key rates given by the formulas in Eqs. (138), (144), and (145), respectively, where we used heuristic numerical methods to evaluate the (fairly simple) minimizations in those formulas. For comparison, the dashed red curve is the corresponding result from Fig. 7 of Ref. [6] (based on smooth-entropy EURs), and the black horizontal line is the asymptotic rate. It can be seen that our results are always an improvement over that work, except for the case of the suboptimal formula in Eq. (138) at small n . We highlight that the formula in Eq. (144) already performs better everywhere despite also proceeding via a smooth min-entropy bound (instead of Rényi privacy amplification); i.e., we genuinely obtained a better bound on smooth min-entropy as compared to Ref. [6]. The choices of S_Ω , λ_{EC} , and epsilon parameters we used in our formulas are described in the main text. We roughly optimized the choices of γ and α by parametrizing them as $\gamma = 10^{-x}$ and $\alpha = 1 + 10^{-y}$ and then taking the best result computed in a grid of values over $x \in [0, 2.5]$ and $y \in [\log_{10} \sqrt{n} - 2, \log_{10} \sqrt{n} + 2]$ (the latter being motivated by the scaling analysis at the end of Sec. VB 1); we leave a more refined approach for future applications.

potentially the loosest step in our proof, and choosing S_Ω such that it only “captures” the typical IID sequences helps to reduce the value of $\max_{\hat{c}_1^n, \hat{c}_1^n \in \hat{\Omega}} H_\alpha(D)_{\rho_{|\hat{c}_1^n, \hat{c}_1^n}}$ there.

Furthermore, in such cases, we find that (denoting the desired bound on honest abort probability as ϵ^{com} , the completeness parameter) it usually seems better to choose the intervals $I_{\hat{c}}$ such that each term causes an abort with probability at most $\epsilon^{\text{com}}/3$ (i.e., we distribute the “abort-probability contributions” evenly) rather than using the same interval width for all terms. Note also that, while these intervals can be simply chosen using, e.g., the Chernoff bound, better results can be obtained by instead using the binomial-distribution analysis described in Refs. [11,46] (either by using built-in software functions that can evaluate binomial-distribution tail bounds or relaxing

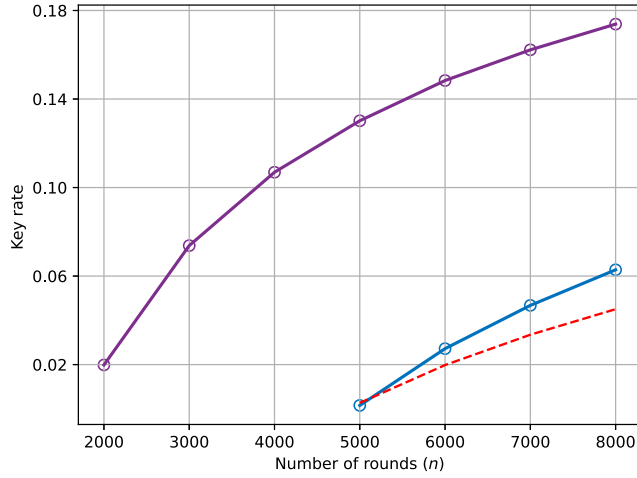


FIG. 2. Similar to Fig. 1, except that the parameter choices are $Q_{\text{thresh}} = 0.0451$, $\xi_{\text{EC}} = 1.19$, and $\epsilon^{\text{secure}} = 10^{-10}$, and the dashed red curve shows the corresponding data points from Ref. [7] instead (which improved the finite-size analysis in Ref. [6]). Here, there is no curve shown for our loosest bound in Eq. (138), as we could not obtain positive key rates from it for the n values in this range, consistent with the observation in Fig. 1 that it performs less well at very small n . These results suggest that our best bound on the smooth min-entropy itself [i.e., that used in Eq. (144)] is still better than Ref. [7] at most n values, though the advantage is not that large. However, in the end, we can achieve much higher actual key rates by instead using the fully Rényi formula in Eq. (145).

them to normal-distribution tail bounds as described in Ref. [46]).

For the above protocol, we can construct GEATT channels $\mathcal{M}_j$ in the fashion described in Ref. [21], with the E_j register in each round storing all the side information Eve collects and updates, including both her quantum side information and the public announcements from each round. These channels are infrequent-sampling channels with the same γ ; hence, we can construct a suitable infrequent-sampling channel $\mathcal{M}$ for use in Theorem V.1, as discussed below Definition V.2. For this channel $\mathcal{M}$, we can apply an EUR for von Neumann entropy [79] to lower bound $H(S|E\tilde{E})_{\nu_{\perp}}$ for any $\nu \in \Sigma$ (i.e., any state that could

be produced by $\mathcal{M} \otimes \text{id}_{\tilde{E}}$). Specifically, if we let $X, \tilde{X}$ denote registers that store Alice and Bob's symmetrized [80] X -measurement outcomes conditioned on $\hat{C} \neq \perp$ (i.e., we are in the “test” component of the infrequent-sampling channel), then

$$\begin{aligned} H(S|E\tilde{E})_{\nu_{\perp}} &\geq 1 - H(X|\tilde{X})_{\nu_{\hat{C} \neq \perp}} \\ &= 1 - h_{\text{bin}}(\Pr[X \neq \tilde{X}] | \hat{C} \neq \perp) \\ &= 1 - h_{\text{bin}}\left(\frac{\nu_{\hat{C}}(1)}{\gamma}\right), \end{aligned} \quad (135)$$

where $H(X|\tilde{X})_{\nu_{\hat{C} \neq \perp}} = h_{\text{bin}}(\Pr[X \neq \tilde{X}] | \hat{C} \neq \perp)$ holds because the marginal distributions of $X, \tilde{X}$ conditioned on $\hat{C} \neq \perp$ are uniform; in the last step, we recall that $\hat{C}$ is set to $\perp$ with probability $1 - \gamma$, and otherwise, it is set to 1 if and only if $X \neq \tilde{X}$. Combined with Lemma B.9 of Ref. [1], we find [note that, here, we have $\dim(S) = 2$ because we designed the protocol such that S is still bit valued even in a test round] $\forall \alpha \in \{1, 1 + (1/\log(5))\}$,

$$H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\perp}} \geq 1 - h_{\text{bin}}\left(\frac{\nu_{\hat{C}}(1)}{\gamma}\right) - (\hat{\alpha} - 1) \log^2(5). \quad (136)$$

Again, one could instead use Corollary IV.2 of Ref. [2] here for tighter but slightly more elaborate bounds; we omit this for ease of presentation.

Without loss of generality, we can assume that once the n measurement steps have been completed, Eve no longer acts on her register E_n (by replacing any operation she does afterwards with its Stinespring isometry). Let ρ denote the state produced in the protocol just before privacy amplification, and let Ω denote the event that both [82] the acceptance test and error verification accepted. Then, since S_{Ω} as defined in Eq. (132) is convex, we can apply Theorem V.1 together with Lemma V.1 and the bound in Eq. (92) for infrequent-sampling channels [which is tight for this protocol, i.e., the equality in Eq. (93) holds] to obtain

$$\begin{aligned} H_{\hat{\alpha}}^{\uparrow}(S_1^n | \hat{C}_1^n E_n)_{\rho_{\Omega}} &\geq \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\nu_{\hat{C}} \in \mathbb{P}_{\hat{C}}} \left(q(\perp) \left(1 - h_{\text{bin}}\left(\frac{\nu_{\hat{C}}(1)}{\gamma}\right) - (\hat{\alpha} - 1) \log^2(5) \right) + \frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \| \nu_{\hat{C}}) \right) n \\ &\quad - \frac{\alpha}{\alpha - 1} \log \frac{1}{p_{\Omega}}, \end{aligned} \quad (137)$$

where we have relaxed the optimization over $\nu \in \Sigma$ by noting that the bound in Eq. (136), in fact, only depends on the classical distribution $\nu_{\hat{C}}$. Note that since the domains of $\mathbf{q}$ and $\nu_{\hat{C}}$ enforce that they are normalized, and also the value of $\nu_{\hat{C}}(\perp)$ is fixed as $1 - \gamma$ by the infrequent-sampling structure, there are, in fact, only three independent variables in the above minimization.

Then, by applying Eq. (87) to convert the above bound to smooth min-entropy and following the proof structure in Ref. [21] or [11], one can show that, if we choose any values [83] $\varepsilon_s, \varepsilon_a, \varepsilon_{EV}, \varepsilon_{PA} \in (0, 1)$ and set

$$\begin{aligned} \ell_{\text{key}} = & \left[\inf_{\mathbf{q} \in S_\Omega} \inf_{\nu_{\hat{c}} \in \mathbb{P}_{\hat{c}}} \left(q(\perp) \left(1 - h_{\text{bin}} \left(\frac{\nu_{\hat{c}}(1)}{\gamma} \right) - (\hat{\alpha} - 1) \log^2 5 \right) + \frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \parallel \nu_{\hat{c}}) \right) n \right. \\ & \left. - \frac{\alpha}{\alpha - 1} \log \frac{1}{\varepsilon_a} - \frac{1}{\alpha - 1} \log \frac{2}{\varepsilon_s^2} - \lambda_{\text{EC}} - \left\lceil \log \frac{1}{\varepsilon_{EV}} \right\rceil - 2 \log \frac{1}{\varepsilon_{PA}} \right], \end{aligned} \quad (138)$$

the protocol will be $\varepsilon^{\text{secure}}$ -secure (see Refs. [6,21] for full definitions, or Ref. [84] under the term “soundness” instead) with [85]

$$\varepsilon^{\text{secure}} = \max \left\{ \frac{\varepsilon_{PA}}{2} + 2\varepsilon_s, \varepsilon_a \right\} + \varepsilon_{EV}. \quad (139)$$

Note that since the optimal choice of α in Eq. (138) is often close to 1, the effects of ε_a and ε_s in that bound are significantly larger than those of ε_{PA} and ε_{EV} . Hence, for our numerical calculations, given some desired value of $\varepsilon^{\text{secure}}$, we use the heuristic choice of setting

$$\begin{aligned} \varepsilon_{PA} &= \varepsilon_{EV} = \varepsilon_{\text{small}}, \\ \varepsilon_a &= \varepsilon^{\text{secure}} - \varepsilon_{\text{small}}, \\ \varepsilon_s &= \frac{1}{2} \left(\varepsilon^{\text{secure}} - \frac{3}{2} \varepsilon_{\text{small}} \right), \end{aligned} \quad (140)$$

where $\varepsilon_{\text{small}}$ is a parameter we choose to maximize ℓ_{key} . Specifically, substituting the above expressions into Eq. (138), given any fixed choice of α , we can find the best $\varepsilon_{\text{small}}$ by differentiating with respect to $\varepsilon_{\text{small}}$ (note that the infimum term is independent of $\varepsilon_{\text{small}}$ and can be entirely ignored for this purpose), which yields the explicit solution

$$\begin{aligned} \varepsilon_{\text{small}} &= \frac{8 + 17(\alpha - 1) - \sqrt{64 + 56(\alpha - 1) + (\alpha - 1)^2}}{2(9 + 12(\alpha - 1))} \varepsilon^{\text{secure}} \\ &\approx \frac{3}{4} (\alpha - 1) \varepsilon^{\text{secure}}. \end{aligned} \quad (141)$$

On the other hand, a tighter bound can be obtained by directly using EURs for Rényi entropies to bound $h_{\hat{\alpha}}$. Specifically, by using the fact that $H_{\hat{\alpha}} \geq H_{\frac{1}{2-\hat{\alpha}}}^{\uparrow}$ (Corollary 4 of Ref. [77]) and then applying the EUR from Theorem 11 of Ref. [32], we have

$$\begin{aligned} H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\perp}} &\geq H_{\frac{1}{2-\hat{\alpha}}}^{\uparrow}(S|E\tilde{E})_{\nu_{\perp}} \\ &\geq 1 - H_{\beta}^{\uparrow}(X|\tilde{X})_{\nu_{|\hat{c} \neq \perp}}, \end{aligned} \quad (142)$$

where $\beta = 1/\hat{\alpha}$. Note that if we write $\hat{\alpha} = 1 + \hat{\mu}$, then $\beta = 1/(1 + \hat{\mu}) = 1 - \hat{\mu} + O(\hat{\mu}^2)$. The $H_{\beta}^{\uparrow}(X|\tilde{X})_{\nu_{|\hat{c} \neq \perp}}$ term is a purely classical Rényi entropy and hence coincides with the entropy from Ref. [86]. Again, using the fact that the symmetrized bits X and $\tilde{X}$ have uniform marginal distributions, we can explicitly calculate

$$\begin{aligned} H_{\beta}^{\uparrow}(X|\tilde{X})_{\nu_{|\hat{c} \neq \perp}} &= \frac{\beta}{1-\beta} \log \left(\sum_{i=0}^1 \left(\sum_{j=0}^1 \left(\frac{\nu_{\hat{c}}(i \oplus j)}{2\gamma} \right)^{\beta} \right)^{1/\beta} \right) \\ &= \frac{1}{1-\beta} \log \left(\left(1 - \frac{\nu_{\hat{c}}(1)}{\gamma} \right)^{\beta} + \left(\frac{\nu_{\hat{c}}(1)}{\gamma} \right)^{\beta} \right). \end{aligned} \quad (143)$$

For α somewhat further away from 1, the above bound has an important advantage over the previous bound in Eq. (136) in that, as $\nu_{\hat{c}}(1) \rightarrow 0$, it converges towards the tight bound $H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\perp}} \geq 1$, unlike Eq. (136), which yields a lower bound that remains of the form $1 - \Theta(\hat{\alpha} - 1)$. With this bound, we conclude that the same security levels as described above can be achieved by instead setting

$$\begin{aligned} \ell_{\text{key}} = & \left[\inf_{\mathbf{q} \in S_\Omega} \inf_{\nu_{\hat{c}} \in \mathbb{P}_{\hat{c}}} \left(q(\perp) \left(1 - \frac{1}{1-\beta} \log \left(\left(1 - \frac{\nu_{\hat{c}}(1)}{\gamma} \right)^{\beta} + \left(\frac{\nu_{\hat{c}}(1)}{\gamma} \right)^{\beta} \right) \right) + \frac{1}{\hat{\alpha} - 1} D(\mathbf{q} \parallel \nu_{\hat{c}}) \right) n \right. \\ & \left. - \frac{\alpha}{\alpha - 1} \log \frac{1}{\varepsilon_a} - \frac{1}{\alpha - 1} \log \frac{2}{\varepsilon_s^2} - \lambda_{\text{EC}} - \left\lceil \log \frac{1}{\varepsilon_{EV}} \right\rceil - 2 \log \frac{1}{\varepsilon_{PA}} \right]. \end{aligned} \quad (144)$$

In the above bounds, we have converted to smooth min-entropy rather than directly using the Rényi privacy amplification theorem of Ref. [10] in order to achieve a

“fairer” comparison to Refs. [6,7]. However, our approach is certainly compatible with the latter since it proceeds by first bounding the Rényi entropy, which typically yields

better finite-size key rates [5]. Furthermore, we have a “fully Rényi” security proof, maximally exploiting the results we have developed in this work. Hence, we also perform some calculations for this approach.

$$\begin{aligned} \ell_{\text{key}} = & \left[\inf_{\mathbf{q} \in S_{\Omega}} \inf_{\nu_{\hat{c}} \in \mathbb{P}_{\hat{c}}} \left(q(\perp) \left(1 - \frac{1}{1-\beta} \log \left(\left(1 - \frac{\nu_{\hat{c}}(1)}{\gamma} \right)^{\beta} + \left(\frac{\nu_{\hat{c}}(1)}{\gamma} \right)^{\beta} \right) \right) + \frac{1}{\hat{\alpha}-1} D(\mathbf{q} \parallel \nu_{\hat{c}}) \right) n \right. \\ & \left. - \lambda_{\text{EC}} - \left\lceil \log \frac{1}{\varepsilon_{\text{EV}}} \right\rceil - \frac{\alpha}{\alpha-1} \log \frac{1}{\varepsilon_{\text{PA}}} + 2 \right], \end{aligned} \quad (145)$$

then the protocol will be $\varepsilon^{\text{secure}}$ -secure with the much simpler security parameter

$$\varepsilon^{\text{secure}} = \varepsilon_{\text{PA}} + \varepsilon_{\text{EV}}. \quad (146)$$

Optimizing the choice of ε_{PA} and ε_{EV} for a desired $\varepsilon^{\text{secure}}$ and fixed α yields the following explicit solution (in this case, it is ε_{PA} that contributes much more significantly to the key length than ε_{EV} , due to the behavior of the Rényi privacy amplification theorem):

$$\varepsilon_{\text{EV}} = \frac{\alpha-1}{2\alpha-1} \varepsilon^{\text{secure}}, \quad \varepsilon_{\text{PA}} = \frac{\alpha}{2\alpha-1} \varepsilon^{\text{secure}}. \quad (147)$$

In Figs. 1 and 2, we plot the key rates $\frac{\ell_{\text{key}}}{n}$ obtained from the formulas in Eqs. (138), (144), and (145) for some simple examples. Comparing them to the corresponding results in Fig. 7 of Ref. [6], we find that while the loosest bound in Eq. (138) is slightly worse at small n , we have better key rates everywhere else as compared to the results in that work. On the other hand, compared to the tighter finite-size analysis in Fig. 1 of Ref. [7] (which was based on improving the Serfling-bound analysis in Ref. [6]), we see that while Eqs. (144) and (145) also performed better in almost all cases (except $n = 5000$ for the former), our loosest bound in Eq. (138) is worse.

These results overall suggest that, in terms of bounding the smooth min-entropy itself, our best approach for doing so can even outperform the improvement achieved in Ref. [7] over Ref. [6], but the difference is not very large. However, since our techniques can instead directly bound the Rényi entropy, for the final purpose of key-rate computations, we can still significantly outperform Ref. [7] by applying the Rényi privacy amplification theorem [10]. (It is true that, technically, our protocol implements infrequent sampling rather than sampling without replacement as in Refs. [6,7]; however, we believe the comparison is still fairly reasonable.) An important question is whether this improvement still holds in the presence of photon loss; we leave this for future work.

We remark that, in fact, using Theorem V.1 for this proof was slightly suboptimal: Our bound for the Ref. [17] model (Theorem VI.1) is slightly tighter, as

Specifically, using the single-round Rényi entropy bounds in Eqs. (142) and (143), together with the Rényi privacy amplification theorem, we can conclude that if we set [11]

previously discussed. However, we chose to present our results based on Theorem V.1 to demonstrate that we can obtain key rates comparable to the smooth-entropy EUR approach in Refs. [6,7] even with that slight suboptimality. [We briefly note though that replacing Eq. (138) with its tighter Theorem VI.1 analog still does not seem to allow it to certify positive key rates in the Fig. 2 parameter regime, though that bound is fairly loose in any case.] Also note that, here, we considered an EB protocol, which does not require a “single-signal interaction” condition when applying the GEAT; when considering PM protocols instead, one should use the Ref. [17] model (Theorem VI.1) to avoid requiring this condition.

C. DIRE from collision-entropy accumulation

In Ref. [46], an experiment was performed to demonstrate DIRE, with a security proof using the EAT (under the original Markov conditions as described in Sec. VI A here). To briefly summarize, each round consists of an infrequent-sampling channel (Definition V.2) such that, in test rounds, the CHSH game is played and the “secret test register” $\tilde{C}_j$ is set to 0 for a loss and 1 for a win; in generation rounds, fixed inputs are supplied to their devices, and the outputs are recorded, with $\tilde{C}_j$ being set to $\perp$. The “public test registers” $\hat{C}_j$ are trivial in this analysis. The secret register S_j for the proof technically consists of outputs from both Alice’s and Bob’s devices; however, for the purposes of the single-round analysis, we follow that work and simply lower bound its entropy by only considering Alice’s output.

As the Ref. [46] analysis was based on the previous EAT, they considered only the von Neumann entropy in the single-round analysis. We could of course employ the same process with our results using the methods discussed above (and we again find improved finite-size performance compared to previous results, which we present in a companion work [63]). However, in this section, we demonstrate an alternative perspective that, given a bound on the single-round min-entropy or collision entropy, we can “accumulate” it to obtain a bound on the overall $H_2^{\uparrow}$ entropy, on which we can directly apply a “traditional” privacy amplification result (Theorem 5.5.1. in Ref. [24]). (A collision-entropy analysis was also used in Ref. [58], but it was under an IID assumption.)

Remark VII.2. Readers interested in results more applicable to DIQKD may refer to the companion work [63]. For the example here, we have chosen randomness expansion rather than QKD because, in the former, *any* $\Omega(n)$ lower bound on the overall $H_2^\uparrow(S_1^n \bar{C}_1^n | T_1^n \hat{E})_{\rho_{\Omega}}$ entropy is enough to eventually produce a nonzero key length. In contrast, for QKD, there is an error-correction term λ_{EC} that remains significant at large n , so an $\Omega(n)$ lower bound on $H_2^\uparrow(S_1^n \bar{C}_1^n | T_1^n \hat{E})_{\rho_{\Omega}}$ would still need to have a sufficiently large implicit constant in order to produce a nonzero key length, even asymptotically.

Specifically, in Refs. [56,57], a bound was derived on $H_\infty^\uparrow(S\bar{C}|\hat{C}T\hat{E})_{\nu_{\perp}}$ as a function of CHSH winning probability. Noting that $H_2 \geq H_\infty^\uparrow$ (Corollary 4 in Ref. [77]), we can write [87]

$$\begin{aligned} H_2(S\bar{C}|\hat{C}T\hat{E})_{\nu_{\perp}} &\geq H_\infty^\uparrow(S\bar{C}|\hat{C}T\hat{E})_{\nu_{\perp}} \\ &\geq f_{\text{CHSH}}\left(\frac{\nu_{\bar{C}}(1)}{\gamma}\right), \end{aligned}$$

where $f_{\text{CHSH}}(w) := 1 - \log\left(1 + \sqrt{2 - \frac{(8w-4)}{4}}\right)$. (148)

Applying the Lemma VI.1 version of Theorem V.1 with the Lemma V.1 bound (these choices are to ensure the Rényi parameter does not change further), we obtain a form of “collision entropy accumulation,” albeit with $H_2^\uparrow$ of the final state rather than H_2 :

$$H_2^\uparrow(S_1^n \bar{C}_1^n | T_1^n \hat{E})_{\rho_{\Omega}} \geq nh_2 - \log \frac{1}{p_{\Omega}},$$

where

$$h_2 = \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\nu_{\bar{C}} \in \mathbb{P}_{\bar{C}}} \left(q(\perp) f_{\text{CHSH}}\left(\frac{\nu_{\bar{C}}(1)}{\gamma}\right) + D(\mathbf{q} \| \nu_{\bar{C}}) \right). \quad (149)$$

Thus, we can apply a “traditional” privacy amplification theorem for unsmoothed $H_2^\uparrow$ (Theorem 5.5.1 of Ref. [24]), from which we conclude that we can obtain an $\varepsilon^{\text{secret}}$ -secret key with length given by

$$\ell_{\text{key}} = \left\lfloor nh_2 - 2 \log \frac{1}{\varepsilon^{\text{secret}}} + 2 \right\rfloor. \quad (150)$$

[Technically, to obtain the above result, we have used the fact that, for this protocol, we have $H_2^\uparrow(S_1^n | T_1^n \hat{E})_{\rho_{\Omega}} = H_2^\uparrow(S_1^n \bar{C}_1^n | T_1^n \hat{E})_{\rho_{\Omega}}$ by Lemma B.7 in Ref. [1] because $\bar{C}_1^n$ in this protocol can be “projectively reconstructed” from $S_1^n T_1^n$. In addition, the log-probability term does not appear in the final key length formula because it simply becomes

an appropriate prefactor in the secrecy definition; see Refs. [10,11].]

The above formula for ℓ_{key} is a linear expression with only an $O(1)$ finite-size correction, so we might hope that it could perform better at small n , where the $O(\sqrt{n})$ finite-size corrections of the previous EAT have larger relative effects. Evaluating the value of h_2 in the above formula for the parameters used in the main experiment of Ref. [46], we find the result $h_2 = 4.47 \times 10^{-9}$, which appears fairly small. However, we note that to achieve the secrecy parameter of $\varepsilon^{\text{secret}} = 3.09 \times 10^{-12}$ that was chosen in that work, the minimum number of rounds required for non-trivial key length (i.e., $\ell_{\text{key}} \geq 1$) with this formula is then $n_{\min} = 1.685 \times 10^{10}$, which is indeed a slight improvement over the value $n_{\min} = 8.951 \times 10^{10}$ found in that work. [On the other hand, if we consider the larger value $n = 1.3824 \times 10^{11}$ used in the actual [46] experiment, the formula in Eq. (150) yields a much smaller ℓ_{key} than the analysis in that work, which is somewhat expected since the rate asymptotically converges to h_2 rather than the single-round von Neumann entropy.]

As mentioned in previous sections, the above approach has the drawback that h_2 is a constant independent of n because the “penalty term” in Eq. (149) does not change with n . This drawback implies, in particular, that it does not converge to $\inf_{\nu_{\bar{C}} \in S_{\Omega}} \nu_{\bar{C}}(\perp) f_{\text{CHSH}}\{\nu_{\bar{C}}(1)/\gamma\}$ even at large n . To overcome this issue, we can fine-tune further by noting that since the Rényi entropies are monotone in α , the lower bound in Eq. (148) also holds for any H_α with $\alpha \leq 2$, and therefore, we could invoke our bounds with any such α instead. Together with the Rényi privacy amplification theorem [10,88], this means we could obtain an $\varepsilon^{\text{secret}}$ -secret key by picking

$$\begin{aligned} \ell_{\text{key}} = & \left\lfloor \inf_{\mathbf{q} \in S_{\Omega}} \inf_{\nu_{\bar{C}} \in \mathbb{P}_{\bar{C}}} \left(q(\perp) f_{\text{CHSH}}\left(\frac{\nu_{\bar{C}}(1)}{\gamma}\right) \right. \right. \\ & \left. \left. + \frac{1}{\alpha-1} D(\mathbf{q} \| \nu_{\bar{C}}) \right) n - \frac{\alpha}{\alpha-1} \log \frac{1}{\varepsilon^{\text{secret}}} + 2 \right\rfloor, \quad (151) \end{aligned}$$

where $\alpha \in (1, 2]$ can be optimized over. Note that, in this approach, the final Rényi entropy $H_\alpha^\uparrow(S_1^n \bar{C}_1^n | T_1^n \hat{E})_{\rho_{\Omega}}$ that we bounded may have a very different Rényi parameter from the single-round bound; however, it has the advantage that, at large n , the “first-order constant” will indeed converge to $\inf_{\nu_{\bar{C}} \in S_{\Omega}} \nu_{\bar{C}}(\perp) f_{\text{CHSH}}\{\nu_{\bar{C}}(1)/\gamma\}$ [e.g., by taking $\alpha = 1 + \Theta(1/\sqrt{n})$]. By optimizing α in this formula in Eq. (151), we find that $\ell_{\text{key}} \geq 1$ can be achieved even at, e.g., $n = 10^{10}$.

In fact, with this perspective, we can also apply the Lemma V.2 bound instead by setting $\alpha' = 2$ and hence requiring $\lceil \alpha/(\alpha-1) \rceil = 2 + \lceil \alpha'/(\alpha'-1) \rceil$ [if we write $\alpha = 1 + \mu$, this translates to $\alpha' = 1 + \lceil \mu/(1-2\mu) \rceil = 1 + \mu + O(\mu^2)$; note that we have to restrict to $\mu < 1/2$,

i.e., $\alpha < 3/2$). Because of symmetries of the protocol, the bound in Eq. (148) also holds for the state ν without conditioning on $\bar{c} = \perp$ (this fact was implicitly used in Ref. [46]). Thus, we can pick

$$\begin{aligned} \ell_{\text{key}} = & \left[\inf_{\mathbf{q} \in \mathcal{S}_\Omega} \inf_{\nu_{\bar{c}} \in \mathbb{P}_{\bar{c}}} \left(f_{\text{CHSH}} \left(\frac{\nu_{\bar{c}}(1)}{\gamma} \right) \right. \right. \\ & \left. \left. + \frac{\alpha''}{\alpha'' - 1} D(\mathbf{q} \parallel \nu_{\bar{c}}) \right) n - \frac{\alpha}{\alpha - 1} \log \frac{1}{\varepsilon^{\text{secret}}} + 2 \right]. \end{aligned} \quad (152)$$

We find that at $n \sim 10^{10}$, this bound is worse than Eq. (151). However, when n becomes closer to the values used in the Ref. [46] experiment, it sometimes performs better than Eq. (151) (though still somewhat worse than the results in Ref. [46] based on single-round von Neumann entropy but, surprisingly, not by a large extent). This behavior essentially seems to be because we have fixed the value of α' in this case, so the other Rényi parameter α'' remains equal to α up to order $O((\alpha - 1)^2)$, hence more or less avoiding the “loss” in Rényi parameter. Thus, at large n (where the optimal α becomes close to 1), it can sometimes outperform Eq. (151) because it does not have the $q(\perp)$ prefactor. However, roughly speaking, we do not expect this to be the case if we were to instead work with von Neumann entropy [via Eq. (86)] in this regime since in that case the Rényi parameters would have the worse scaling $\alpha', \alpha'' = 1 + 2\mu + O(\mu^2)$ as discussed previously, assuming we choose $\alpha' = \alpha''$ [89].

Finally, we highlight that numerical exploration again suggests that, rather than using the accept condition in the Ref. [46] experiment (which only constrains the frequency of $\bar{c} = 0$), our bounds yield better results if we instead follow the approach in Remark VII.1 (while preserving the same bound on honest abort probability).

VIII. CONCLUSION AND FUTURE WORK

In summary, in this work, we have found a connection between entropy accumulation and QEFs, yielding families of Rényi entropy bounds that are suitable for use in both variable-length and fixed-length protocols. Our results for the latter case have the important advantage of not requiring affine min-tradeoff functions; furthermore, we find that they give a significant improvement, in practice, over previous EAT or GEAT bounds. Since our approach proceeds via Rényi entropies, it also unlocks a variety of options for security proofs based on any Rényi entropies, including “fully Rényi” security proofs (without an IID assumption) that approach the “correct” asymptotic behavior by taking $\alpha \rightarrow 1$.

Certainly, one question for future consideration would be whether the bounds could be further tightened. As discussed in Sec. VII A, for fixed-length protocols, it seems many steps in the proof are tight, apart from Lemma IV.9.

It would be interesting to see if improvements could be found on that step. However, we highlight again that the current bound is already tight enough to outperform the smoothed-entropy EURs in at least some contexts. For variable-length protocols, it may be worth exploring how the results would compare against a suitable adaptation of the variable-length security proofs in Ref. [90] to handle non-IID attacks (other than by using the postselection technique [91,92]). Roughly speaking, the approach in that work relies on constructing a statistical estimator for the final Rényi entropy, in a somewhat different sense from the log-mean-exponential nature of our H_α^f -entropy analysis. While that work only constructed such estimators for the IID scenario, it seems that, in principle, there should be no fundamental obstruction to constructing such estimators in a non-IID fashion as well, and resolving that issue might yield an interesting alternative to this approach [93].

Additionally, Refs. [1,4] also used the concept of entropy accumulation to obtain upper bounds on the final smooth max-entropy, via bounds on the Rényi entropies for $\alpha < 1$ (or via a duality argument, in the latter work). Such bounds can be useful, for instance, in studying one-shot distillable entanglement [19]. Our proof techniques can also be used to obtain similar results, though we found a number of interesting technical subtleties. We present a detailed discussion of these results in Appendix E.

Another consideration is the fact that in current DIQKD security proofs, the handling of the test-round registers is highly inconvenient—since they do not fulfill the NS condition, one has to include them in the $\bar{C}_1^n$ registers on the “left side” of the conditioning and then shift them to the “right side” via chain rules [29,36,37]. Ideally, to resolve this issue, one needs a version of entropy accumulation that does not require the test-round registers to explicitly appear in the entropy terms (or be “reconstructible” from the registers that appear, in the sense of Ref. [4]). This solution is not straightforward with the proof approaches thus far, but it remains an interesting open question that should be further explored. Otherwise, it may be interesting to consider the question of whether there is a more natural way to handle the $\bar{C}_1^n$ registers for variable-length protocols rather than simply shifting them onto the right side of the conditioning (especially in the case of DIRE), perhaps by using some other structure in H_α^f entropies.

Remark VIII.1. For fixed-length protocols using infrequent-sampling channels (Definition V.2), we can at least propose an improved method for handling the $\bar{C}_1^n$ registers as compared to previous works such as Refs. [5,29,36,58]. Specifically, let us suppose the protocol satisfies the following properties (here, we focus on the GEAT model, but analogous statements hold for the EAT model):

- (i) The E_n register at the end of the protocol contains a copy of some classical registers T_1^n that record whether each round is a test or generation round.

- (ii) Conditioned on the event Ω , the fraction of test rounds is at most some fixed constant $\gamma^{\max}$.

These properties are usually easy to satisfy when designing a protocol (the second one by choosing the accept condition to inherently impose the required constraint on the test-round fraction—this usually does not affect the completeness parameter significantly since the honest behavior is IID). The results in this work give bounds on, e.g., $H_\alpha^\uparrow(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega}$, but the main quantity of interest in, e.g., DIQKD security proofs is usually something like $H_\alpha^\uparrow(S_1^n | \hat{C}_1^n E_n)_{\rho_\Omega}$ (possibly with additional conditioning registers). We now observe that given the above two properties, we can easily relate these quantities as follows.

First, let us suppose that there exist classical registers Z_j with a common alphabet $\mathcal{Z}$, such that Z_j takes a fixed value in generation rounds, and $\bar{C}_1^n$ can be “projectively reconstructed” from $S_1^n Z_1^n \hat{C}_1^n E_n$ (in the sense of Lemma B.7 of Ref. [1])—this can be trivially fulfilled by the simple choice $Z_j = \bar{C}_j$, but the subsequent bounds are more flexible if we allow the possibility that they could be, e.g., some public announcements. Then, for any $\alpha \in [1/2, \infty]$, we have

$$\begin{aligned}
 & H_\alpha^\uparrow(S_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} \\
 & \geq H_\alpha^\uparrow(S_1^n | Z_1^n \hat{C}_1^n E_n)_{\rho_\Omega} \\
 & \geq H_\alpha^\uparrow(S_1^n Z_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} - H_0^\uparrow(Z_1^n | T_1^n)_{\rho_\Omega} \\
 & \geq H_\alpha^\uparrow(S_1^n Z_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} - \max_{t_1^n \text{ s.t. } \rho_\Omega(t_1^n) > 0} H_0(Z_1^n)_{\rho_{t_1^n}} \\
 & \geq H_\alpha^\uparrow(S_1^n Z_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} - \gamma^{\max} n \log |\mathcal{Z}|, \tag{153}
 \end{aligned}$$

where in the last line we can replace $|\mathcal{Z}|$ with $|\mathcal{Z}| - 1$ if the alphabet $\mathcal{Z}$ contains a particular symbol (say, $\perp$) that never occurs in test rounds. In the above, the second line is [94] proven in Appendix F [see Eq. (F2), noting that E_n contains the register T_1^n]; the third line follows from the fact that, since $Z_1^n T_1^n$ are classical, we can [see Eq. (5.27) in Ref. [30]] write $H_0^\uparrow(Z_1^n | T_1^n)_{\rho_\Omega}$ in the form given in Definitions 3.1.2 and 3.1.4 of Ref. [24]; and the fourth line holds because, given the properties we imposed, we see that, conditioned on any t_1^n value with nonzero probability in ρ_Ω , there are at most $\gamma^{\max} n$ positions in the string Z_1^n that are not set to a fixed value. The final line can then be straightforwardly bounded using our main results in this work by observing that

$$\begin{aligned}
 H_\alpha^\uparrow(S_1^n Z_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} &= H_\alpha^\uparrow(S_1^n Z_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} \\
 &\geq H_\alpha^\uparrow(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega}, \tag{154}
 \end{aligned}$$

where the equality holds by Lemma B.7 of Ref. [1] and the inequality holds since Z_1^n are classical.

The above chain of computations serves to bound both $H_\alpha^\uparrow(S_1^n | \hat{C}_1^n E_n)_{\rho_\Omega}$ and $H_\alpha^\uparrow(S_1^n | Z_1^n \hat{C}_1^n E_n)_{\rho_\Omega}$, so one can use whichever is more convenient in a DIQKD security proof. The latter is useful if, for instance, the Z_1^n registers represent public announcements that do not fulfill the NS or Markov conditions; see, e.g., Ref. [63]. We believe that this bound should not only be simpler but also tighter than the previous approaches in Refs. [5, 29, 36, 58], which were based on chain rules that changed the smoothing parameter or Rényi parameter [95].

However, for variable-length protocols, this technique does not work directly because we do not condition on an “acceptance event,” so it seems less straightforward to constrain the state support in the subtracted entropic term. As discussed previously, one approach might be to use Lemma IV.6 and then apply the EAT to bound the resulting $H_{\alpha'}(Z_1^n | T_1^n)_\rho$ term on the *unconditioned* state [noting that, for an infrequent-sampling channel, the single-round $H_{\alpha'}(Z_j | T_j)_\nu$ entropy is bounded even without “testing”], but the bound might be slightly worse.

We also note that, in this work, we have focused on presenting fairly simple example applications, such as fully qubit BB84 and a simple DIRE scenario. In separate works, we apply these results to more sophisticated protocols such as decoy-state QKD and DIQKD.

ACKNOWLEDGMENTS

We are very grateful to Peter Brown and Thomas van Himbeek for discussions of their work on $H_\alpha^{\uparrow f}$ entropies—our presentation in Sec. IV in terms of $H_\alpha^{\uparrow f}$ entropies was formulated based on their approach, though we developed the overall proof structure that led to Theorem V.1 mostly independently. We also thank Ashutosh Marwah for providing us with the proof of Lemma F.1, as well as Frédéric Dupuis, Hao Hu, Tony Metger, Renato Renner, Martin Sandfuchs, and Ramona Wolf for helpful discussions. A. A. and E. T. conducted research at the Institute for Quantum Computing, at the University of Waterloo, which is supported by Innovation, Science, and Economic Development Canada. Support was also provided by NSERC under the Discovery Grants Program, Grant No. 341495. T. H. acknowledges support from the Marshall and Arlene Bennett Family Research Program, the Minerva Foundation with funding from the Federal German Ministry for Education and Research and the Israel Science Foundation (ISF), and the Directorate for Defense Research and Development (DDR&D), Grant No. 3426/21.

APPENDIX A: COMPARISON TO PREVIOUS GEATT DEFINITION

Here, we outline some differences between the conditions in Ref. [4] and our approach. In that work, only a single “testing register” C_j was produced in each round,

and the bounds they obtained were on entropies of the form $\mathbb{H}(S_1^n|E_n)$ (for various entropies $\mathbb{H}$) for the final state, under a condition that C_1^n can be “projectively reconstructed” from $S_1^n E_n$ in that state. In this work, we have two such registers, $\bar{C}_j$ and $\hat{C}_j$, in each round, and we instead take the approach of obtaining bounds on the entropies of the form $\mathbb{H}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)$, where $\bar{C}_1^n \hat{C}_1^n$ are explicitly involved in the final bound but we do not impose the projective reconstruction condition. However, note that if $\bar{C}_1^n$ and $\hat{C}_1^n$ can separately be projectively reconstructed from S_1^n and E_n , respectively (which should be basically equivalent to the projective reconstruction property for C_1^n in that work because it requires C_1^n to be a deterministic function of outcomes of separate projective measurements on S_1^n and E_n , which can therefore be viewed as $\bar{C}_1^n$ and $\hat{C}_1^n$), then $\mathbb{H}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n) = \mathbb{H}(S_1^n | E_n)$ for any entropy with “reasonable” data-processing properties; thus, our results should be basically equivalent in those aspects. Similar considerations hold when considering the single-round entropies $\mathbb{H}(S_j \bar{C}_j | \hat{C}_j E_j)$ as well. [Strictly speaking, Ref. [4] does not state that the projective reconstruction property is required for individual rounds. However, a close inspection of the proof shows that, in fact, it is implicitly required to obtain the bound just before Eq. (4.10) in their proof because their argument is based on the argument in Ref. [2], which requires this property in single rounds as well.]

APPENDIX B: DETAILED PROOFS

1. Proof of Theorem IV.1

Let $M > 0$ be any value such that $M - f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) > (M/2) > 0$ for all the $f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j)$ in the theorem statement (for all j). Now, for each j , define a read-and-prepare channel $\mathcal{D}_j: \bar{C}_1^j \hat{C}_1^j \rightarrow \bar{C}_1^j \hat{C}_1^j \mathcal{D}_j$ of the form described in Lemma IV.2 so that the state it prepares on $\mathcal{D}_j$ satisfies

$$\begin{aligned} M - f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) &\leq H_\alpha(\mathcal{D}_j)_{\rho_{|\bar{c}_1^j \hat{c}_1^j}} \\ &\leq M - f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) + 2^{-\frac{M}{2}} \log e \end{aligned} \quad (\text{B1})$$

for all $\alpha \in [0, \infty]$. Now, let $\mathcal{N}_j: R_{j-1} E_{j-1} \bar{C}_1^{j-1} \hat{C}_1^{j-1} \rightarrow D_j \bar{C}_j S_j R_j E_j \bar{C}_1^j \hat{C}_1^j$ denote a channel that does the following (note that its input registers differ from $\mathcal{M}_j$ by also including $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$, and its output registers also include $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ and two additional registers $\bar{C}_j, D_j$):

- (1) Apply $\mathcal{M}_j \otimes \mathcal{P}_j$, where $\mathcal{P}_j$ is a pinching channel on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ (in its classical basis).
- (2) Copy the classical register $\bar{C}_j$ onto another classical register $\bar{\bar{C}}_j$.
- (3) Generate a D_j register by applying the above read-and-prepare channel $\mathcal{D}_j$ on $\bar{C}_1^j \hat{C}_1^j$.

Note that the third step can indeed be implemented as a read-and-prepare channel for *any* input state, even if it is not originally classical on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$, because the pinching channel in the first step forces the resulting state to be classical on those registers. The channels $\mathcal{N}_j$ form a valid sequence of GEAT channels (without testing) according to Definition III.1 by identifying the notation in these channels with the notation in that definition as follows: For the input registers,

$$(i) R_{j-1} \bar{C}_1^{j-1} \leftrightarrow R_{j-1},$$

$$(ii) E_{j-1} \hat{C}_1^{j-1} \leftrightarrow E_{j-1},$$

and for the output registers,

$$(i) D_j \bar{C}_j S_j \leftrightarrow S_j,$$

$$(ii) R_j \bar{C}_1^j \leftrightarrow R_j,$$

$$(iii) E_j \hat{C}_1^j \leftrightarrow E_j.$$

To verify that the NS condition of Definition III.1 is satisfied by this identification, we note that, by letting $\mathcal{R}_j$ be the channel in Definition III.2 and defining $\mathcal{R}'_j := \mathcal{R}_j \otimes \mathcal{P}'_j$ where $\mathcal{P}'_j$ is a pinching channel on $\hat{C}_1^{j-1}$ (in its classical basis), we have

$$\begin{aligned} \text{Tr}_{D_j \bar{C}_j S_j R_j \bar{C}_1^j} \circ \mathcal{N}_j &= \text{Tr}_{S_j \bar{C}_1^j} \circ (\mathcal{M}_j \otimes \mathcal{P}_j) \\ &= (\text{Tr}_{S_j \bar{C}_j R_j} \circ \mathcal{M}_j) \otimes (\text{Tr}_{\bar{C}_1^{j-1}} \circ \mathcal{P}_j) \\ &= (\mathcal{R}_j \circ \text{Tr}_{R_{j-1}}) \otimes (\mathcal{P}'_j \circ \text{Tr}_{\bar{C}_1^{j-1}}) \\ &= \mathcal{R}'_j \circ \text{Tr}_{R_{j-1} \bar{C}_1^{j-1}}, \end{aligned} \quad (\text{B2})$$

as desired. In the above, the first line holds because the partial trace $\text{Tr}_{D_j \bar{C}_j}$ removes all registers generated by $\mathcal{N}_j$ after applying $\mathcal{M}_j \otimes \mathcal{P}_j$, the second line is just a channel regrouping, the third line holds by the NS condition on $\mathcal{M}_j$ in Definition III.2 of GEATT channels (and the collapsing part of the pinching channel with the partial trace), and the last line is again a channel regrouping.

These channels $\mathcal{N}_j$ have the critical property that the state $\mathcal{N}_n \circ \dots \circ \mathcal{N}_1[\omega^0]$ would be identical to $\mathcal{M}_n \circ \dots \circ \mathcal{M}_1[\omega^0]$ on all registers that are present in the latter [96]. Therefore, we can now write $\rho = \mathcal{N}_n \circ \dots \circ \mathcal{N}_1[\omega^0]$ without danger of ambiguity with respect to the state ρ in the theorem statement by viewing the former as just an extension of the latter. Then, according to Lemma 3.6 of Ref. [4] (Fact III.1 stated above), since $\mathcal{N}_j$ is a sequence of GEAT channels, we have

$$H_\alpha(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho \geq \sum_j \inf_{\omega' \in \Sigma'_j} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\omega'}, \quad (\text{B3})$$

where Σ'_j denotes the set of all states that could be produced by $\mathcal{N}_j$ acting on some initial state $\omega' \in S_=(R_{j-1} E_{j-1} \bar{C}_1^{j-1} \hat{C}_1^{j-1} \tilde{E})$ [97]. However, recalling that

the $\bar{C}_j$ register produced by each $\mathcal{N}_j$ channel is always just a copy of the $\bar{C}_j$ register (and also that, in the final state, we still have $\bar{C}_1^n = \bar{C}_1^n$ because the subsequent channels do not disturb the classical $\bar{C}_j$ registers), this result is equivalent to

$$H_\alpha(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho \geq \sum_j \inf_{\nu' \in \Sigma_j} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu'}. \quad (\text{B4})$$

We shall now bound the terms on the right-hand side in terms of quantities involving only the original channels $\mathcal{M}_j$. Consider any j and take any state $\nu'_{D_j \bar{C}_j S_j R_j E_j \tilde{C}_j \hat{C}_j \tilde{E}} = \mathcal{N}_j[\omega'_{R_{j-1} E_{j-1} \bar{C}_1^{j-1} \hat{C}_1^{j-1} \tilde{E}}]$ (for some ω') in the corresponding infimum. This state is classical on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$; furthermore, recalling that $\mathcal{N}_j$ always begins by applying a pinching channel on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$, we can also take the input state ω' to be classical on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ without loss of generality. Letting $\nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ and $\omega'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ denote the respective states conditioned on [98] $\bar{C}_1^{j-1} \hat{C}_1^{j-1} = \bar{c}_1^{j-1} \hat{c}_1^{j-1}$, it is straightforward to see that we also have (since $\mathcal{N}_j$ does not disturb $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ if it is already classical):

$$\begin{aligned} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\sigma &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}_j \hat{c}_j} \sigma(\bar{c}_j \hat{c}_j)^\alpha \sigma(\hat{c}_j)^{1-\alpha} 2^{(1-\alpha)(H_\alpha(D_j)_{\sigma_{|\bar{c}_j \hat{c}_j}} - D_\alpha(\sigma_{S_j E_j \tilde{E} | \bar{c}_j \hat{c}_j} \| \mathbb{I}_{S_j} \otimes \sigma_{E_j \tilde{E} | \bar{c}_j \hat{c}_j}))} \right) \\ &\geq \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}_j \hat{c}_j} \sigma(\bar{c}_j \hat{c}_j)^\alpha \sigma(\hat{c}_j)^{1-\alpha} 2^{(1-\alpha)(M - f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) - D_\alpha(\sigma_{S_j E_j \tilde{E} | \bar{c}_j \hat{c}_j} \| \mathbb{I}_{S_j} \otimes \sigma_{E_j \tilde{E} | \bar{c}_j \hat{c}_j}))} \right) \\ &= M + H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}} (S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\sigma, \end{aligned} \quad (\text{B7})$$

where the inequality in the second line holds because the expression is monotonically increasing with respect to the $H_\alpha(D_j)_{\sigma_{|\bar{c}_j \hat{c}_j}}$ terms [for any $\alpha \in (0, 1) \cup (1, \infty)$]; thus, we can apply the lower bound in Eq. (B1). [More precisely, in order to apply that lower bound, we recall that $\sigma := \nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}} = \mathcal{N}_j[\omega'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}]$ by Eq. (B5), and therefore the D_j register in σ has indeed been produced by a read-and-prepare channel satisfying Eq. (B1), acting on a state in which $\bar{C}_1^{j-1} \hat{C}_1^{j-1} = \bar{c}_1^{j-1} \hat{c}_1^{j-1}$.]

Critically (for a fixed $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$), the only registers involved in this lower bound are the registers $S_j \bar{C}_j \hat{C}_j E_j \tilde{E}$ that can be produced by $\mathcal{M}_j$ (with an extension to an identity channel on $\tilde{E}$) [99]. Furthermore, recall that $\nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ can be produced by $\mathcal{N}_j$ according to Eq. (B5), so we can write

$$\nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}} = \mathcal{N}_j[\omega'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}], \quad (\text{B5})$$

a property we will need later in our proof. For now, we observe that since ν' is a mixture of the conditional states $\nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$, we can lower bound it by the “worst-case” term in the mixture as follows:

$$\begin{aligned} &H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu'} \\ &\geq H_\alpha(D_j S_j \bar{C}_j | \bar{C}_1^{j-1} \hat{C}_1^{j-1} E_j \tilde{E})_{\nu'} \\ &\geq \min_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}}, \end{aligned} \quad (\text{B6})$$

where the first inequality is by data processing (Fact II.1) and the second inequality holds by considering Fact II.2. (Alternatively, one can directly apply quasiconvexity of Rényi divergence, as described in Proposition 7.35 of Ref. [74], which implies quasiconcavity of the corresponding conditional entropy.) Now, consider any particular value of $\bar{c}_1^{j-1} \hat{c}_1^{j-1}$, and for brevity in the upcoming calculation, let us write $\sigma := \nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$. This state is classical on $\bar{C}_j \hat{C}_j$, so we can follow a similar chain of calculations as in Eq. (37) to obtain

$$\begin{aligned} &H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}} (S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}} \\ &= H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}} (S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\mathcal{N}_j[\omega'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}]} \\ &= H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}} (S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\mathcal{M}_j[\omega]}, \end{aligned} \quad (\text{B8})$$

where ω is just $\omega'_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ with $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ traced out. It is now only a function of $\mathcal{M}_j$ evaluated on some input state $\omega_{R_{j-1} E_{j-1} \tilde{E}}$ and the specified QES values. Putting this all together, we conclude that

$$\begin{aligned} &\inf_{\nu' \in \Sigma_j} H_\alpha(D_j S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_{\nu'} \\ &\geq M + \min_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} \inf_{\nu \in \Sigma_j} H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}} (S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu, \end{aligned} \quad (\text{B9})$$

giving us a lower bound on the right-hand side of Eq. (B4) that only involves the original GEATT channels $\mathcal{M}_j$.

Let us now turn to the left-hand side of Eq. (B4). Again performing calculations analogous to Eq. (37), we obtain

$$\begin{aligned}
H_\alpha(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}_1^n \hat{c}_1^n} \rho(\bar{c}_1^n \hat{c}_1^n)^\alpha \rho(\hat{c}_1^n)^{1-\alpha} 2^{(1-\alpha)(H_\alpha(D_1^n)_{\rho|_{\bar{c}_1^n \hat{c}_1^n}} - D_\alpha(\rho_{S_j E_n | \bar{c}_1^n \hat{c}_1^n} \|\mathbb{I}_{S_j} \otimes \rho_{E_n | \bar{c}_1^n \hat{c}_1^n}))} \right) \\
&= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}_1^n \hat{c}_1^n} \rho(\bar{c}_1^n \hat{c}_1^n)^\alpha \rho(\hat{c}_1^n)^{1-\alpha} 2^{(1-\alpha)(\sum_j H_\alpha(D_j)_\rho |_{\bar{c}_1^n \hat{c}_1^n} - D_\alpha(\rho_{S_j E_n | \bar{c}_1^n \hat{c}_1^n} \|\mathbb{I}_{S_j} \otimes \rho_{E_n | \bar{c}_1^n \hat{c}_1^n}))} \right) \\
&\leq \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}_1^n \hat{c}_1^n} \rho(\bar{c}_1^n \hat{c}_1^n)^\alpha \rho(\hat{c}_1^n)^{1-\alpha} 2^{(1-\alpha)(\sum_j (M-f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}(\bar{c}_j \hat{c}_j) + 2^{-\frac{M}{2}} \log e) - D_\alpha(\rho_{S_j E_n | \bar{c}_1^n \hat{c}_1^n} \|\mathbb{I}_{S_j} \otimes \rho_{E_n | \bar{c}_1^n \hat{c}_1^n}))} \right) \\
&= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}_1^n \hat{c}_1^n} \rho(\bar{c}_1^n \hat{c}_1^n)^\alpha \rho(\hat{c}_1^n)^{1-\alpha} 2^{(1-\alpha)(nM - f_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) + n2^{-\frac{M}{2}} \log e - D_\alpha(\rho_{S_j E_n | \bar{c}_1^n \hat{c}_1^n} \|\mathbb{I}_{S_j} \otimes \rho_{E_n | \bar{c}_1^n \hat{c}_1^n}))} \right) \\
&= nM + H_\alpha^{f_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho + n2^{-\frac{M}{2}} \log e. \tag{B10}
\end{aligned}$$

In the above, the third line holds because each D_j register is produced by independently applying a read-and-prepare channel on $\bar{C}_1^j \hat{C}_1^j$, and therefore we have $\rho_{D_1^n | \bar{c}_1^n \hat{c}_1^n} = \otimes_{j=1}^n \rho_{D_j | \bar{c}_1^j \hat{c}_1^j}$. The fourth line holds because the expression is again monotonically increasing with respect to all the $H_\alpha(D_j)$ terms [for any $\alpha \in (0, 1) \cup (1, \infty)$], so we can bound it using the upper bound in Eq. (B1). The fifth line simply substitutes the definition of $f_{\text{full}}(\bar{c}_1^n \hat{c}_1^n)$ in Eq. (57).

Substituting Eqs. (B9) and (B10) into Eq. (B4), we see that the nM terms can be canceled, yielding the conclusion

$$\begin{aligned}
H_\alpha^{f_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho &\geq \sum_j \min_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} \inf_{\nu \in \Sigma_j} H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}}(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu - n2^{-\frac{M}{2}} \log e. \tag{B11}
\end{aligned}$$

However, since this bound holds for arbitrary (sufficiently large) M , we can take the $M \rightarrow \infty$ limit, so the $2^{-\frac{M}{2}}$ term vanishes, yielding the desired final bound in Eq. (58).

To obtain Eq. (60), note that, by Lemma IV.7, each QES $\hat{f}_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}$ as defined in Eq. (59) satisfies

$$\begin{aligned}
&\inf_{\nu \in \Sigma_j} H_\alpha^{\hat{f}_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}}(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu \\
&= \inf_{\nu \in \Sigma_j} H_\alpha^{f_{|\bar{c}_1^{j-1} \hat{c}_1^{j-1}}}(S_j \bar{C}_j | \hat{C}_j E_j \tilde{E})_\nu - \kappa_{\bar{c}_1^{j-1} \hat{c}_1^{j-1}} = 0. \tag{B12}
\end{aligned}$$

Thus, by simply applying Eq. (58) for these QESs instead, we obtain Eq. (60).

2. Proof of Lemma V.3

For brevity in this proof, let us use $\tilde{\mathbf{f}}$, $\tilde{\lambda}$, and $\tilde{\rho}_{\bar{C}\hat{C}}$, respectively, to denote the restrictions of $\mathbf{f}$, λ , and $\rho_{\bar{C}\hat{C}}$

to $\text{supp}(\rho_{\bar{C}\hat{C}})$. In particular, $\tilde{\rho}_{\bar{C}\hat{C}}$ is a distribution on $\text{supp}(\rho_{\bar{C}\hat{C}})$ with full support. In addition, let $\tilde{\mathbf{D}}_\alpha$ denote the tuple of values $\{D_\alpha(\rho_{Q Q' \wedge \bar{C} \hat{C}} \|\mathbb{I}_Q \otimes \rho_{Q' \wedge \bar{C} \hat{C}})\}_{\bar{C} \hat{C} \in \text{supp}(\rho_{\bar{C}\hat{C}})}$ (note that every term in this tuple is finite, as argued below Definition IV.1).

We first note that, by slightly rewriting the formula for $H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho$, we obtain

$$\begin{aligned}
G_{\alpha,\rho}(\mathbf{f}) &= \frac{1}{(\alpha-1)\ln 2} \ln \left(\sum_{\bar{C} \hat{C} \in \text{supp}(\rho_{\bar{C}\hat{C}})} \rho(\bar{C} \hat{C}) \right. \\
&\quad \times e^{(\alpha-1)(\ln 2)(f(\bar{C} \hat{C}) + D_\alpha(\rho_{Q Q' \wedge \bar{C} \hat{C}} \|\mathbb{I}_Q \otimes \rho_{Q' \wedge \bar{C} \hat{C}}))} \Big) \\
&= \frac{1}{(\alpha-1)\ln 2} \text{logsumexp}(\ln(\tilde{\rho}_{\bar{C}\hat{C}})) \\
&\quad + (\alpha-1)(\ln 2)(\tilde{\mathbf{f}} + \tilde{\mathbf{D}}_\alpha), \tag{B13}
\end{aligned}$$

where logsumexp denotes the base- e log-sum-exponential function (see, e.g., Ref. [26]), and $\ln(\tilde{\rho}_{\bar{C}\hat{C}})$ simply denotes the elementwise logarithm of the distribution $\tilde{\rho}_{\bar{C}\hat{C}}$ (which is well defined since it is a full-support distribution). Since the log-sum-exponential function is convex [26] and we have $\alpha > 1$, the last expression is a convex function of $\tilde{\mathbf{f}}$, which implies $G_{\alpha,\rho}(\mathbf{f})$ is a convex function of $\mathbf{f}$ as claimed (noting that it is constant with respect to any $\mathbf{f}$ components outside of $\tilde{\mathbf{f}}$).

Noting that $G_{\alpha,\rho}$ is finite over all of $\mathbb{R}^{|\bar{C}\hat{C}|}$, the fact that it is convex implies that taking the convex conjugate twice returns the original function [26]. Hence, the remainder of the proof is focused only on proving that its convex conjugate is indeed the function $G_{\alpha,\rho}^*$ defined in Eq. (106)—once this has been shown, they will be convex conjugates of each other as claimed; in addition, convex conjugates are always convex, so $G_{\alpha,\rho}^*$ will be convex as claimed.

Now, by Definition V.3, $G_{\alpha,\rho}^*$ is the convex conjugate of $G_{\alpha,\rho}(\mathbf{f})$ iff the following relation holds:

$$G_{\alpha,\rho}^*(\lambda) = \sup_{\mathbf{f} \in \mathbb{R}^{|\tilde{\mathcal{C}} \times \hat{\mathcal{C}}|}} (\lambda \cdot \mathbf{f} - G_{\alpha,\rho}(\mathbf{f})). \quad (\text{B14})$$

We first note that for any λ such that $\text{supp}(\lambda) \not\subseteq \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$ —i.e., there exists some $\tilde{c}\hat{c} \notin \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$ such that $\lambda(\tilde{c}\hat{c}) \neq 0$ —the above optimization takes the value $+\infty$ because, as noted in Eq. (B13), the $G_{\alpha,\rho}(\mathbf{f})$ term would be independent of the corresponding $f(\tilde{c}\hat{c})$ value; hence, we could just take either $f(\tilde{c}\hat{c}) \rightarrow -\infty$ or $f(\tilde{c}\hat{c}) \rightarrow +\infty$ [depending on the sign of $\lambda(\tilde{c}\hat{c})$] to make the above optimization diverge to $+\infty$. Note that this value indeed matches the claimed formula for $G_{\alpha,\rho}^*$ in Eq. (106) because, for any λ such that $\text{supp}(\lambda) \not\subseteq \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$, either we have $\lambda \in \mathbb{P}_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}$, in which case the formula gives a value $+\infty$ due to the $D(\lambda||\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$ term, or we have $\lambda \notin \mathbb{P}_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}$, in which case the formula gives a value $+\infty$ directly.

Hence, in the remainder of our analysis, we only need to consider λ such that $\text{supp}(\lambda) \subseteq \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$; i.e., λ is only supported on $\text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$, in which case we have $\lambda \cdot \mathbf{f} = \tilde{\lambda} \cdot \tilde{\mathbf{f}}$. In addition, note that by Eq. (B13), we can write $G_{\alpha,\rho}(\mathbf{f}) = \tilde{G}_{\alpha,\rho}(\tilde{\mathbf{f}})$, where $\tilde{G}_{\alpha,\rho}$ simply denotes the last line of Eq. (B13). Hence, for such λ , we see the defining optimization for $G_{\alpha,\rho}^*$ reduces to

$$\begin{aligned} G_{\alpha,\rho}^*(\lambda) &= \sup_{\tilde{\mathbf{f}} \in \mathbb{R}^{|\tilde{\mathcal{C}} \times \hat{\mathcal{C}}|}} (\tilde{\lambda} \cdot \tilde{\mathbf{f}} - \tilde{G}_{\alpha,\rho}(\tilde{\mathbf{f}})) \\ &= \sup_{\mathbf{g} \in \mathbb{R}^{|\text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})|}} (\tilde{\lambda} \cdot \mathbf{g} - \tilde{G}_{\alpha,\rho}(\mathbf{g})) \end{aligned} \quad (\text{B15})$$

since the objective only depends on the restricted values $\tilde{\mathbf{f}}$.

Since $\tilde{G}_{\alpha,\rho}$ is convex as previously discussed, the above optimization is a concave maximization problem; hence, any stationary point yields a global maximum. By differentiating the objective function, we see that for any $\mathbf{g} \in \mathbb{R}^{|\text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})|}$, it is a stationary point if and only if it satisfies

$$\forall \tilde{c}\hat{c} \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}), \quad \lambda(\tilde{c}\hat{c}) = \frac{\rho(\tilde{c}\hat{c})e^{(\alpha-1)(\ln 2)(g(\tilde{c}\hat{c}) + D_\alpha(\rho_{QQ' \wedge \tilde{c}\hat{c}} || \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}))}}{\sum_{\tilde{c}'\hat{c}' \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})} \rho(\tilde{c}'\hat{c}')e^{(\alpha-1)(\ln 2)(g(\tilde{c}'\hat{c}') + D_\alpha(\rho_{QQ' \wedge \tilde{c}'\hat{c}'} || \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}'}))}}. \quad (\text{B16})$$

Note, however, that these equations do not necessarily always have a solution, so it would not be fully correct to simply substitute these equations into the objective function. To resolve this issue, we perform the following case analysis, under the implicit understanding that in all cases we are also taking $\text{supp}(\lambda) \subseteq \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$ as discussed above.

- (i) $\lambda \in \mathbb{P}_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}$ and has full support on $\text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$ [i.e., $\lambda(\tilde{c}\hat{c}) > 0$ for all $\tilde{c}\hat{c} \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$]: For this case, $\log(\lambda(\tilde{c}\hat{c})/\rho(\tilde{c}\hat{c}))$ is finite for all $\tilde{c}\hat{c} \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$.

Hence, if we set

$$g(\tilde{c}\hat{c}) = \frac{1}{\alpha-1} \log \frac{\lambda(\tilde{c}\hat{c})}{\rho(\tilde{c}\hat{c})} - D_\alpha(\rho_{QQ' \wedge \tilde{c}\hat{c}} || \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}) \quad (\text{B17})$$

for all $\tilde{c}\hat{c} \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$, then we see it is a valid solution to the above conditions in Eq. (B16), noting that, for this $\mathbf{g}$, the denominator in those conditions is simply

$$\sum_{\tilde{c}'\hat{c}' \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})} \rho(\tilde{c}'\hat{c}')e^{(\alpha-1)(\ln 2)(g(\tilde{c}'\hat{c}') + D_\alpha(\rho_{QQ' \wedge \tilde{c}'\hat{c}'} || \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}'}))} = \sum_{\tilde{c}'\hat{c}' \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})} \lambda(\tilde{c}'\hat{c}') = 1, \quad (\text{B18})$$

where the last equality holds since $\lambda \in \mathbb{P}_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}$ and we also suppose $\text{supp}(\lambda) \subseteq \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})$. By substituting this stationary point into Eq. (B15), we obtain

$$\begin{aligned} G_{\alpha,\rho}^*(\lambda) &= \sum_{\tilde{c}\hat{c} \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})} \lambda(\tilde{c}\hat{c}) \left(\frac{1}{\alpha-1} \log \frac{\lambda(\tilde{c}\hat{c})}{\rho(\tilde{c}\hat{c})} - D_\alpha(\rho_{QQ' \wedge \tilde{c}\hat{c}} || \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}) \right) - \tilde{G}_{\alpha,\rho}(\mathbf{g}) \\ &= \frac{1}{\alpha-1} D(\lambda || \rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}) - \sum_{\tilde{c}\hat{c} \in \text{supp}(\rho_{\tilde{\mathcal{C}}\hat{\mathcal{C}}})} \lambda(\tilde{c}\hat{c}) D_\alpha(\rho_{QQ' \wedge \tilde{c}\hat{c}} || \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}}), \end{aligned} \quad (\text{B19})$$

where in the second line we used the definition of KL divergence and the fact that, for this $\mathbf{g}$, we have $\tilde{G}_{\alpha,\rho}(\mathbf{g}) = 0$ due to Eq. (B18).

- (ii) $\lambda \in \mathbb{P}_{\bar{c}\hat{c}}$ and does not have full support on $\text{supp}(\rho_{\bar{c}\hat{c}})$: The reasoning is basically the same as the preceding case, except that for every $\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})$ such that $\lambda(\bar{c}\hat{c}) = 0$, we note that the supremum with respect to that $g(\bar{c}\hat{c})$ term in Eq. (B15) is approached by taking the $g(\bar{c}\hat{c}) \rightarrow -\infty$ limit [because $\tilde{G}_{\alpha,\rho}$ is monotonically increasing with respect to each $g(\bar{c}\hat{c})$ value]. In that limit, their contribution to the sum in the definition of $\tilde{G}_{\alpha,\rho}$ becomes trivial since

$$\lim_{g(\bar{c}\hat{c}) \rightarrow -\infty} e^{(\alpha-1)(\ln 2)(g(\bar{c}\hat{c}) + D_\alpha(\rho_{QQ'} \wedge \bar{c}\hat{c} \| \mathbb{I}_Q \otimes \rho_{Q'} \wedge \bar{c}\hat{c}))} = 0. \quad (\text{B20})$$

Therefore, we can basically set those values in the sum to zero and restrict our attention to the supremum over the remaining $\mathbf{g}$ components, which then lets us apply essentially the same analysis as the preceding case.

- (iii) $\lambda \notin \mathbb{P}_{\bar{c}\hat{c}}$ and there is at least one $\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})$ with $\lambda(\bar{c}\hat{c}) < 0$: For such cases, note that as the corresponding $g(\bar{c}\hat{c})$ term decreases towards $-\infty$, the objective goes to $+\infty$ because the $\lambda(\bar{c}\hat{c})g(\bar{c}\hat{c})$ term goes to $+\infty$ and the $-\tilde{G}_{\alpha,\rho}(g)$ term is monotonically increasing. Therefore, $G_{\alpha,\rho}^*(\lambda) = +\infty$ for such λ , as claimed in Eq. (106).
- (iv) $\lambda \notin \mathbb{P}_{\bar{c}\hat{c}}$ and $\lambda(\bar{c}\hat{c}) \geq 0$ for all $\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})$: With the implicit condition $\text{supp}(\lambda) \subseteq \text{supp}(\rho_{\bar{c}\hat{c}})$, this is only possible when $\sum_{\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})} \lambda(\bar{c}\hat{c}) \neq 1$.

Consider the choice of $\mathbf{g}$ given by taking some $k \in \mathbb{R}$ and setting $g(\bar{c}\hat{c}) = k$ for all $\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})$. Then, the last line of Eq. (B15) becomes

$$G_{\alpha,\rho}^*(\lambda) = \sup_{k \in \mathbb{R}} \left(k \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})} \lambda(\bar{c}\hat{c}) - 1 \right) + \frac{1}{(\alpha-1)\ln 2} \text{logsumexp}(\ln(\tilde{\rho}_{\bar{c}\hat{c}})) + (\alpha-1)(\ln 2)\tilde{\mathbf{D}}_\alpha \right). \quad (\text{B21})$$

Since the logsumexp term is independent of k , we see that if we have $\sum_{\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})} \lambda(\bar{c}\hat{c}) > 1$ [respectively, $\sum_{\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{c}\hat{c}})} \lambda(\bar{c}\hat{c}) < 1$], then as $k \rightarrow +\infty$ (respectively, $k \rightarrow -\infty$) the optimization increases towards $+\infty$, and thus $G_{\alpha,\rho}^*(\lambda) = +\infty$.

These cases are exhaustive and hence yield the desired result.

3. Proof of Lemma V.1

Lemma V.1 has almost the same proof as Theorem V.1, except we introduce a single inequality $H_{\hat{\alpha}}(D\bar{S}\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} \geq H_{\hat{\alpha}}(D\bar{S}|\bar{C}\hat{C}E\tilde{E})_{\nu^\omega}$ into the proof, which simplifies the final results.

We again begin with the second line of the bound in Eq. (103). Taking any read-and-prepare channel of the form described in Lemma IV.1 and extending any ν^ω in the infimum with this channel yields

$$\begin{aligned} H_{\hat{\alpha}}^f(\bar{S}\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} &= H_{\hat{\alpha}}(D\bar{S}\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega} - M \\ &\geq H_{\hat{\alpha}}(D\bar{S}|\bar{C}\hat{C}E\tilde{E})_{\nu^\omega} - M \\ &= \frac{1}{1-\hat{\alpha}} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{(1-\hat{\alpha})H_{\hat{\alpha}}(D\bar{S}|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega}} \right) - M \\ &= \frac{1}{1-\hat{\alpha}} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{(1-\hat{\alpha})(H_{\hat{\alpha}}(D)_{\nu_{\bar{c}\hat{c}}^\omega} + H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega})} \right) - M \\ &= \frac{1}{1-\hat{\alpha}} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{(1-\hat{\alpha})(-f(\bar{c}\hat{c}) + H_{\hat{\alpha}}(S|E\tilde{E})_{\nu_{\bar{c}\hat{c}}^\omega})} \right), \end{aligned} \quad (\text{B22})$$

where the first line is due to Eq. (36), the second line is an application of Proposition 5.5 of Ref. [30] by noting $\nu_{\bar{C}\hat{C}E\tilde{E}}^\omega$ is separable across the registers $\bar{C}$ and $\hat{C}E\tilde{E}$, the third line follows from Fact II.2, the fourth line holds since $\nu_{D\bar{S}E\tilde{E}}^\omega = \nu_{D|\bar{c}\hat{c}}^\omega \otimes \nu_{SE\tilde{E}|\bar{c}\hat{c}}^\omega$, and the last line follows from Eq. (35). Furthermore, note that $H_{\hat{\alpha}}(D\bar{S}|\bar{C}\hat{C}E\tilde{E})_{\nu^\omega} - M$ is

convex in ω (by Remark IV.2), and all lines after that point are equalities; therefore, the last line is also convex in ω .

Thus, we can apply exactly the same analysis as in the rest of the Theorem V.1 proof, replacing $H_{\hat{\alpha}}^f(\bar{S}\bar{C}|\hat{C}E\tilde{E})_{\nu^\omega}$ with the lower bound given in the last line above, except that we would modify the definition of $G_{\hat{\alpha},\nu^\omega}$ to

$$G_{\hat{\alpha}, \nu^\omega}(\mathbf{f}) := -\frac{1}{1-\hat{\alpha}} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) \right. \\ \left. \times 2^{(1-\hat{\alpha})(-f(\bar{c}\hat{c}) + H_{\hat{\alpha}}(S|EE)_{\nu_{\bar{c}\hat{c}}^\omega})} \right) \quad (\text{B23})$$

and carry out the subsequent calculations with $-H_{\hat{\alpha}}(S|EE)_{\nu_{\bar{c}\hat{c}}^\omega}$ in place of $D_{\hat{\alpha}}(\nu_{SE\bar{E}\wedge\hat{c}}^\omega \| \mathbb{I}_S \otimes \nu_{E\bar{E}\wedge\hat{c}}^\omega)$.

To show that the equality holds for the case where $\bar{C}$ is trivial, we note that the only point in the above calculations that differs from Sec. VC is the inequality in the second line of Eq. (B22), which is immediately redundant if $\bar{C}$ is trivial. Alternatively, we could directly prove equality by simply noting that, without the $\bar{C}$ registers, we can replace all the divergence terms in the sum with conditional entropies by writing

$$\begin{aligned} & -D_{\hat{\alpha}}(\nu_{SE\bar{E}\wedge\hat{c}}^\omega \| \mathbb{I}_S \otimes \nu_{E\bar{E}\wedge\hat{c}}^\omega) \\ &= -D_{\hat{\alpha}}(\nu_{SE\bar{E}|\hat{c}}^\omega \| \mathbb{I}_S \otimes \nu_{E\bar{E}|\hat{c}}^\omega) \\ &= H_{\hat{\alpha}}(S|E\bar{E})_{\nu_{\hat{c}}}, \end{aligned} \quad (\text{B24})$$

where the first equality holds because the Rényi divergence remains invariant if both arguments are multiplied by a common, strictly positive factor (see Definition II.5), recalling that all terms in the sum have $\nu(\hat{c}) > 0$.

4. Proof of Lemma V.2

Lemma V.1 is again proven via similar ideas, with the bound instead relaxed using the chain rule of Ref. [42].

Once again, we begin with the second line of the bound in Eq. (103). Now, instead, we consider a read-and-prepare channel $\bar{C}\hat{C} \rightarrow \bar{C}\hat{C}D$ of the form described in Lemma IV.2 so that, for any $\alpha \in [0, \infty]$, the bound in Eq. (38) holds; i.e., all Rényi entropy values of the D register (conditioned on $\bar{C}\hat{C} = \bar{c}\hat{c}$) lie in the interval $[M - f(\bar{c}\hat{c}), M - f(\bar{c}\hat{c}) + 2^{-M/2} \log e]$. If we extend any ν^ω in the infimum with this channel, we have

$$\begin{aligned} H_{\hat{\alpha}}^f(S\bar{C}|\hat{C}E\bar{E})_{\nu^\omega} &\geq H_{\hat{\alpha}}(DS\bar{C}|\hat{C}E\bar{E})_{\nu^\omega} - M - 2^{-\frac{M}{2}} \log e \\ &\geq H_{\alpha'}(S\bar{C}|\hat{C}E\bar{E})_{\nu^\omega} + H_{\alpha'}^\dagger(D|S\bar{C}\hat{C}E\bar{E})_{\nu^\omega} \\ &\quad - M - 2^{-\frac{M}{2}} \log e, \end{aligned} \quad (\text{B25})$$

where the first line holds by Eq. (39) and the second line is a special case of Proposition 7 in Ref. [42]. Before proceeding further, we note that the second term in the last line of Eq. (B25) can be bounded as

$$\begin{aligned} H_{\alpha'}^\dagger(D|S\bar{C}\hat{C}E\bar{E})_{\nu^\omega} &= \frac{\alpha''}{1-\alpha''} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{\left(\frac{1-\alpha''}{\alpha''}\right) H_{\alpha'}^\dagger(D|SE\bar{E})_{\nu_{\bar{c}\hat{c}}^\omega}} \right) \\ &= \frac{\alpha''}{1-\alpha''} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{\left(\frac{1-\alpha''}{\alpha''}\right) H_{\alpha'}^\dagger(D)_{\nu_{\bar{c}\hat{c}}^\omega}} \right) \\ &\geq \frac{\alpha''}{1-\alpha''} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{-\left(\frac{1-\alpha''}{\alpha''}\right) f(\bar{c}\hat{c})} \right) + M, \end{aligned} \quad (\text{B26})$$

where the first equality is due to Fact II.2, the second equality holds since $\nu_{DSE\bar{E}|\bar{c}\hat{c}}^\omega = \nu_{D|\bar{c}\hat{c}}^\omega \otimes \nu_{SE\bar{E}|\bar{c}\hat{c}}^\omega$ and $H_{\alpha'}^\dagger(D)_{\nu_{\bar{c}\hat{c}}^\omega} = H_{\alpha'}^\dagger(D)_{\nu_{\bar{c}\hat{c}}^\omega}$ when there is no conditioning register, and the inequality follows from the lower bound in Eq. (38). Combining Eq. (B26) with Eq. (B25), we have

$$\begin{aligned} H_{\hat{\alpha}}^f(S\bar{C}|\hat{C}E\bar{E})_{\nu^\omega} &\geq H_{\alpha'}(S\bar{C}|\hat{C}E\bar{E})_{\nu^\omega} - 2^{-\frac{M}{2}} \log e \\ &\quad + \frac{\alpha''}{1-\alpha''} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{-\left(\frac{1-\alpha''}{\alpha''}\right) f(\bar{c}\hat{c})} \right). \end{aligned} \quad (\text{B27})$$

Since the above bound holds for arbitrary (sufficiently large) M , we can take the $M \rightarrow \infty$ limit so the $2^{-\frac{M}{2}}$ term vanishes. Taking this into account and using the bound in Eq. (B27), our desired result follows by applying exactly the same analysis as in the rest of the Theorem V.1 proof, except that we replace $G_{\hat{\alpha}, \rho}(\mathbf{f})$ with

$$\begin{aligned} G_{\alpha', \alpha'', \nu^\omega}(\mathbf{f}) &:= -H_{\alpha'}(S\bar{C}|\hat{C}E\bar{E})_{\nu^\omega} \\ &\quad - \frac{\alpha''}{1-\alpha''} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) 2^{-\left(\frac{1-\alpha''}{\alpha''}\right) f(\bar{c}\hat{c})} \right). \end{aligned} \quad (\text{B28})$$

Note that the above expression is concave with respect to ω , as required for those remaining proof steps. This result follows by observing that $H_{\alpha'}(S\bar{C}|\hat{C}E\bar{E})_{\nu^\omega}$ is convex in ω by Remark IV.2; thus, we have $\alpha'' > 1$, so $-\left[\alpha''/(1-\alpha'')\right] \log(\cdot)$ is a concave function while the values $\nu^\omega(\bar{c}\hat{c})$ are affine functions of ω [100]. [To make the correspondence with the Theorem V.1 proof even more explicit, we can rewrite the above expression as

$$\begin{aligned} G_{\alpha', \alpha'', \nu^\omega}(\mathbf{f}) &= -\frac{1}{1-\alpha''} \log \left(\sum_{\bar{c}\hat{c} \in \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)} \nu^\omega(\bar{c}\hat{c}) \right. \\ &\quad \left. \times 2^{(1-\alpha'')(-f(\bar{c}\hat{c}) + H_{\alpha'}(S\bar{C}|\hat{C}E\bar{E})_{\nu_{\bar{c}\hat{c}}^\omega})} \right), \end{aligned} \quad (\text{B29})$$

where $\tilde{\alpha}'' := [(2\alpha'' - 1)/\alpha'']$, so we are carrying out the remaining calculations with $\tilde{\alpha}''$ in place of $\hat{\alpha}$ and a single value $H_{\hat{\alpha}'}(S\tilde{C}|\hat{C}E\tilde{E})_{\nu^\omega}$ in place of all the $-D_{\hat{\alpha}}(\nu_{SE\tilde{E}\wedge\tilde{C}\hat{C}}^\omega \otimes \mathbb{I}_S \otimes \nu_{E\tilde{E}\wedge\hat{C}}^\omega)$ terms.]

APPENDIX C: ALTERNATIVE PROOFS OF STRONG DUALITY

Here, we provide an alternative proof of Lemma V.4 that provides options for removing the finite-dimensionality assumption on $\tilde{Q}$ [at least for the purposes of proving this lemma in isolation—other steps, such as the fundamental GEAT bound in Eq. (B3), still currently require that assumption, due to the use of a de Finetti argument in its proof], possibly by imposing extra conditions on S_Ω .

We begin by removing some “extraneous” degrees of freedom from the optimizations. Specifically, given the channel $\mathcal{M}$, let us introduce a notion of its “supporting alphabet” [101] $\mathcal{C}_\mathcal{M} \subseteq \bar{\mathcal{C}} \times \hat{\mathcal{C}}$, which we define as the set of values $\bar{c}\hat{c}$ that can be produced with nonzero probability by some input state to $\mathcal{M}$:

$$\mathcal{C}_\mathcal{M} := \{(\bar{c}, \hat{c}) \in \bar{\mathcal{C}} \times \hat{\mathcal{C}} \mid \nu^\omega(\bar{c}\hat{c}) > 0 \text{ for some } \omega \in S_=(\tilde{Q})\}. \quad (\text{C1})$$

We will write $\mathbb{P}_{\mathcal{C}_\mathcal{M}}$ to denote distributions on $\mathcal{C}_\mathcal{M}$. Basically, our first goal is to “remove some dependencies” on terms corresponding to $\bar{c}\hat{c} \notin \mathcal{C}_\mathcal{M}$.

Observe that for any λ such that $\text{supp}(\lambda) \not\subseteq \mathcal{C}_\mathcal{M}$, by definition of $\mathcal{C}_\mathcal{M}$, we have $\text{supp}(\lambda) \not\subseteq \text{supp}(\nu_{\bar{c}\hat{c}}^\omega)$ for every ω . Thus, we can exclude any such λ from the infimum in the last line of Eq. (112) without changing its value because, for such λ , we have $G_{\hat{\alpha}, \nu^\omega}^*(\lambda) = +\infty$ for all ω [due to the $D(\lambda \parallel \nu_{\bar{c}\hat{c}}^\omega)$ term]. For convenience, let us introduce the notation $\mu_{\oplus 0}$ for any distribution $\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}$ to mean the corresponding distribution in $\mathbb{P}_{\bar{\mathcal{C}}\hat{\mathcal{C}}}$ obtained by padding μ with zero entries. With this notation, we can continue from the last line of Eq. (112) to obtain

$$\begin{aligned} r_{\hat{\alpha}}(\mathbf{f}) &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}} \inf_{\omega \in S_=(\tilde{Q})} (G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0}) + (\mathbf{q} - \mu_{\oplus 0}) \cdot \mathbf{f}) \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}} (J_{\hat{\alpha}}(\mu) + (\mathbf{q} - \mu_{\oplus 0}) \cdot \mathbf{f}), \end{aligned} \quad (\text{C2})$$

where we introduce a new function $J_{\hat{\alpha}}$ that computes the infimum over the only term involving ω :

$$J_{\hat{\alpha}}(\mu) := \inf_{\omega \in S_=(\tilde{Q})} G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0}). \quad (\text{C3})$$

Thus, from the last line of Eq. (C2), we see that $\sup_{\mathbf{f}} r_{\hat{\alpha}}(\mathbf{f})$ is the dual problem of

$$\begin{aligned} &\inf_{\mathbf{q} \in S_\Omega} \inf_{\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}} J_{\hat{\alpha}}(\mu) \\ &\text{s.t. } \mathbf{q} - \mu_{\oplus 0} = \mathbf{0}, \end{aligned} \quad (\text{C4})$$

and to obtain our desired result, we show that strong duality holds for this problem.

For this purpose, we first note that the objective $J_{\hat{\alpha}}(\mu)$ has the following critical properties with respect to μ :

- (i) It is convex over $\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}$ because $G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0})$ is jointly convex in (μ, ω) , and for a jointly convex function of two variables, taking the infimum with respect to one variable over a convex set preserves convexity in the other variable [see Chapter 3.2.5 of Ref. [26]]—as long as the infimum is not $-\infty$ everywhere, which is easily seen to be true for $G_{\hat{\alpha}, \nu^\omega}^*$.
- (ii) It is finite over $\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}$ because we can construct a feasible point ω in Eq. (C3) with a finite objective value: By definition of $\mathcal{C}_\mathcal{M}$, for each $\bar{c}\hat{c} \in \mathcal{C}_\mathcal{M}$, we can find some ω such that $\nu_{\bar{c}\hat{c}}^\omega(\bar{c}\hat{c}) > 0$; by taking a mixture of such cases, we can obtain an ω such that $\nu_{\bar{c}\hat{c}}^\omega$ has full support on $\mathcal{C}_\mathcal{M}$ (by linearity of $\mathcal{M}$), which means $D(\mu_{\oplus 0} \parallel \nu_{\bar{c}\hat{c}}^\omega)$ and hence also $G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0})$ is finite for this ω [102]. [The $D_{\hat{\alpha}}(\nu_{SE\tilde{E}\wedge\tilde{C}\hat{C}}^\omega \otimes \mathbb{I}_S \otimes \nu_{E\tilde{E}\wedge\hat{C}}^\omega)$ terms in the sum are all finite as previously discussed, so they pose no issues.]
- (iii) It is continuous over $\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}$ as long as we choose PUR to be a continuous function because, in that case, $G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0})$ is continuous in (μ, ω) (as discussed in the main text), and we are taking its infimum over a compact set $S_=(\tilde{Q})$. [Note that while $G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0})$ is only continuous in an extended-real sense, $J_{\hat{\alpha}}(\mu)$ is finite everywhere by the preceding point and hence continuous in the standard sense.]

Since $J_{\hat{\alpha}}(\mu)$ is entirely independent of $\mathbf{q}$, the above properties trivially give (joint) convexity, finiteness, and continuity over $(\mathbf{q}, \mu) \in \mathbb{P}_{\bar{\mathcal{C}}\hat{\mathcal{C}}} \times \mathbb{P}_{\mathcal{C}_\mathcal{M}}$ as well. Thus, we can again suppose S_Ω is closed without loss of generality since the continuity property over $\mathbb{P}_{\bar{\mathcal{C}}\hat{\mathcal{C}}} \times \mathbb{P}_{\mathcal{C}_\mathcal{M}}$ allows us to switch between S_Ω and its closure. With these properties, we have strong duality by the Clark-Duffin condition (or Sion’s minimax theorem), after which we obtain the desired final result by “reversing” all the above transformations:

$$\begin{aligned} \sup_{\mathbf{f}} r_{\hat{\alpha}}(\mathbf{f}) &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}} J_{\hat{\alpha}}(\mu) \\ &\text{s.t. } \mathbf{q} - \mu_{\oplus 0} = \mathbf{0} \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\mu \in \mathbb{P}_{\mathcal{C}_\mathcal{M}}} \inf_{\omega \in S_=(\tilde{Q})} G_{\hat{\alpha}, \nu^\omega}^*(\mu_{\oplus 0}) \\ &\text{s.t. } \mathbf{q} - \mu_{\oplus 0} = \mathbf{0} \\ &= \inf_{\mathbf{q} \in S_\Omega} \inf_{\lambda \in \mathbb{P}_{\bar{\mathcal{C}}\hat{\mathcal{C}}}} \inf_{\omega \in S_=(\tilde{Q})} G_{\hat{\alpha}, \nu^\omega}^*(\lambda) \\ &\text{s.t. } \mathbf{q} - \lambda = \mathbf{0}, \end{aligned} \quad (\text{C5})$$

where the last line holds because, as discussed previously, any λ such that $\text{supp}(\lambda) \not\subseteq \mathcal{C}_M$ yields $G_{\hat{\alpha}, \nu^\omega}^*(\lambda) = +\infty$ for every ω .

Remark C.1. In this proof of Lemma V.4, the *only* point where we invoked the finite-dimensionality condition was in showing that $J_{\hat{\alpha}}$ is continuous [where we used compactness of $S_=(\tilde{Q})$ —all other properties, such as convexity and finiteness, were true even for infinite-dimensional $\tilde{Q}$. Hence, this approach also provides an alternative method to obtain the desired result without requiring finite dimensionality of $\tilde{Q}$, if we instead impose additional conditions on S_Ω in order to use Slater’s condition, which requires no continuity properties. Specifically, suppose we additionally require that the relative interior of S_Ω contains a distribution $\mathbf{q}^*$ such that $q^*(\bar{c}\hat{c}) > 0$ if and only if $\bar{c}\hat{c} \in \mathcal{C}_M$ [i.e., $\text{supp}(\mathbf{q}^*) = \mathcal{C}_M$]. In that case, if we let $\mu^* \in \mathbb{P}_{\mathcal{C}_M}$ be the distribution $\mathbf{q}^*$ with the terms outside $\mathcal{C}_M$ removed, we see that $(\mathbf{q}^*, \mu^*)$ is a relative interior point of the domain in the constrained optimization in Eq. (C4) [in which the objective $J_{\hat{\alpha}}(\mu)$ is finite [103] everywhere], and it satisfies the equality constraint. This finding suffices to invoke Slater’s condition to claim that strong duality holds for that optimization, yielding the desired result without any finite-dimensionality conditions [104].

We also highlight that the interior-point requirement stated above should hold in any practical protocol because S_Ω would need to contain a “tolerance interval” for each outcome value $\bar{c}\hat{c} \in \mathcal{C}_M$. A rigorous formulation of this claim is as follows. Given that S_Ω is convex, the interior-point requirement holds whenever the following conditions are fulfilled:

- (1) For every distribution $\mathbf{q} \in S_\Omega$, we have $\text{supp}(\mathbf{q}) \subseteq \mathcal{C}_M$.
- (2) There exists some “reference” distribution $\mathbf{q}^{\text{ref}}$ with $\text{supp}(\mathbf{q}^{\text{ref}}) \subseteq \mathcal{C}_M$, and some $\delta > 0$, such that S_Ω contains all distributions $\mathbf{q}$ with $|q(\bar{c}\hat{c}) - q^{\text{ref}}(\bar{c}\hat{c})| \leq \delta$ for all $\bar{c}\hat{c} \in \mathcal{C}_M$ [105].

To prove this formulation suffices, simply construct the desired relative interior point by taking $\mathbf{q}^{\text{ref}}$ and perturbing it if necessary so that it has full support on $\mathcal{C}_M$; it is straightforward to show that such a perturbation always exists while keeping it in the relative interior of S_Ω (under the first condition listed above, which ensures the $\bar{c}\hat{c} \notin \mathcal{C}_M$ terms do not “contribute” to the affine hull of S_Ω). In addition, any practical protocol should satisfy these conditions because it would need to accept with nontrivial probability on some honest behavior; assuming, for simplicity, that this honest behavior is IID (though various non-IID scenarios can also be considered), it necessarily implies that S_Ω must contain all frequency distributions of the form just described, with $\mathbf{q}^{\text{ref}}$ being the honest single-round distribution and δ a small but strictly positive value.

An alternative prospect would be to try proving that $J_{\hat{\alpha}}$ is continuous even for infinite-dimensional $\tilde{Q}$. We believe this property is plausible, though proving this claim seems

slightly subtle because, in that case, $S_=(\tilde{Q})$ is not closed, and taking the infimum over such a set does not generically preserve continuity. A more detailed analysis of the continuity properties of $J_{\hat{\alpha}}$ may be able to resolve this point. In the process, one might be able to remove the use of continuity of Pur [which is also slightly subtle in the infinite-dimensional case because Eq. (29) does not directly generalize] because, in fact, we only need continuity properties of the “subsequent” quantities $D(\mu_{\oplus 0} \parallel \nu_{\bar{c}\hat{c}}^\omega)$ and $D_{\hat{\alpha}}(\nu_{SE\bar{E}\wedge\bar{c}\hat{c}} \parallel \mathbb{I}_S \otimes \nu_{E\bar{E}\wedge\bar{c}\hat{c}})$.

APPENDIX D: REPLACING DISTINCT CHANNELS WITH A SINGLE CHANNEL

We show here that the convex range of any (finite) set of channels can indeed be equivalently described using the range of a single channel (as in the set of its possible output states) via a simple direct-sum construction. Note that this construction is “generic” and does not use, e.g., the NS conditions of GEATT channels.

Lemma D.1. Let $\{\mathcal{M}_j\}_{j=1}^n$ be any set of channels $\mathcal{M}_j: \tilde{Q}_j \rightarrow Q'_j Q''_j \dots$ (for some finite number of output registers $Q'_j, Q''_j, \dots$), such that the registers Q'_j (respectively, $Q''_j, \dots$) can all be embedded in a common register Q' (respectively, $Q'', \dots$). Define $\tilde{Q}$ to be a register with Hilbert space $\mathcal{H}_{\tilde{Q}} = \bigoplus_{j=1}^n \mathcal{H}_{\tilde{Q}_j}$, and write $Q_j := Q'_j Q''_j \dots$ and $Q := Q' Q'' \dots$ for brevity.

Define a channel $\mathcal{M}: \tilde{Q} \rightarrow Q$ as follows: It first performs a projective measurement where outcome j corresponds to the projector onto $\mathcal{H}_{\tilde{Q}_j}$; then, conditioned on the outcome value j , it implements the channel $\mathcal{M}_j$ and embeds the output in Q . Next, the convex range Σ of $\{\mathcal{M}_j\}_{j=1}^n$ is equal to the range of $\mathcal{M}$; i.e., we have $\Sigma = \{\mathcal{M}[\omega_{\tilde{Q}}] \mid \omega \in S_=(\tilde{Q})\}$. Furthermore, for any register $\tilde{E}$, the convex range of $\{\mathcal{M}_j \otimes \text{id}_{\tilde{E}}\}_{j=1}^n$ is equal to the range of $\mathcal{M} \otimes \text{id}_{\tilde{E}}$.

The last statement involving $\text{id}_{\tilde{E}}$ is for applications in statements such as Theorem V.1, where we would like to preserve the structure of the channels acting as the identity on $\tilde{E}$.

Proof. It is easy to see that $\Sigma \subseteq \{\mathcal{M}[\omega_{\tilde{Q}}] \mid \omega \in S_=(\tilde{Q})\}$ since by, definition, every state in Σ has the form $\sum_j p_j \mathcal{M}_j[\omega_{\tilde{Q}_j}^{(j)}]$ for some probability distribution $\mathbf{p}$ and states $\omega_{\tilde{Q}_j}^{(j)}$, and can hence be generated by $\mathcal{M}$ from the input state $\bigoplus_j p_j \omega_{\tilde{Q}_j}^{(j)}$. To see the reverse containment, note that the initial projective measurement in $\mathcal{M}$ collapses any input state into the form $\bigoplus_j p_j \omega_{\tilde{Q}_j}^{(j)}$, and thus the final state produced by $\mathcal{M}$ has the form $\sum_j p_j \mathcal{M}_j[\omega_{\tilde{Q}_j}^{(j)}]$, which again lies in Σ by definition.

A similar argument yields the analogous statement for $\{\mathcal{M}_j \otimes \text{id}_{\tilde{E}}\}_{j=1}^n$ and $\mathcal{M} \otimes \text{id}_{\tilde{E}}$. Here, however, when proving the reverse containment, we use the fact that,

although the initial projective measurement does not act on $\tilde{E}$, it still collapses any input state into the form $\sum_j p_j \omega_{\tilde{Q}\tilde{E}}^{(j)}$, where $p_j \omega_{\tilde{Q}\tilde{E}}^{(j)} = (P_j \otimes \mathbb{I}) \omega_{\tilde{Q}\tilde{E}} (P_j \otimes \mathbb{I})$, with P_j being the projector onto $\mathcal{H}_{\tilde{Q}_j}$. This ensures each $\omega_{\tilde{Q}\tilde{E}}^{(j)}$ is a state such that $\omega_{\tilde{Q}}^{(j)}$ is supported on $\mathcal{H}_{\tilde{Q}_j}$, which suffices for the proof to continue. ■

Previous versions of this work were instead based on the concept of a “rate-bounding channel,” defined as follows. In this definition, as in Lemma IV.8, we denote the input space for the rate-bounding channel as a single register $\tilde{Q}$ that does not necessarily have to match the GEATT channel inputs, and we have not included a “memory register” R in its output of the rate-bounding channel—again, this is because these properties are not needed for our proofs.

Definition D.1. (Rate-bounding channel) Let $\{\mathcal{M}_j\}_{j=1}^n$ be a sequence of GEATT channels where all $\tilde{C}_j$ (respectively, $\hat{C}_j$) are isomorphic to a single register $\tilde{C}$ (respectively, $\hat{C}$) with alphabet $\tilde{C}$ (respectively, $\hat{C}$). A rate-bounding channel for $\{\mathcal{M}_j\}_{j=1}^n$ is a channel $\mathcal{M}: \tilde{Q} \rightarrow SE\tilde{C}\hat{C}$ such that, for any QES f on $\tilde{C}\hat{C}$ and any $\alpha \in (1, \infty)$, we have

$$\min_j \inf_{\nu \in \Sigma_j} H_\alpha^f(S_j \tilde{C}_j | \hat{C}_j E_j \tilde{E})_\nu \geq \inf_{\nu \in \Sigma} H_\alpha^f(S \tilde{C} | \hat{C} E \tilde{E})_\nu, \quad (\text{D1})$$

where Σ_j denotes the set of all states of the form $\mathcal{M}_j[\omega_{R_{j-1}E_{j-1}\tilde{E}}]$ for some initial state $\omega \in S_=(R_{j-1}E_{j-1}\tilde{E})$ and, analogously, Σ denotes the set of all states of the form $\mathcal{M}[\omega_{\tilde{Q}\tilde{E}}]$ for some initial state $\omega \in S_=(\tilde{Q}\tilde{E})$, with $\tilde{E}$ being a register of large enough dimension to serve as a purifying register for any of the $R_j E_j$ registers or the $\tilde{Q}$ register.

Theorem V.1 and similar statements still hold if we instead take $\mathcal{M}$ to be a rate-bounding channel rather than one that generates the convex range. In fact, such a formulation with rate-bounding channels is potentially more general in scope because it only requires the channel $\mathcal{M}$ to “characterize” the H_α^f -entropy values rather than the actual states in the convex range. However, we believe the formulation with the convex range is simpler to follow and also sufficient to cover most applications. [We also note that a previous version of this paper contained an incorrect statement that, in any sequence of GEATT channels, one of the channels would form a rate-bounding channel—that statement has a quantifier ordering issue, namely, that the bound in Eq. (D1) must hold for all f rather than a specific f . However, the construction of rate-bounding channels as presented in Lemma D.2 below is indeed valid but more elaborate than simply taking one of the channels in the sequence.]

The direct-sum construction in Lemma D.1 also suffices to construct a rate-bounding channel as follows. Again, this construction preserves infrequent-sampling structure as long as γ is the same in all rounds (since the projection

onto $\mathcal{H}_{R_{j-1}E_{j-1}}$ commutes with the classical “test/generation random choice”) and should cause no loss of tightness if we do not have *a priori* knowledge of how the channels in different rounds might behave differently [since it ensures that Eq. (D1) holds with equality].

Lemma D.2. Let $\{\mathcal{M}_j\}_{j=1}^n$ be a sequence of GEATT channels where all S_j (respectively, $\tilde{C}_j, \hat{C}_j$) are isomorphic to a single register S (respectively, $\tilde{C}, \hat{C}$) so that each channel is isomorphic to a channel $\mathcal{M}'_j: R_{j-1}E_{j-1} \rightarrow SR_j E_j \tilde{C} \hat{C}$. Define $\tilde{Q}$ to be a register with Hilbert space $\mathcal{H}_{\tilde{Q}} = \bigoplus_{j=1}^n \mathcal{H}_{R_{j-1}E_{j-1}}$, and define E to be a register with Hilbert space $\mathcal{H}_E = \bigoplus_{j=1}^n \mathcal{H}_{E_j}$.

Define a channel $\mathcal{M}: \tilde{Q} \rightarrow SE\tilde{C}\hat{C}$ as follows: It first performs a projective measurement where outcome j corresponds to the projector onto $\mathcal{H}_{R_{j-1}E_{j-1}}$; then conditioned on the outcome value j , it implements the channel $\mathcal{M}'_j$ and traces out the R_j register (while embedding the E_j register in E). Then, $\mathcal{M}$ is a valid rate-bounding channel; i.e., it satisfies the defining condition in Eq. (D1). Furthermore, the bound in that condition becomes an equality for this $\mathcal{M}$.

Proof. It is easy to see that Eq. (D1) holds since this $\mathcal{M}$ contains a “copy” of each $\mathcal{M}_j$ (formally, every feasible point on the left-hand side of Eq. (D1) straightforwardly yields a feasible point on the right-hand side with the same value). To see that the reverse inequality also holds, again note that the initial projective measurement in $\mathcal{M}$ produces a state that is a classical mixture of states supported on the $\mathcal{H}_{R_{j-1}E_{j-1}}$ spaces, so we can lower bound its H_α^f entropy using the worst-case term in the mixture [formally, using Lemmas IV.3 and IV.4 the same way as in Eq. (B6)]. ■

APPENDIX E: THE $\alpha < 1$ REGIME

Similar to Refs. [1,4], for the $\alpha < 1$ regime, we can instead derive *upper* bounds on the global Rényi entropy $H_\alpha^\uparrow(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho|_\Omega}$. This approach in turn yields upper bounds on the global smooth max-entropy $H_{\max}^\epsilon(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho|_\Omega}$ [e.g., via Lemma B.10 of Ref. [1], which includes a smooth max-entropy version of the bound in Eq. (87) in the opposite direction].

Some results in this appendix are more naturally stated in terms of Petz divergences and entropies, defined as follows. Note that, while we technically state definitions for $\alpha \in [0, \infty]$, the Petz divergences are not well behaved outside of $\alpha \in [0, 2]$; e.g., they may not satisfy data processing.

Definition E.1. For any $\rho, \sigma \in \text{Pos}(A)$ with $\text{Tr}[\rho] \neq 0$, and $\alpha \in (0, 1) \cup (1, \infty)$, the Petz divergence between ρ and σ is defined as

$$\bar{D}_\alpha(\rho || \sigma) = \frac{1}{\alpha - 1} \log \frac{\text{Tr}[\rho^\alpha \sigma^{1-\alpha}]}{\text{Tr}[\rho]}, \quad (\text{E1})$$

for $(\alpha < 1 \wedge \rho \not\subseteq \sigma)$ or $(\text{supp}(\rho) \subseteq \text{supp}(\sigma))$. Otherwise, we set $\bar{D}_\alpha(\rho||\sigma) = \infty$. For $\alpha > 1$, the $\sigma^{1-\alpha}$ term is defined via the Moore-Penrose pseudoinverse if σ is not full support [30]. The above definition is extended to $\alpha \in \{0, 1, \infty\}$ by taking the respective limits. Similar to the sandwiched Rényi divergences, for the $\alpha = 1$ case, it also reduces to the Umegaki divergence, and for classical states, it also reduces to the classical Rényi divergences.

Definition E.2. For any bipartite state $\rho \in \mathcal{S}_=(AB)$ and $\alpha \in [0, \infty]$, we define the following two Petz conditional entropies:

$$\begin{aligned}\bar{H}_\alpha(A|B)_\rho &= -\bar{D}_\alpha(\rho_{AB}||\mathbb{I}_A \otimes \rho_B), \\ \bar{H}_\alpha^\uparrow(A|B)_\rho &= \sup_{\sigma_B \in \mathcal{S}_=(B)} -\bar{D}_\alpha(\rho_{AB}||\mathbb{I}_A \otimes \sigma_B).\end{aligned}\quad (\text{E2})$$

For $\alpha = 1$, both the above values coincide and are equal to the von Neumann entropy.

For $\alpha \in [0, 2]$, the Petz divergences (and hence entropies) satisfy data processing [106] as in Fact II.1; similarly, for $\alpha \in (0, 1) \cup (1, 2)$, they obey the relations in Fact II.2 when conditioned on classical registers [technically, the relations for the cases of $\bar{D}_\alpha$ and $\bar{H}_\alpha$ hold more broadly over all of $\alpha \in (0, 1) \cup (1, \infty)$]. We define a Petz version of f -weighted entropies via the obvious analog (also discussed in Ref. [18], apart from the small differences mentioned in Remark IV.1):

Definition E.3. Let $\rho \in \mathcal{S}_=(\bar{C}\hat{C}QQ')$ be a state where $\bar{C}$ and $\hat{C}$ are classical with alphabets $\bar{\mathcal{C}}$ and $\hat{\mathcal{C}}$, respectively. Given a QES f on $\bar{C}\hat{C}$ and a value $\alpha \in (0, 1) \cup (1, \infty)$, we define

$$\begin{aligned}\bar{H}_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho &:= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c})^\alpha \rho(\hat{c})^{1-\alpha} 2^{(1-\alpha)(-f(\bar{c}\hat{c}) - \bar{D}_\alpha(\rho_{Q\bar{C}|\bar{c}\hat{c}}||\mathbb{I}_Q \otimes \rho_{Q'|\bar{c}\hat{c}}))} \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}\hat{c}} \rho(\bar{c}\hat{c}) 2^{(1-\alpha)(-f(\bar{c}\hat{c}) - \bar{D}_\alpha(\rho_{Q\bar{C}|\bar{c}\hat{c}}||\mathbb{I}_Q \otimes \rho_{Q'|\bar{c}\hat{c}}))} \right) \\ &= \frac{1}{1-\alpha} \log \left(\sum_{\bar{c}\hat{c}} 2^{-(1-\alpha)f(\bar{c}\hat{c})} \text{Tr}[(\rho_{Q\bar{C}|\bar{c}\hat{c}})^\alpha (\rho_{Q'|\bar{c}\hat{c}})^{1-\alpha}] \right),\end{aligned}\quad (\text{E3})$$

where the sum is over all $\bar{c}\hat{c}$ values such that $\rho(\bar{c}\hat{c}) > 0$, and we leave some tensor factors of identity implicit in the last expression.

We now present the $\alpha < 1$ version of Theorem IV.1. Note that this statement is slightly simpler in that it does not need the additional purifying registers $\bar{E}$ in the single-round terms because, by data processing, the maximum in those terms is always attainable by a state that is “trivial” on that register. In addition, our current version of this statement has the slight restriction that, while the QES choices can be different in each round, they cannot explicitly depend on the $\bar{c}_1^{j-1}\hat{c}_1^{j-1}$ values from previous rounds, unlike Theorem IV.1, because of a subtle difficulty regarding the NS conditions. We believe that this issue could be overcome, in principle, but we defer further discussion of this point until Remark E.1.

Theorem E.1. Let $\{\mathcal{M}_j\}_{j=1}^n$ be a sequence of channels $R_{j-1}E_{j-1} \rightarrow S_jR_jE_j\bar{C}_j\hat{C}_j$ such that the output registers $\bar{C}_j\hat{C}_j$ are always classical (for any input state), and let $\rho \in \mathcal{S}_=(S_1^n\bar{C}_1^n\hat{C}_1^nE_nR_n)$ be a state of the form $\rho = \mathcal{M}_n \circ \dots \circ \mathcal{M}_1[\omega^0]$ (leaving some identity channels implicit) for some initial state $\omega^0 \in \mathcal{S}_=(R_0E_0)$. Suppose that each $\mathcal{M}_j$ has some Stinespring dilation $V_j: R_{j-1}E_{j-1} \rightarrow S_jR_jE_j\bar{C}_j\hat{C}_jF_j$ (with “environment” system F_j), such that V_j satisfies the following NS condition: [107]

$\exists$ a channel $\mathcal{R}_j: R_{j-1} \rightarrow R_j\bar{C}_j\hat{C}_jF_j$ such that

$$\text{Tr}_{S_jE_j} \circ V_j = \mathcal{R}_j \circ \text{Tr}_{E_{j-1}}.$$

For each j , let $f_{|j}$ be a QES on registers $\bar{C}_j\hat{C}_j$. Define the following QES on $\bar{C}_1^n\hat{C}_1^n$:

$$f_{\text{full}}(\bar{c}_1^n\hat{c}_1^n) := \sum_{j=1}^n f_{|j}(\bar{c}_j\hat{c}_j). \quad (\text{E4})$$

Take any $\alpha \in (2/3, 1)$, and let $\tilde{\alpha} = [(3\alpha - 2)/(2\alpha - 1)]$. Then, we have

$$\begin{aligned}\bar{H}_\alpha^f(S_1^n\bar{C}_1^n|\hat{C}_1^nE_n)_\rho &\leq \sum_j \kappa_j, \\ \text{where } \kappa_j &:= \sup_{\nu \in \Sigma_j} \bar{H}_{\tilde{\alpha}}^{f_{|j}}(S_j\bar{C}_j|\hat{C}_jE_j)_\nu,\end{aligned}\quad (\text{E5})$$

where Σ_j denotes the set of all states of the form $\mathcal{M}_j[\omega_{R_{j-1}E_{j-1}}]$ for some initial state $\omega \in \mathcal{S}_=(R_{j-1}E_{j-1})$.

Consequently, if we instead define the following “normalized” QES on $\bar{C}_1^n\hat{C}_1^n$:

$$\hat{f}_{\text{full}}(\bar{c}_1^n \hat{c}_1^n) := \sum_{j=1}^n \hat{f}_{|j}(\bar{c}_j \hat{c}_j),$$

where $\hat{f}_{|j}(\bar{c}_j \hat{c}_j) := f_{|j}(\bar{c}_j \hat{c}_j) + \kappa_j$, (E6)

then

$$H_{\alpha}^{\hat{f}_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \leq 0. \quad (\text{E7})$$

Note that, again, if we write $\alpha = 1 - \mu$ for some $\mu > 0$, then

$$\tilde{\alpha} = \frac{1 - 3\mu}{1 - 2\mu} = 1 - \frac{\mu}{1 - 2\mu} = 1 - \mu - O(\mu^2), \quad (\text{E8})$$

so $\tilde{\alpha}$ is slightly “further from 1” than α but only by a “higher-order” amount. The NS condition might appear slightly elaborate, but as a simple example, we highlight that, as observed in Ref. [4], it is automatically fulfilled whenever the action of $\mathcal{M}_j$ is to first apply some arbitrary channel $\tilde{\mathcal{M}}_j: R_{j-1} \rightarrow S_j \bar{C}_j \hat{C}_j T_j R_j$ and then incorporate $\hat{C}_j T_j$ into the side information E_j without “disturbing” the state already on the register E_{j-1} [108]. This process fulfills the NS condition in Eq. (E4) without requiring any further structure (e.g., Markov conditions) on the channels. We now present the proof of the above theorem.

Proof. Again, let $M > 0$ be any value such that $M - f_{|j}(\bar{c}_j \hat{c}_j) > (M/2) > 0$ for all $f_{|j}(\bar{c}_j \hat{c}_j)$ in the theorem statement; then, for each j , define a read-and-prepare channel $\mathcal{D}_j: \bar{C}_j \hat{C}_j \rightarrow \bar{C}_j \hat{C}_j D_j$ of the form described in Lemma IV.2 so that the state it prepares on D_j always satisfies

$$M - f_{|j}(\bar{c}_j \hat{c}_j) \leq H_{\alpha}(D_j)_{\rho_{|\bar{c}_j \hat{c}_j}} \leq M - f_{|j}(\bar{c}_j \hat{c}_j) + 2^{-\frac{M}{2}} \log e, \quad (\text{E9})$$

for all $\alpha \in [0, \infty]$. Consider the channels $\mathcal{N}_j: R_{j-1} E_{j-1} \rightarrow D_j S_j R_j E_j \bar{C}_j \hat{C}_j$ defined by $\mathcal{N}_j := \mathcal{D}_j \circ \mathcal{M}_j$. (This is the same idea as the Theorem IV.1 proof, except that, since we now do not “track” the past $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ values, we can define these channels much more simply.) Again, view ρ in the theorem statement as the reduced state of an extended version $\rho = \mathcal{N}_n \circ \dots \circ \mathcal{N}_1[\omega^0]$. Our goal will be to prove the following bound (where, again, Σ'_j is the set of possible output states of $\mathcal{N}_j$, though here we do not need the purifying system $\tilde{E}$):

$$\bar{H}_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \leq \sum_j \sup_{\nu' \in \Sigma'_j} \bar{H}_{2-\frac{1}{\alpha}}^{\uparrow}(D_j S_j \bar{C}_j | \hat{C}_j E_j)_{\nu'}. \quad (\text{E10})$$

The remainder of the proof will then quickly follow the same way as before, up to some adjustments in Rényi parameters.

Let $U_j: \bar{C}_j \hat{C}_j \rightarrow \bar{C}_j \hat{C}_j D_j G_j$ be a Stinespring dilation of $\mathcal{D}_j$, in which case $U_j \circ V_j: R_{j-1} E_{j-1} \rightarrow D_j S_j R_j E_j \bar{C}_j \hat{C}_j F_j G_j$ is a Stinespring dilation of $\mathcal{N}_j$. We extend this trivially to another isometry $W_j := (U_j \circ V_j) \otimes \text{id}_{\hat{C}_1^{j-1} F_1^{j-1} G_1^{j-1}}$, i.e., an isometry with input and output registers given by

$$W_j: R_{j-1} E_{j-1} \hat{C}_1^{j-1} F_1^{j-1} G_1^{j-1} \rightarrow D_j S_j R_j E_j \bar{C}_j \hat{C}_j F_j G_j \hat{C}_1^j F_1^j G_1^j. \quad (\text{E11})$$

The purpose of constructing this extension is to ensure that the output registers can be exactly partitioned into registers that will appear on the “left side of the conditioning” in the desired bound (i.e., $D_j S_j \bar{C}_j$) and registers that will appear in the input registers of the subsequent W_j channel (i.e., $R_j E_j \hat{C}_1^j F_1^j G_1^j$), which is a structure we will need later in the proof.

Thus, we can view the state ρ in the above bounds as the reduced state of a pure state $|\rho\rangle_{D_1^n S_1^n R_n E_n \bar{C}_1^n \hat{C}_1^n F_1^n G_1^n \tilde{E}_0} := W_n \circ \dots \circ W_1 |\omega^0\rangle_{R_0 E_0 \tilde{E}_0}$, where $|\omega^0\rangle_{R_0 E_0 \tilde{E}_0}$ is a purification of $\omega_{R_0 E_0}^0$. Similarly, any $\nu' \in \Sigma'_j$ can be viewed as the reduced state of a pure state $|\nu'\rangle_{D_j S_j R_j E_j \bar{C}_j \hat{C}_j F_j G_j \tilde{E}} := W_j |\omega\rangle_{R_{j-1} E_{j-1} \hat{C}_1^{j-1} F_1^{j-1} G_1^{j-1} \tilde{E}}$, where $|\omega\rangle_{R_{j-1} E_{j-1} \hat{C}_1^{j-1} F_1^{j-1} G_1^{j-1} \tilde{E}}$ is a pure state (for some register $\tilde{E}$ of sufficiently large dimension). Then, by a duality relation (Theorem 2 in Ref. [77]) between the Rényi entropies $\bar{H}_{\alpha}^{\uparrow}$ and $H_{1/\alpha}$ (for all $\alpha \in [0, \infty]$), we have

$$\begin{aligned} \bar{H}_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n \tilde{E}_0)_{\rho} &= -H_{\beta}(D_1^n S_1^n \bar{C}_1^n | R_n F_1^n G_1^n)_{\rho}, \\ \text{where } \beta &= \frac{1}{\alpha}, \\ \bar{H}_{2-\frac{1}{\alpha}}^{\uparrow}(D_j S_j \bar{C}_j | \hat{C}_j E_j)_{\nu'} &= -H_{\hat{\beta}}(D_j S_j \bar{C}_j | R_j F_1^j G_1^j \tilde{E})_{\nu'}, \\ \text{where } \hat{\beta} &= \frac{1}{2-\frac{1}{\alpha}} = \frac{1}{2-\beta}. \end{aligned} \quad (\text{E12})$$

Note that since $\alpha \in (1/2, 1)$, we have $\beta \in (1, 2)$. We also highlight that we placed the purifications $\tilde{E}_0$ and $\tilde{E}$ on opposite sides in the above two equations to simplify some subsequent arguments.

Hence, our task basically reduces to relating $H_{\beta}(D_1^n S_1^n \bar{C}_1^n | R_n F_1^n G_1^n)_{\rho}$ and $H_{\hat{\beta}}(D_j S_j \bar{C}_j | R_j F_1^j G_1^j \tilde{E})_{\nu'}$. For this purpose, we show that the W_j form a sequence of GEAT channels (Definition III.1) satisfying NS conditions between suitable registers. Recall that each W_j channel has input registers $R_{j-1} E_{j-1} \hat{C}_1^{j-1} F_1^{j-1} G_1^{j-1}$, and partition them into “memory” registers $E_{j-1} \hat{C}_1^{j-1}$ (which do not appear in these entropy terms) and “side-information” registers $R_{j-1} F_1^{j-1} G_1^{j-1}$ (which appear in the conditioning registers of these entropy terms). Critically, the NS condition on V_j

implies that the W_j channels are nonsignaling from $E_{j-1}\hat{C}_1^{j-1}$ to $R_j F_1^j G_1^j$; more precisely, if we define a channel $\tilde{\mathcal{R}}_j := (\text{Tr}_{D_j \tilde{C}_j \hat{C}_j} \circ U_j \circ \mathcal{R}_j) \otimes \text{id}_{F_1^{j-1} G_1^{j-1}}$, where $\mathcal{R}_j$ is the channel in the theorem condition in Eq. (E4), then this is a channel $\tilde{\mathcal{R}}_j: R_{j-1} F_1^{j-1} G_1^{j-1} \rightarrow R_j F_1^j G_1^j$ such that (leaving various identity channels implicit)

$$\begin{aligned} \text{Tr}_{D_j S_j \tilde{C}_j E_j \hat{C}_1^j} \circ W_j &= \text{Tr}_{D_j S_j \tilde{C}_j E_j \hat{C}_1^j} \circ U_j \circ V_j \\ &= \text{Tr}_{D_j \tilde{C}_j \hat{C}_j} \circ U_j \circ \text{Tr}_{S_j E_j} \circ V_j \circ \text{Tr}_{\hat{C}_1^{j-1}} \\ &= \text{Tr}_{D_j \tilde{C}_j \hat{C}_j} \circ U_j \circ \mathcal{R}_j \circ \text{Tr}_{E_{j-1}} \circ \text{Tr}_{\hat{C}_1^{j-1}} \\ &= \tilde{\mathcal{R}}_j \circ \text{Tr}_{E_{j-1} \hat{C}_1^{j-1}}, \end{aligned} \quad (\text{E13})$$

where, in the second line, we commute some partial traces with channels that act purely as identity on the corresponding registers (namely, U_j acts as identity on $S_j E_j \hat{C}_1^{j-1}$ and V_j acts as identity on $\hat{C}_1^{j-1}$); in the third line, we apply the NS condition in Eq. (E4) imposed in the theorem; and in the fourth line, we substitute the definition of $\tilde{\mathcal{R}}_j$. Hence, the W_j form a sequence of GEAT channels, and with this sequence, we can finally apply (Lemma 3.6 of Ref. [4] and Fact III.1 stated above) to conclude that [since $\beta \in (1, 2)$ and $\hat{\beta} = 1/(2 - \beta)$]

$$\begin{aligned} H_\beta(D_1^n S_1^n \tilde{C}_1^n | R_n F_1^n G_1^n)_\rho \\ \geq \sum_j \inf_{\nu \in \Sigma_j''} H_{\hat{\beta}}(D_j S_j \tilde{C}_j | R_j F_1^j G_1^j \tilde{E})_\nu, \end{aligned} \quad (\text{E14})$$

where Σ_j'' denotes the set of all states of the form $W_j | \omega >_{R_{j-1} E_{j-1} \hat{C}_1^{j-1} F_1^{j-1} G_1^{j-1} \tilde{E}}$ for some ω .

Substituting the duality relations in Eq. (E12) and noting that the data-processing inequality implies $\bar{H}_\alpha^\dagger(D_1^n S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_\rho \leq \bar{H}_\alpha^\dagger(D_1^n S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n \tilde{E}_0)_\rho$, we obtain the desired bound in Eq. (E10). To obtain the claimed results in the theorem, we first use the inequalities $\bar{H}_\alpha \leq \bar{H}_\alpha^\dagger$ and $\bar{H}_\alpha^\dagger \leq \bar{H}_{2-\frac{1}{\alpha}}$ (Corollary 4 in Ref. [77]) on the left- and right-hand sides, respectively, to obtain

$$\begin{aligned} \bar{H}_\alpha(D_1^n S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_\rho &\leq \sum_j \sup_{\nu \in \Sigma_j'} \bar{H}_{\tilde{\alpha}}(D_j S_j \tilde{C}_j | \hat{C}_1^j E_j)_\nu \\ &\leq \sum_j \sup_{\nu \in \Sigma_j'} \bar{H}_{\tilde{\alpha}}(D_j S_j \tilde{C}_j | \hat{C}_j E_j)_\nu, \end{aligned} \quad (\text{E15})$$

where $\tilde{\alpha} = 2 - [1/(2 - \frac{1}{\alpha})] = [(3\alpha - 2)/(2\alpha - 1)]$, and the second line holds by data processing. These entropies can then be related to the (Petz) f -weighted entropies $\bar{H}_\alpha^{\text{full}}(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_\rho$ and $\bar{H}_{\tilde{\alpha}}^{f_{\tilde{\alpha}}}(S_j \tilde{C}_j | \hat{C}_j E_j)_\nu$ in the same way as in Lemma IV.2, noting that Petz divergences also satisfy the relations in Fact II.2, thus yielding the claimed bound in

Eq. (E5) by taking $M \rightarrow \infty$. The other claimed bound in Eq. (E6) is also obtained in a similar way: By Lemma IV.7, each $\hat{f}_{|j}$ satisfies

$$\sup_{\nu \in \Sigma_j} \bar{H}_{\tilde{\alpha}}^{f_{\tilde{\alpha}}}(S_j \tilde{C}_j | \hat{C}_j E_j)_\nu = \sup_{\nu \in \Sigma_j} \bar{H}_{\tilde{\alpha}}^{f_{\tilde{\alpha}}}(S_j \tilde{C}_j | \hat{C}_j E_j)_\nu - \kappa_j = 0. \quad (\text{E16})$$

Hence, applying Eq. (E5) to the QESs $\hat{f}_{|j}$ yields Eq. (E6). ■

We now state the analog of Theorem V.1. Here, we present it in terms of a rate-bounding channel (except one that instead upper bounds the entropies) to have a slightly wider scope as compared to presenting it using the convex range; however, from the discussion in Appendix D, we see that both approaches would be very similar. (In either case, it is unnecessary to consider the additional purifying register $\tilde{E}$, for the reasons discussed earlier.)

Theorem E.2. Consider a state ρ and channels $\{\mathcal{M}_j\}_{j=1}^n$ fulfilling the conditions described in Theorem E.1, such that, furthermore, all $\tilde{C}_j$ (respectively, $\hat{C}_j$) are isomorphic to a single register $\tilde{C}$ (respectively, $\hat{C}$) with alphabet $\tilde{\mathcal{C}}$ (respectively, $\hat{\mathcal{C}}$). Let $\mathcal{M}: \tilde{\mathcal{Q}} \rightarrow SE\tilde{C}\hat{C}$ be a channel such that, for any QES f on $\tilde{C}\hat{C}$ and any $\alpha \in (0, 1)$, we have

$$\max_j \sup_{\nu \in \Sigma_j} \bar{H}_\alpha^f(S_j \tilde{C}_j | \hat{C}_j E_j)_\nu \leq \sup_{\nu \in \Sigma} \bar{H}_\alpha^f(S\tilde{C} | \hat{C}E)_\nu, \quad (\text{E17})$$

where Σ_j denotes the set of all states of the form $\mathcal{M}_j[\omega_{R_{j-1} E_{j-1}}]$ for some initial state $\omega \in S_{=}(R_{j-1} E_{j-1})$ and, analogously, Σ denotes the set of all states of the form $\mathcal{M}[\omega_{\tilde{\mathcal{Q}}}]$ for some initial state $\omega \in S_{=}(\tilde{\mathcal{Q}})$.

Take any $\alpha \in (3/4, 1)$, and let $\tilde{\alpha} = [(4\alpha - 3)/(3\alpha - 2)]$. Suppose, furthermore, that $\rho = p_\Omega \rho_{|\Omega} + (1 - p_\Omega) \rho_{|\bar{\Omega}}$ for some $p_\Omega \in (0, 1]$ and normalized states $\rho_{|\Omega}, \rho_{|\bar{\Omega}}$. Let S_Ω be a convex set of probability distributions on the alphabet $\tilde{\mathcal{C}} \times \hat{\mathcal{C}}$, such that for all $\tilde{c}_1^n \hat{c}_1^n$ with nonzero probability in $\rho_{|\Omega}$, the frequency distribution $\text{freq}_{\tilde{c}_1^n \hat{c}_1^n}$ lies in S_Ω . Then, letting $\sigma_{\tilde{C}\hat{C}}$ denote the distribution on $\tilde{C}\hat{C}$ induced by any state $\sigma_{\tilde{C}\hat{C}}$, we have

$$\begin{aligned} H_\alpha^\dagger(S_1^n \tilde{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}} &\leq n \bar{h}_{\tilde{\alpha}} + \frac{\alpha}{1 - \alpha} \log \frac{1}{p_\Omega}, \\ \text{where } \bar{h}_{\tilde{\alpha}} &= \sup_{\mathbf{q} \in S_\Omega} \sup_{\nu \in \Sigma} \left(-\frac{1}{1 - \tilde{\alpha}} D(\mathbf{q} \| \nu_{\tilde{C}\hat{C}}) \right. \\ &\quad \left. - \sum_{\tilde{c}\hat{c} \in \text{supp}(\nu_{\tilde{C}\hat{C}})} q(\tilde{c}\hat{c}) \bar{D}_{\tilde{\alpha}}(\nu_{SE\tilde{c}\hat{c}} \| \mathbb{I}_S \otimes \nu_{E\hat{c}}) \right), \end{aligned} \quad (\text{E18})$$

and the objective function in the above supremum is jointly concave in ν and $\mathbf{q}$. Furthermore, for any $\alpha', \alpha'' \in (1/2, 1)$ such that $[\tilde{\alpha}/(\tilde{\alpha} - 1)] = [\alpha'/(\alpha' - 1)] + [\alpha''/(\alpha'' - 1)]$, we have

$$\bar{h}_{\bar{\alpha}} \leq \sup_{\mathbf{q} \in S_{\Omega}} \sup_{\nu \in \Sigma} \left(-\frac{\alpha''}{1-\alpha''} D(\mathbf{q} \| \nu_{\bar{C}\hat{C}}) + H_{\alpha'}(S\bar{C}|\hat{C}E)_{\nu} \right), \quad (\text{E19})$$

and the objective function in the above supremum is jointly concave in ν and $\mathbf{q}$.

Again, if we write $\alpha = 1 - \mu$ for some $\mu > 0$, then

$$\bar{\alpha} = \frac{1-4\mu}{1-3\mu} = 1 - \frac{\mu}{1-3\mu} = 1 - \mu - O(\mu^2), \quad (\text{E20})$$

so $\bar{\alpha}$ is slightly “further from 1” than α but only by a higher-order amount. [In fact, more precisely, the $O(\mu^2)$ terms in Eqs. (64), (E8), and (E20) have the forms $\mu^2 + O(\mu^3)$, $2\mu^2 + O(\mu^3)$, $3\mu^2 + O(\mu^3)$, respectively, as one might perhaps expect by counting the number of Rényi parameter changes in the various proofs.] Hence, the KL divergence term has a negative prefactor in this case and thus can be interpreted as a “penalty function” in the concave maximization that defines $\bar{h}_{\bar{\alpha}}$, just as described in Sec. VB. Furthermore, if the $\bar{C}_j$ registers are trivial, then we again have a similar result to Lemma V.1:

$$\begin{aligned} \bar{h}_{\bar{\alpha}} = & \sup_{\mathbf{q} \in S_{\Omega}} \sup_{\nu \in \Sigma} \left(-\frac{1}{1-\bar{\alpha}} D(\mathbf{q} \| \nu_{\hat{C}}) \right. \\ & \left. + \sum_{\hat{C} \in \text{supp}(\nu_{\hat{C}})} q(\hat{C}) \bar{H}_{\bar{\alpha}}(S|\hat{C}E)_{\nu} \right), \quad (\text{E21}) \end{aligned}$$

simply because $\bar{D}_{\bar{\alpha}}(\nu_{SE \wedge \hat{C}} \| \mathbb{I}_S \otimes \nu_{E \wedge \hat{C}}) = -\bar{H}_{\bar{\alpha}}(S|\hat{C}E)_{\nu}$. Perhaps somewhat curiously though, if the $\bar{C}_j$ registers are nontrivial, then it seems less straightforward to obtain an analog of that lemma—essentially, the data-processing inequality is in the “wrong direction” for an analogous proof to carry through. Still, we highlight that, since the required conditions on the channels are in fact quite minimal (as discussed below Theorem E.1 and in Ref. [4]), for practical applications, it might be possible to focus on the case where $\bar{C}_j$ is trivial. Alternatively, one could work with the looser bound in Eq. (E19) (which is analogous to Lemma V.2), possibly using the “projective reconstruction” property in Lemma B.7 of Ref. [1] to add or remove the $\bar{C}_j$ registers as necessary. We leave a detailed resolution of this question for future work.

Proof. The proof is again analogous to our proof of Theorem V.1; we highlight the key steps. It is slightly more convenient to start from the intermediate bound in Eq. (E10) in the preceding proof, which we use to obtain a slightly looser bound,

$$\begin{aligned} H_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} & \leq \bar{H}_{2-\frac{1}{\alpha}}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} \\ & \leq \sum_j \sup_{\nu' \in \Sigma_j'} \bar{H}_{\bar{\alpha}}^{\uparrow}(D_j S_j \bar{C}_j | \hat{C}_j^j E_j)_{\nu'}, \\ \text{where } \tilde{\alpha} = 2 - \frac{1}{2-\frac{1}{\alpha}} & = \frac{3\alpha-2}{2\alpha-1}, \\ & \leq \sum_j \sup_{\nu' \in \Sigma_j'} \bar{H}_{\bar{\alpha}}(D_j S_j \bar{C}_j | \hat{C}_j^j E_j)_{\nu'}, \\ \text{where } \bar{\alpha} = 2 - \frac{1}{\tilde{\alpha}} & = \frac{4\alpha-3}{3\alpha-2}, \\ & \leq \sum_j \sup_{\nu' \in \Sigma_j'} \bar{H}_{\bar{\alpha}}(D_j S_j \bar{C}_j | \hat{C}_j E_j)_{\nu'}. \quad (\text{E22}) \end{aligned}$$

In the first and third lines, we used the bounds $H_{\alpha}^{\uparrow} \leq \bar{H}_{2-\frac{1}{\alpha}}^{\uparrow}$ and $\bar{H}_{\alpha}^{\uparrow} \leq \bar{H}_{2-\frac{1}{\alpha}}$ (Corollary 4 in Ref. [77]), respectively; the second line is Eq. (E10); and the last line is from data processing.

We relate the $H_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho}$ term to $H_{\alpha}^{\uparrow}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}}$ in a similar fashion to the Corollary IV.1 proof, letting $\tilde{\Omega}$ denote the set of all $\bar{c}_1^n \hat{c}_1^n$ values such that $\text{freq}_{\bar{c}_1^n \hat{c}_1^n} \in S_{\Omega}$:

$$\begin{aligned} H_{\alpha}^{\uparrow}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}} & \leq H_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_{|\Omega}} - \min_{\bar{c}_1^n \hat{c}_1^n \in \tilde{\Omega}} H_{\alpha}(D_1^n)_{\rho_{|\bar{c}_1^n \hat{c}_1^n}} \\ & \leq H_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} - \min_{\bar{c}_1^n \hat{c}_1^n \in \tilde{\Omega}} H_{\alpha}(D_1^n)_{\rho_{|\bar{c}_1^n \hat{c}_1^n}} \\ & \quad + \frac{\alpha}{1-\alpha} \log \frac{1}{p_{\Omega}} \\ & \leq H_{\alpha}^{\uparrow}(D_1^n S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho} + \max_{\bar{c}_1^n \hat{c}_1^n \in \tilde{\Omega}} -H_{\alpha}(D_1^n)_{\rho_{|\bar{c}_1^n \hat{c}_1^n}} \\ & \quad + \frac{\alpha}{1-\alpha} \log \frac{1}{p_{\Omega}}, \quad (\text{E23}) \end{aligned}$$

where the second line holds by similar arguments to the Lemma IV.9 proof and the third line is (Lemma B.5 in Ref. [1]) in the $\alpha < 1$ regime.

Thus, by picking all the QESs $f_{|j}$ to be equal to a single QES f , and relating the entropies of the D_j registers to the QES values in the same way as in Lemma IV.2, followed by taking the $M \rightarrow \infty$ limit, we obtain an analog of Corollary V.1:

$$\begin{aligned}
H_\alpha^\dagger(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_{\rho_\Omega} &\leq n \sup_{\nu \in \Sigma} \bar{H}_\alpha^f(S\bar{C} | \hat{C}E)_\nu \\
&\quad + \max_{\bar{c}_1^n \hat{c}_1^n \in \bar{\Omega}} \sum_{j=1}^n f(\bar{c}_j \hat{c}_j) + \frac{\alpha}{1-\alpha} \log \frac{1}{p_\Omega} \\
&\leq \sup_{\mathbf{q} \in S_\Omega} \sup_{\nu \in \Sigma} (\bar{H}_\alpha^f(S\bar{C} | \hat{C}E)_\nu + \mathbf{f} \cdot \mathbf{q}) n \\
&\quad + \frac{\alpha}{1-\alpha} \log \frac{1}{p_\Omega}. \tag{E24}
\end{aligned}$$

The best upper bound would be given by minimizing over the choice of QES f on the right-hand side; hence, we only need to show that this yields the claimed formula for $\bar{h}_{\bar{\alpha}}$, analogous to the strong duality proof in Lemma V.4. For this purpose, we define a sign-flipped version of $G_{\alpha,\rho}$ from Lemma V.3 (to avoid having to introduce and discuss “concave conjugates”), with Petz instead of sandwiched divergences:

$$\hat{G}_{\alpha,\rho}(\mathbf{f}) := \bar{H}_\alpha^f(Q\bar{C} | \hat{C}Q')_\rho. \tag{E25}$$

From the log-sum-exponential formulation in Eq. (B13) (with a sign flip), we see that $\hat{G}_{\alpha,\rho}(\mathbf{f})$ is again convex in $\mathbf{f}$ since $\alpha < 1$; by analogous calculations, we find that its convex conjugate is

$$\begin{aligned}
\hat{G}_{\alpha,\rho}^*(\lambda) &:= \frac{1}{1-\alpha} D(-\lambda \| \rho_{\bar{C}\hat{C}}) \\
&\quad - \sum_{\bar{c}\hat{c} \in \text{supp}(\rho_{\bar{C}\hat{C}})} \lambda(\bar{c}\hat{c}) \bar{D}_\alpha(\rho_{Q\bar{C}Q' \wedge \bar{c}\hat{c}} \| \mathbb{I}_Q \otimes \rho_{Q' \wedge \hat{c}})
\end{aligned} \tag{E26}$$

if $-\lambda \in \mathbb{P}_{\bar{C}\hat{C}}$ and $+\infty$ otherwise. Again, since $\hat{G}_{\alpha,\rho}$ is a convex function with domain $\mathbb{R}^{[\bar{C} \times \hat{C}]}$, we find that $\hat{G}_{\alpha,\rho}$ is also the convex conjugate of $\hat{G}_{\alpha,\rho}^*$; thus, we have $\hat{G}_{\alpha,\rho}(\mathbf{f}) = \sup_{\lambda \in \mathbb{R}^{[\bar{C} \times \hat{C}]}} (\lambda \cdot \mathbf{f} - \hat{G}_{\alpha,\rho}^*(\lambda))$. Therefore, we again write

$$\begin{aligned}
\bar{H}_\alpha^f(S\bar{C} | \hat{C}E)_\nu + \mathbf{f} \cdot \mathbf{q} &= \hat{G}_{\bar{\alpha},\nu}(\mathbf{f}) + \mathbf{f} \cdot \mathbf{q} \\
&= \sup_{\lambda \in \mathbb{R}^{[\bar{C} \times \hat{C}]}} (\lambda \cdot \mathbf{f} - \hat{G}_{\bar{\alpha},\nu}^*(\lambda) + \mathbf{f} \cdot \mathbf{q}) \\
&= \sup_{\lambda' \in \mathbb{P}_{\bar{C}\hat{C}}} (-\hat{G}_{\bar{\alpha},\nu}^*(-\lambda') + \mathbf{f} \cdot (\mathbf{q} - \lambda')),
\end{aligned} \tag{E27}$$

where the last line holds via a reparametrization $\lambda' = -\lambda$. Furthermore, by Lemma IV.1 (adapted to the Petz case), we know there exists a read-and-prepare channel that can extend any state ν so that we have $\bar{H}_\alpha^f(S\bar{C} | \hat{C}E)_\nu = \bar{H}_{\bar{\alpha}}(D\bar{S}\bar{C} | \hat{C}E)_\nu - M$ for some fixed M ; it thus follows from the convexity of Petz divergences for $\alpha \in (0, 1]$ that $\bar{H}_\alpha^f(S\bar{C} | \hat{C}E)_\nu$ is concave in ν . (Here, we do not need to exploit

purifying functions because, in this Rényi parameter regime, $\bar{H}_{\bar{\alpha}}$ is genuinely concave with respect to the state.) Therefore, we can proceed similarly to the Lemma V.4 proof: We see that $\hat{G}_{\bar{\alpha},\nu}^*(\lambda)$ is jointly convex in (λ, ν) since, by definition, it is a supremum over a family of functions $\lambda \cdot \mathbf{f} - \hat{G}_{\bar{\alpha},\nu}(\mathbf{f})$ that are each jointly convex in (λ, ν) . Therefore, $-\hat{G}_{\bar{\alpha},\nu}^*(-\lambda') + \mathbf{f} \cdot (\mathbf{q} - \lambda')$ is jointly concave in $(\mathbf{q}, \nu, \lambda')$, which allows us to apply the same strong duality arguments to conclude that

$$\begin{aligned}
&\inf_{\mathbf{f}} \sup_{\mathbf{q} \in S_\Omega} \sup_{\nu \in \Sigma} \sup_{\lambda' \in \mathbb{P}_{\bar{C}\hat{C}}} (-\hat{G}_{\bar{\alpha},\nu}^*(-\lambda') + \mathbf{f} \cdot (\mathbf{q} - \lambda')) \\
&= \sup_{\mathbf{q} \in S_\Omega} \sup_{\nu \in \Sigma} -\hat{G}_{\bar{\alpha},\nu}^*(-\mathbf{q}).
\end{aligned} \tag{E28}$$

This process gives the first claimed result in Eq. (E18) by just substituting the definition of $-\hat{G}_{\bar{\alpha},\nu}^*(-\mathbf{q})$. To obtain the looser bound in Eq. (E19), we perform similar calculations except with the relaxation

$$H_{\bar{\alpha}}(D\bar{S}\bar{C} | \hat{C}E)_\nu \leq H_{\alpha'}(S\bar{C} | \hat{C}E)_\nu + H_{\alpha'}^\dagger(D | S\bar{C} \hat{C}E)_\nu, \tag{E29}$$

which is a special case of Proposition 8 in Ref. [42]; this approach lets us apply the same arguments as the Lemma V.2 proof. ■

Remark E.1. In the Theorem E.1 proof, the obstruction to allowing the QESs to depend on the past $\bar{C}_j \hat{C}_j$ values is that, in this case, it seems we would need to define the $\mathcal{N}_j$ channels the same way as the Theorem IV.1 proof, in which case, they act “nontrivially” on the $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ registers (albeit only in a read-and-prepare fashion). However, to apply Fact III.1, it seems we would then need an NS condition from $E_{j-1} \bar{C}_1^{j-1} \hat{C}_1^{j-1}$ to $R_j F_j^j G_j^j$, which would not be satisfied since this construction of the $\mathcal{N}_j$ channels would nontrivially signal from the $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$ registers to the Stinespring dilation F_j . A different arrangement of the conditioning registers might resolve this issue, but we leave it for future work [109].

As a purely informal nonrigorous remark, however, we note that the role of the NS condition in deriving upper bounds on, e.g., $\bar{H}_\alpha^{f_{\text{full}}}(S_1^n \bar{C}_1^n | \hat{C}_1^n E_n)_\rho$ appears to be a way to enforce that the channels do not “destroy” information in the conditioning systems since it would be impossible to derive useful upper bounds if they do so. More specifically, if the Stinespring dilation of a channel does not “signal out of” some registers, it informally seems to imply that it “preserves the information” in those registers, as we would want. However, we note that the NS condition seems to be “too strong” as a method to enforce this information-preserving property—for instance, if the $\mathcal{D}_j$ read-and-prepare channels acted on $\bar{C}_1^{j-1} \hat{C}_1^{j-1}$, this would still preserve the information on them, despite violating the

NS condition in the form described above. Hence, the NS condition may not be the optimal way to approach this proof (or perhaps this obstacle can be overcome by finding an appropriate Stinespring dilation that correctly enforces this information-preserving property via the NS condition).

Separately, we also observe that our above proofs involved multiple changes in Rényi parameter (albeit only higher-order changes) to convert between sandwiched and Petz entropies or between $\bar{H}_\alpha$ and $\bar{H}_\alpha^\uparrow$. It would be convenient if the argument could be streamlined to avoid some of these conversions, for instance, by defining some notion of $\bar{H}_\alpha^{\uparrow f}(Q\bar{C}|\hat{C}Q')$. However, as noted in Remark IV.1, care would be needed regarding how to define the optimization over the second arguments of the divergence terms in that case.

Finally, we could again perform the above proof under the Markov conditions of the original EAT instead, so we could use Corollary 3.5 of Ref. [1] in place of Lemma 3.6 of Ref. [4] (i.e., Fact III.1). In that case, we expect there would be no changes of Rényi parameter since that statement directly bounds the sandwiched entropies H_α [basically, Eq. (117) holds in the opposite direction, with a supremum instead of infimum], and we could replace Lemma B.5 of Ref. [1] with Lemma B.6 of Ref. [1] (which only works for the $\alpha < 1$ regime) to avoid needing a conversion to $H_\alpha^\uparrow$ when conditioning on Ω . This approach might also allow the QESs to depend on the past $\bar{C}_1^{j-1}\hat{C}_1^{j-1}$ values by incorporating them into the conditioning registers in such a way that the Markov conditions hold. However, we defer this issue to be resolved in future work if it should become important—we believe that the conditions in Theorem E.1 are sufficiently less restrictive that it would be of more general use than a version with the Markov condition, even with the aforementioned drawbacks.

APPENDIX F: ONE-SHOT CHAIN RULE

We thank Ashutosh Marwah for providing us with the proof of this claim. For our calculations here, we briefly make use of the Petz entropies as presented in Definition E.2.

Lemma F.1. For any $\rho \in \mathcal{S}_=(A_1A_2B)$ and $\alpha \in [1/2, \infty]$, we have

$$\begin{aligned} H_\alpha^\uparrow(A_1|A_2B)_\rho &\geq H_\alpha^\uparrow(A_1A_2|B)_\rho - \bar{H}_0^\uparrow(A_2|B)_\rho \\ &\geq H_\alpha^\uparrow(A_1A_2|B)_\rho - H_0^\uparrow(A_2|B)_\rho. \end{aligned} \quad (\text{F1})$$

Consequently, for any $\rho \in \mathcal{S}_=(A_1A_2B_1B_2)$ and $\alpha \in [1/2, \infty]$, we have

$$\begin{aligned} H_\alpha^\uparrow(A_1|A_2B_1B_2)_\rho &\geq H_\alpha^\uparrow(A_1A_2|B_1B_2)_\rho - \bar{H}_0^\uparrow(A_2|B_2)_\rho \\ &\geq H_\alpha^\uparrow(A_1A_2|B_1B_2)_\rho - H_0^\uparrow(A_2|B_2)_\rho. \end{aligned} \quad (\text{F2})$$

If the registers in the $\bar{H}_0^\uparrow$ and $H_0^\uparrow$ terms are classical, then there is no difference between those versions of the bounds since those values are then equal as mentioned previously.

Proof. Let $\beta \in [1/2, \infty]$ be such that $1/\alpha + 1/\beta = 2$, and purify ρ onto some register C . Focusing on the registers A_1A_2C , by Corollary C.3 of Ref. [110,111] [and also implicitly observed in Eq. (44) of Ref. [1]], we have the following chain rule, for any $\sigma \in \mathcal{S}_=(C)$ such that $H_\beta^\uparrow(A_1|C)_\rho = -D_\beta(\rho_{A_1C}||\mathbb{I}_{A_1} \otimes \sigma_C)$:

$$H_\beta^\uparrow(A_1A_2|C)_\rho \geq H_\beta^\uparrow(A_1|C)_\rho + H_\beta(A_2|A_1C)_\nu, \quad (\text{F3})$$

where $\nu \in \mathcal{S}_=(A_2A_1C)$ is a state defined by

$$\begin{aligned} \nu_{A_2A_1C} &:= \nu_{A_1C}^{1/2} \rho_{A_1C}^{-1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} \nu_{A_1C}^{1/2}, \\ \text{where } \nu_{A_1C} &:= \frac{(\rho_{A_1C}^{1/2} \sigma_C^{\frac{1-\beta}{\beta}} \rho_{A_1C}^{1/2})^\beta}{\text{Tr}[(\rho_{A_1C}^{1/2} \sigma_C^{\frac{1-\beta}{\beta}} \rho_{A_1C}^{1/2})^\beta]} \in \mathcal{S}_=(A_1C), \end{aligned} \quad (\text{F4})$$

leaving some tensor factors of identity implicit for brevity and defining $\rho_{A_1C}^{-1/2}$ via the Moore-Penrose pseudoinverse if ρ_{A_1C} is not full support. Note that, from the definition of ν_{A_1C} , we immediately see that $\ker(\rho_{A_1C}) \subseteq \ker(\nu_{A_1C})$, and therefore,

$$\text{supp}(\nu_{A_1C}) \subseteq \text{supp}(\rho_{A_1C}), \quad (\text{F5})$$

a property we will soon need.

Importantly, the state ν satisfies

$$H_\beta(A_2|A_1C)_\nu \geq H_\infty(A_2|A_1C)_\nu \geq H_\infty(A_2|A_1C)_\rho, \quad (\text{F6})$$

where the first inequality is simply by monotonicity in β and the second inequality follows from the SDP characterization of D_∞ (Ref. [112] and Proposition 4.3 of Ref. [30]), as follows:

$$\begin{aligned} D_\infty(\rho_{A_2A_1C}||\mathbb{I}_{A_2} \otimes \rho_{A_1C}) &= \inf \{ \lambda | \rho_{A_2A_1C} \leq 2^\lambda \mathbb{I}_{A_2} \otimes \rho_{A_1C} \} \\ &= \inf \{ \lambda | \rho_{A_1C}^{-1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} \leq 2^\lambda \mathbb{I}_{A_2} \otimes \mathbb{I}_{\text{supp}(\rho_{A_1C})} \} \\ &\geq \inf \{ \lambda | \nu_{A_1C}^{1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} \nu_{A_1C}^{1/2} \leq 2^\lambda \mathbb{I}_{A_2} \otimes \nu_{A_1C} \} \\ &= \inf \{ \lambda | \nu_{A_2A_1C} \leq 2^\lambda \mathbb{I}_{A_2} \otimes \nu_{A_1C} \} \\ &= D_\infty(\nu_{A_2A_1C}||\mathbb{I}_{A_2} \otimes \nu_{A_1C}), \end{aligned} \quad (\text{F7})$$

where $\mathbb{I}_{\text{supp}(\rho_{A_1C})}$ denotes the projector on $\text{supp}(\rho_{A_1C})$. In the above, the third and fourth lines hold because $M \geq N \Rightarrow L^\dagger ML \geq L^\dagger NL$ for any operator L , and thus

$$\begin{aligned}
\rho_{A_2A_1C} &\leq 2^\lambda \mathbb{I}_{A_2} \otimes \rho_{A_1C} \\
&\Leftrightarrow \rho_{A_1C}^{-1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} \leq 2^\lambda \mathbb{I}_{A_2} \otimes \mathbb{I}_{\text{supp}(\rho_{A_1C})}, \\
&\Rightarrow \nu_{A_1C}^{1/2} \rho_{A_1C}^{-1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} \nu_{A_1C}^{1/2} \leq 2^\lambda \mathbb{I}_{A_2} \otimes \nu_{A_1C}, \quad (\text{F8})
\end{aligned}$$

where the first implication is bidirectional because we have both $\rho_{A_1C}^{-1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} = \mathbb{I}_{\text{supp}(\rho_{A_1C})}$ and $\rho_{A_1C}^{1/2} \mathbb{I}_{\text{supp}(\rho_{A_1C})} \rho_{A_1C}^{1/2} = \rho_{A_1C}$ (and also $\rho_{A_1C}^{1/2} \rho_{A_2A_1C} \rho_{A_1C}^{-1/2} \rho_{A_1C}^{1/2} = \rho_{A_2A_1C}$), while the second implication is just in one direction because we can only be sure that $\nu_{A_1C}^{1/2} \mathbb{I}_{\text{supp}(\rho_{A_1C})} \nu_{A_1C}^{1/2} = \nu_{A_1C}$ [due to Eq. (F5)] not $\nu_{A_1C}^{-1/2} \nu_{A_1C} \nu_{A_1C}^{-1/2} \stackrel{?}{=} \mathbb{I}_{\text{supp}(\rho_{A_1C})}$ [113].

Therefore, we can conclude that

$$H_\beta^\uparrow(A_1A_2|C)_\rho \geq H_\beta^\uparrow(A_1|C)_\rho + H_\infty(A_2|A_1C)_\rho, \quad (\text{F9})$$

and by applying the duality relations $H_\beta^\uparrow(A_1A_2|C)_\rho = -H_\alpha^\uparrow(A_1A_2|B)_\rho$, $H_\beta^\uparrow(A_1|C)_\rho = -H_\alpha^\uparrow(A_1|A_2B)_\rho$ for $H_\alpha^\uparrow$ [32,33] and $H_\infty(A_2|A_1C)_\rho = -\bar{H}_0^\uparrow(A_2|B)_\rho$ between sandwiched and Petz entropies [77], the above is equivalent to

$$H_\alpha^\uparrow(A_1A_2|B)_\rho \leq H_\alpha^\uparrow(A_1|A_2B)_\rho + \bar{H}_0^\uparrow(A_2|B)_\rho. \quad (\text{F10})$$

This approach yields our claimed bounds in Eq. (F1) [where the second line follows from the generic relation $H_\alpha^\uparrow \geq \bar{H}_\alpha^\uparrow$ between sandwiched and Petz entropies; see Eq. (4.88) in Ref. [30]]. To obtain our claimed bounds in Eq. (F2), we simply set $B := B_1B_2$ in the first line of Eq. (F1) and apply the data-processing inequality $\bar{H}_0^\uparrow(A_2|B_1B_2)_\rho \leq \bar{H}_0^\uparrow(A_2|B_2)_\rho$ for Petz entropies (see the statements below Definition E.2) and then again apply $H_\alpha^\uparrow \geq \bar{H}_\alpha^\uparrow$. [We do not directly obtain the second line in Eq. (F2) by data processing on $H_0^\uparrow$ because it was shown in Ref. [45] that the sandwiched entropies do not satisfy data processing for $\alpha \in (0, 1/2)$; that work does not explicitly specify the $\alpha = 0$ case, but the construction may generalize accordingly]. ■

distribution with characterized devices using entropy accumulation, [arXiv:2203.06554v1](https://arxiv.org/abs/2203.06554).

- [6] M. Tomamichel and A. Leverrier, *A largely self-contained and complete security proof for quantum key distribution*, *Quantum* **1**, 14 (2017).
- [7] Charles Ci-Wen Lim, F. Xu, J.-W. Pan, and A. Ekert, *Security analysis of quantum key distribution with small block length and its application to quantum space communications*, *Phys. Rev. Lett.* **126**, 100501 (2021).
- [8] While intermediate steps in the entropy accumulation proofs of Refs. [1,2,4] involve bounds of a roughly similar form, the critical difference is that, in those bounds, the value on the right-hand side is a minimization over *all* possible single-round states, which results in trivial bounds if directly applied in a protocol.
- [9] In fact, the $[\alpha/(\alpha-1)] \log[1/(\Pr[\Omega])]$ term does not affect the final key rates in sufficiently “simple” protocols, as discussed in Refs. [10,11]; however, other $O(1)$ corrections arise when considering, e.g., privacy amplification theorems.
- [10] F. Dupuis, *Privacy amplification and decoupling without smoothing*, *IEEE Trans. Inf. Theory* **69**, 7784 (2023).
- [11] L. Kamin, A. Arqand, I. George, N. Lütkenhaus, and Ernest Y.-Z. Tan, *Finite-size analysis of prepare-and-measure and decoy-state quantum key distribution via entropy accumulation*, *PRX Quantum* **6**, 020342 (2025).
- [12] S. Pironio and S. Massar, *Security of practical private randomness generation*, *Phys. Rev. A* **87**, 012336 (2013).
- [13] R. Jain, C. A. Miller, and Y. Shi, *Parallel device-independent quantum key distribution*, *IEEE Trans. Inf. Theory* **66**, 5567 (2020).
- [14] T. Vidick, *Parallel DIQKD from parallel repetition*, [arXiv:1703.08508](https://arxiv.org/abs/1703.08508).
- [15] R. Jain and S. Kundu, *A direct product theorem for quantum communication complexity with applications to device-independent cryptography*, *SIAM J. Comput.* **54**, 964 (2025).
- [16] A caveat here is that if the security proof uses a constant Rényi parameter independent of n , then the h_α term in our result is also independent of n —thus, even at large n , it does not converge to exactly the minimum Rényi entropy over single-round states compatible with the accept condition. This finding likely reflects the general principle that Rényi entropies have “worse” chain rules as compared to von Neumann entropy. However, for the purposes of security proofs, we can overcome this issue in various ways by tuning the Rényi parameters as a function of n ; we discuss this case further in Sec. VII C.
- [17] T. van Himbeek and P. Brown, *Tight and general finite-size security of quantum key distribution* (2025), presented at QCrypt 2023 and QIP 2024 (to be published).
- [18] Y. Zhang, H. Fu, and E. Knill, *Efficient randomness certification by quantum probability estimation*, *Phys. Rev. Res.* **2**, 013016 (2020).
- [19] R. Arnon-Friedman and J.-D. Bancal, *Device-independent certification of one-shot distillable entanglement*, *New J. Phys.* **21**, 033010 (2019).
- [20] S. Bäuml, C. Pascual-García, V. Wright, O. Fawzi, and A. Acín, *Security of discrete-modulated continuous-variable quantum key distribution*, *Quantum* **8**, 1418 (2024).

- [1] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation*, *Commun. Math. Phys.* **379**, 867 (2020).
- [2] F. Dupuis and O. Fawzi, *Entropy accumulation with improved second-order term*, *IEEE Trans. Inf. Theory* **65**, 7596 (2019).
- [3] T. Metger, O. Fawzi, D. Sutter, and R. Renner, *Generalised entropy accumulation*, in *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)* (2022), pp. 844–850, [10.1109/FOCS54457.2022.00085](https://doi.org/10.1109/FOCS54457.2022.00085).
- [4] T. Metger, O. Fawzi, D. Sutter, and R. Renner, *Generalised entropy accumulation*, *Commun. Math. Phys.* **405**, 261 (2024).
- [5] I. George, J. Lin, T. van Himbeek, K. Fang, and N. Lütkenhaus, *Finite-key analysis of quantum key*

- [21] T. Metger and R. Renner, *Security of quantum key distribution from generalised entropy accumulation*, *Nat. Commun.* **14**, 1 (2023).
- [22] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, *Phys. Rev. Lett.* **68**, 557 (1992).
- [23] A. Ferenczi and N. Lütkenhaus, *Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning*, *Phys. Rev. A* **85**, 052310 (2012).
- [24] R. Renner, *Security of quantum key distribution*, Ph.D. thesis, Swiss Federal Institute of Technology Zurich (ETH Zurich), 2005, diss. ETH No. 16242.
- [25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2010).
- [26] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, England, 2004).
- [27] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution*, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [28] J. Lin and N. Lütkenhaus, *Simple security analysis of phase-matching measurement-device-independent quantum key distribution*, *Phys. Rev. A* **98**, 042332 (2018).
- [29] R. Arnon-Friedman, R. Renner, and T. Vidick, *Simple and tight device-independent security proofs*, *SIAM J. Comput.* **48**, 181 (2019).
- [30] M. Tomamichel, *Quantum Information Processing with Finite Resources* (Springer International Publishing, New York, 2016).
- [31] R. L. Frank and E. H. Lieb, *Monotonicity of a relative Rényi entropy*, *J. Math. Phys. (N.Y.)* **54**, 122201 (2013).
- [32] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, *On quantum Rényi entropies: A new generalization and some properties*, *J. Math. Phys. (N.Y.)* **54**, 122203 (2013).
- [33] S. Beigi, *Sandwiched Rényi divergence satisfies data processing inequality*, *J. Math. Phys. (N.Y.)* **54**, 122202 (2013).
- [34] M. Mosonyi and T. Ogawa, *Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies*, *Commun. Math. Phys.* **334**, 1617 (2014).
- [35] In that model, the E_n register will usually also contain a copy of $\hat{C}_1^n$, but this does not affect any of the final bounds.
- [36] E. Y.-Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, and C. C.-W. Lim, *Improved DIQKD protocols with finite-size analysis*, *Quantum* **6**, 880 (2022).
- [37] E. Cervero-Martín and M. Tomamichel, *Device independent security of quantum key distribution from monogamy-of-entanglement games*, *Quantum* **9**, 1652 (2025).
- [38] This definition could likely be extended to $\alpha \in \{0, 1, \infty\}$ by taking the respective limits. However, our subsequent discussions suggest that, for instance, the $\alpha = \infty$ case would essentially correspond to H_∞ conditional entropies, which are simply zero in many circumstances (unlike $H_\infty^\uparrow$) and hence unlikely to be of much interest. Furthermore, in Theorem V.1, the $[1/(\hat{\alpha} - 1)]$ factor would be zero at $\hat{\alpha} = \infty$, which makes the result somewhat trivial; see the discussion in Sec. V B.
- [39] Earlier versions of this work referred to H_α^f as a QES entropy; we have chosen to update the terminology to bring it more in line with Ref. [17].
- [40] There is no danger of ambiguity in having used ρ to denote all states in this lemma since a read-and-prepare channel always simply extends a state without “disturbing” any registers.
- [41] In fact, this M term can be entirely avoided if we first use the “normalization property” in Lemma IV.7 below to shift all the f values to negative values, allowing us to choose $M = 0$. Alternatively, $M = 0$ could be achieved by modifying our construction to instead follow Ref. [1] and generate a pair of quantum registers $D\bar{D}$, and then use the fact that $H_\alpha(D|\bar{D})$ can be assigned negative values to obtain $H_\alpha(DQ\bar{C}|\bar{D}\hat{C}Q')_\rho = H_\alpha^f(Q\bar{C}|\hat{C}Q')_\rho$. However, in that case, it might not straightforwardly hold that $H_\alpha(D|\bar{D}) = H_\alpha^\uparrow(D|\bar{D})$.
- [42] F. Dupuis, *Chain rules for quantum Rényi entropies*, *J. Math. Phys. (N.Y.)* **56**, 022203 (2015).
- [43] It may appear strange to make the Q register trivial since, in some protocols, it corresponds to the raw “secret data,” but the idea is that in Ref. [18] and follow-up works, the QEF analysis is applied in such a way that the $\bar{C}$ register itself contains all the raw “secret data.” Our results can be viewed as slightly extending their approach by also allowing for an additional, possibly quantum Q (for the case where Q is classical, it can still be basically accommodated in their approach by incorporating it into the $\bar{C}$ register but choosing a QES/QEF that is independent of its value).
- [44] To avoid potential confusion, we highlight that, for each j , we have multiple different QESs, which are indexed by the values $\bar{c}_1^{j-1}\hat{c}_1^{j-1}$. We also highlight that each such QES is a function on the alphabet of $\bar{C}_j\hat{C}_j$ only *not* the “preceding” registers $\bar{C}_1^{j-1}\hat{C}_1^{j-1}$. Of course, by the equivalence between k -tuples and functions on a discrete set of size k , in principle, we could view the tuple of values $\{f_{|\bar{c}_1^{j-1}\hat{c}_1^{j-1}}(\bar{c}_j\hat{c}_j)\}_{\bar{c}_1^{j-1}\hat{c}_1^{j-1}}$ as being a function on the alphabet of $\bar{C}_1^j\hat{C}_1^j$, but for this theorem statement, it is more convenient to use the presented form. (In other contexts, it can be convenient to view it as such a function, but we defer that discussion to later work.)
- [45] M. Berta, O. Fawzi, and M. Tomamichel, *On variational expressions for quantum relative entropies*, *Lett. Math. Phys.* **107**, 2239 (2017).
- [46] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, *Device-independent randomness expansion against quantum side information*, *Nat. Phys.* **17**, 448 (2021).
- [47] While the resulting lower bound on $H_\alpha^{\hat{f}_{\text{full}}}(S_1^n|\bar{C}_1^n\hat{C}_1^n E_n)_\rho$ is not zero, this is easily addressed by either using Lemma IV.7 to “normalize” the lower bound to zero or, equivalently, just modifying the analysis to hash to a shorter key.
- [48] We write this condition in this form to highlight that Ω does not have to be an event defined entirely on the state ρ itself, which allows more flexibility in applications. This is

also why we use a separate symbol $\tilde{\Omega}$ to denote the set of values $\tilde{c}_1^n \hat{c}_1^n$ such that $\rho_{|\Omega}(\tilde{c}_1^n \hat{c}_1^n) > 0$.

- [49] Strictly speaking, the convex range is not fully defined by only the channels $\mathcal{E}_j$ since one also has to specify the various embeddings. However, all of our subsequent results hold for any choice of embeddings, so we will usually not specify this explicitly.
- [50] The potential exception here would be for protocols where one has *a priori* knowledge that some rounds would behave differently from others, for instance, in satellite QKD where the photon losses are likely to vary over the course of the protocol. In that case, there are potential benefits to be gained from the more general “adaptive” analysis described in the previous section, though, as mentioned, such an analysis would be more elaborate than the results we present in this section.
- [51] This assumption does not affect its applicability to DI security proofs (at least, assuming that the dimensions are finite but unbounded) because, in such security proofs, we can suppose that $\mathcal{M}$ acts on systems of finite but unknown dimension and say that the bounds we derive are independent of this dimension and hence valid for any such $\mathcal{M}$ [36].
- [52] A. Winick, N. Lütkenhaus, and P.J. Coles, *Reliable numerical key rates for quantum key distribution*, *Quantum* **2**, 77 (2018).
- [53] In fact, rather than $H_{\alpha'}$ specifically, for the purposes of this argument, we can discuss any Rényi entropy $\mathbb{H}$ satisfying $H_{\min} \leq \mathbb{H} \leq H$ because, for any classical-quantum state ρ_{CQ} , we have $\mathbb{H}(C|Q)_{\rho} = 0$ for some such $\mathbb{H}$ if and only if $\mathbb{H}(C|Q)_{\rho} = 0$ for all such $\mathbb{H}$ [since $\mathbb{H}(C|Q)_{\rho} = 0$ implies $H_{\min}(C|Q)_{\rho} = 0$, which implies the conditional states $\rho_{Q|c}$ are all perfectly distinguishable and hence $H(C|Q)_{\rho} = 0$ as well].
- [54] Technically, to complete the argument we must rule out the possibility of a sequence of feasible values *limiting* to zero. To do so, we can follow the steps described in the proof of Lemma V.4 to replace S_{Ω} with its closure by a continuity argument, in which case, for finite-dimensional $\tilde{Q}$, we obtain a continuous optimization over a compact set and hence the infimum is attained (and hence strictly positive). An alternative prospect is to introduce another convex optimization $\inf_{\mathbf{q} \in S_{\Omega}} \inf_{\omega \in S_{\tilde{Q}}} H_{\alpha'}(S\tilde{C}|\hat{C}E\tilde{E})_{\nu^{\omega}}$ subject to the constraint $\|\mathbf{q} - \nu_{\tilde{C}\hat{C}}^{\omega}\|_1 \leq \delta$, which matches the “simplistic” optimization in Eq. (83) when picking $\delta = 0$. It seems likely that one could prove the optimal value of this optimization is continuous with respect to $\delta \geq 0$ (for instance, by modifying the arguments in Ref. [55]); if so, then, by continuity, there exists some $\delta_{\star} > 0$ such that this optimization is lower bounded by, say, $h_{\star}/2$. Thus, we can conclude the desired property that every feasible $(\mathbf{q}, \omega)$ in our bound Eq. (82) is *bounded away from zero* since for every such point we either have $\|\mathbf{q} - \nu_{\tilde{C}\hat{C}}^{\omega}\|_1 \leq \delta_{\star}$ and thus $H_{\alpha'}(S\tilde{C}|\hat{C}E\tilde{E})_{\nu^{\omega}} \geq h_{\star}/2 > 0$ or $D(\mathbf{q}||\nu_{\tilde{C}\hat{C}}^{\omega}) \geq \delta_{\star}^2/(2 \ln 2) > 0$ by Pinsker’s inequality. This prospective approach has the advantage that, in the DI case, it seems plausible that we still have continuity with respect to δ even after later proof steps where we further minimize over the GEATT channels themselves (to accommodate all possible measurements and dimensions). However, we leave a rigorous proof of these continuity claims for future work since here we only aim to give a plausibility argument that $h_{\star}$ is “usually” nonzero.
- [55] R. J. Duffin, *Clark’s Theorem on linear programs holds for convex programs*, *Proc. Natl. Acad. Sci. U.S.A.* **75**, 1624 (1978).
- [56] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Random numbers certified by Bell’s theorem*, *Nature (London)* **464**, 1021 (2010).
- [57] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices*, *Nat. Commun.* **2**, 238 (2011).
- [58] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, *Towards a realization of device-independent quantum key distribution*, *Quantum Sci. Technol.* **4**, 035011 (2019).
- [59] The latter bound holds whenever $\tilde{C}$ has the property that it can be “projectively reconstructed” from $S\tilde{C}E$ in the sense of Lemma B.7 of Ref. [1], by simply observing that, in that case, the lemma gives us $H_{\alpha'}(S\tilde{C}|\hat{C}E\tilde{E}) = H_{\alpha'}(S|\hat{C}E\tilde{E})$ and $H(S\tilde{C}|\hat{C}E\tilde{E}) = H(S|\hat{C}E\tilde{E})$, so we can apply the continuity bound of Lemma B.9 of Ref. [1] without including $\tilde{C}$.
- [60] Similar to Ref. [2], this choice is just to demonstrate a possible scaling; for the best finite-size bounds, one should optimize the Rényi parameter choices numerically for each n .
- [61] One can tune α' and α'' in other ways; e.g., if we fix one as a constant and set the other to $1 + \mu$, then we can obtain $\hat{\alpha}, \alpha = 1 + \mu + O(\mu^2)$, but this approach sacrifices the option to bring the constant one closer to 1.
- [62] We highlight that this loss comes inherently from the Lemma V.1 bound rather than the subsequent bound in Eq. (92) since the latter is an equality in such scenarios.
- [63] T. A. Hahn, E. Y.-Z. Tan, and P. Brown, *Bounds on Petz-Rényi divergences and their applications for device-independent cryptography*, *arXiv:2408.12313v1*.
- [64] Alternatively, one can directly show that this expression is jointly convex in $(\mathbf{t}, \tilde{\nu}^{\omega}(\tilde{c}\hat{c}))$ by using the fact that the function $x \log(x/y)$ is jointly convex on $(x, y) \in \mathbb{R}_{\geq 0}^2$. However, this case ignores any “coupling” with the prefactors of the entropy terms in, e.g., Lemma V.1.
- [65] This claim is, in fact, somewhat delicate. First, note that for n IID instances of a Bernoulli random variable with expectation p_{exp} , if we write the observed success frequency as Q_{obs} , then the probability that $|Q_{\text{obs}} - p_{\text{exp}}|$ exceeds some value δ can be shown to be at most $2e^{-\frac{\delta^2 n}{3p_{\text{exp}}}}$ by a Chernoff bound argument. Thus (focusing only on the $\perp \perp$ term and ignoring contributions from other test-round outcomes), we can choose $\delta_{\gamma} = \delta'_{\gamma} = \sqrt{(3\gamma/n) \log(2/\epsilon_{\text{com}})}$ while still ensuring an accept probability of at least $1 - O(\epsilon_{\text{com}})$ on honest IID behavior (by applying the Chernoff bound argument with $p_{\text{exp}} = \gamma$, viewing a single-round “success” as the event that $\perp \perp$ did *not* occur). In that case, if we pick the scaling of γ with n to be any function that goes to zero more slowly than $1/n$

(as is indeed the case in the subsequent analysis), we see that δ_γ and δ'_γ would indeed become arbitrarily small compared to γ . However, if we pick $\gamma \propto 1/n$ *exactly*, this argument does not work, just as in Ref. [2]. We leave a more detailed analysis [perhaps preserving the $D(\mathbf{r}||\mathbf{s})$ term to avoid invoking an explicit lower bound on γ_q] for future work.

- [66] The KL divergence term is already convex, so it suffices to show convexity of this entropy term alone. Still, it is true that, in principle, there may be situations where the *sum* of the KL divergence term and entropy term is convex even if the latter is not convex by itself—considering this possibility might help in tackling the issue we shall shortly discuss regarding the full linear combination $\sum_{\tilde{c}\hat{c}} q(\tilde{c}\hat{c})H(S|E\tilde{E})_{\nu_{|\tilde{c}\hat{c}}}$. However, we leave this more elaborate possibility for future work, if it is relevant.
- [67] If $\mathcal{Z}$ and $\mathcal{G}$ are not trace preserving, care is needed to ensure consistency with the definition in Eq. (16) we chose here for Umegaki divergence.
- [68] Note that in the $G_{\alpha,\rho}^*$ formula, the first case can still take a value $+\infty$ for some values of λ due to the $D(\lambda||\rho_{\tilde{c}\hat{c}})$ term. Specifically, this happens whenever $\text{supp}(\lambda) \not\subseteq \text{supp}(\rho_{\tilde{c}\hat{c}})$.
- [69] In this lemma, Lagrange dual problems are defined in the sense described in, e.g., Ref. [26]. Since the constraints are equality constraints, there is an arbitrary sign convention to pick when defining the dual variables; see the last line of Eq. (112) for the sign convention we used.
- [70] In this paragraph, we informally refer to “the” best choice of f , though this is technically a misnomer because it is necessarily nonunique—given any QES f in Corollary V.1, inspecting the bound shows that $f + \kappa$ for any $\kappa \in \mathbb{R}$ yields an identical bound since the κ dependence “cancels off.” (Loosely speaking, this nonuniqueness seems to arise from the implicit normalization constraint in the domains S_Ω and $\mathbb{P}_{\tilde{c}\hat{c}}$, though we leave further analysis for future work.) Furthermore, it might potentially be possible that the optimal f is not attained, as we discuss later. However, this nonuniqueness or nonattainability does not have any effects on our actual proofs of Lemma V.4 or Theorem V.1; we are merely highlighting a technicality in our informal statements here.
- [71] For our proofs, let us say continuity and closedness are defined with respect to the topology induced by, say, the 1-norm.
- [72] This is because we have argued above that the expressions in Eqs. (78) and (79) are equal for *any* choice of purifying function, which means that the latter is independent of the choice of purifying function. Thus, we can focus on any specific choice without loss of generality; in particular, under the finite-dimensionality assumption, we can pick the one shown in Eq. (29), which is indeed continuous (this can be seen by, e.g., computing the fidelity between purifications of δ -close states under that formula and then applying Fuchs–van de Graaf to convert to 1-norm distance).
- [73] An alternative approach, similar to the convexity argument above: After noting that ν^ω is continuous in ω , observe that $G_{\tilde{\alpha},\nu^\omega}^*(\mathbf{f}) = -H_{\tilde{\alpha}}^f(S\tilde{C}|\hat{C}E\tilde{E})_{\nu^\omega} = M - H_{\tilde{\alpha}}(DS\tilde{C}|\hat{C}E\tilde{E})_{\nu^\omega}$ for a suitable extending channel as defined in Lemma IV.1, so $G_{\tilde{\alpha},\nu^\omega}^*(\mathbf{f})$ is continuous in ω (by the continuity of conditional Rényi entropy with respect to the state). This implies that $G_{\tilde{\alpha},\nu^\omega}^*(\lambda)$ is lower semicontinuous with respect to (λ, ω) since it is a supremum over a family of functions $\lambda \cdot \mathbf{f} - G_{\tilde{\alpha},\nu^\omega}^*(\mathbf{f})$ that are each lower semicontinuous with respect to (λ, ω) . Thus, we have lower semicontinuity of $G_{\tilde{\alpha},\nu^\omega}^*(\lambda) + (\mathbf{q} - \lambda) \cdot \mathbf{f}$ with respect to $(\mathbf{q}, \lambda, \omega)$, which suffices to apply the version of our subsequent argument based on Sion’s minimax theorem (which only requires semicontinuity rather than continuity).
- [74] S. Khatri and M. M. Wilde, *Principles of quantum communication theory: A modern approach*, arXiv:2011.04672.
- [75] The registers $\tilde{A}$ in these statements are intended to include shield systems as well, if required by the security proof.
- [76] While we also applied Lemma B.5 of Ref. [1] to account for conditioning on Ω , note that when applying the Rényi privacy amplification theorem of Ref. [10], the $[\alpha/(\alpha - 1)] \log[1/(\Pr[\Omega])]$ term essentially does not affect the final key rates—see, e.g., Refs. [10,11] or Secs. VII B and VII C of this work.
- [77] M. Tomamichel, M. Berta, and M. Hayashi, *Relating different quantum generalizations of the conditional Rényi entropy*, J. Math. Phys. (N.Y.) **55**, 082206 (2014).
- [78] Since the test rounds are only measured in the X basis, in this formula, we could instead view Q_{thresh} as only being the “phase error rate” rather than the QBER with respect to multiple bases. However, since the error-correction term λ_{EC} instead depends on error rates in generation rounds (i.e., the Z -basis error rate), for simplicity, in this analysis we view Q_{thresh} as a single QBER parameter that characterizes error rates in any basis; thus, we can use it in the formula in Eq. (133) for λ_{EC} .
- [79] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, *The uncertainty principle in the presence of quantum memory*, Nat. Phys. **6**, 659 (2010).
- [80] In other words, after they have XOR’d their outcomes with the symmetrization bit F . Note that, strictly speaking, in order to apply EURs to the values S , X , and $\tilde{X}$ (which are produced after symmetrization, i.e., not the raw outcomes of X or Z measurements), we are implicitly applying a standard argument [81] that the same overall state (including all side information) could instead be produced by just taking the raw outcomes of measurements on some other initial state, essentially by “commuting” the symmetrization with the measurements by reexpressing it as a rotation on the premeasurement qubits. An alternative option would be to omit the symmetrization step and instead use, e.g., Fano’s inequality to write $H(X|\tilde{X})_{\nu_{|\hat{C} \neq \perp}} \leq h_{\text{bin}}(\Pr[X \neq \tilde{X}]|\hat{C} \neq \perp)$ for the purposes of the bound in Eq. (135), but this would require more steps to extend to the Rényi EUR bound in Eq. (142).
- [81] R. Renner, N. Gisin, and B. Kraus, *Information-theoretic security proof for quantum-key-distribution protocols*, Phys. Rev. A **72**, 012332 (2005).
- [82] Note that this event is a stricter condition than just the acceptance test accepting (which would be the event $\text{freq}_{\mathcal{C}_1^n} \in S_\Omega$), so it remains the case that every distribution $\hat{\mathcal{C}}_1^n$ with nonzero probability in the conditional state $\rho_{|\Omega}$

- satisfies $\text{freq}_{\mathcal{C}_1^n} \in S_\Omega$; i.e., the first condition on S_Ω in Theorem V.1 indeed holds. Also note that we are implicitly exploiting the fact that, in Theorem V.1, Ω does not have to be an event defined entirely on the $\hat{\mathcal{C}}_1^n$ registers, as discussed in Corollary IV.1.
- [83] The parameter ε_{EV} here is denoted as ε_{KV} in Ref. [21]; we have used different notation simply because we refer to the relevant step as “error verification” instead of “key validation.”
- [84] C. Portmann and R. Renner, *Security in quantum cryptography*, *Rev. Mod. Phys.* **94**, 025008 (2022).
- [85] To obtain this result, we have basically added the correctness and secrecy parameters from Ref. [21], except that the secrecy parameter in that work is rescaled by a factor of 2 as compared to Refs. [6,84], so we have first adjusted it accordingly. We have also removed the dependence of the secrecy parameter in that work on ε_{EV} because, for our protocol, we perform the acceptance test directly on the $\hat{\mathcal{C}}_1^n$ registers rather than guessing; see Ref. [11].
- [86] S. Arimoto, *Information measures and capacity of order alpha for discrete memoryless channels*, *Topics Inf. Theor.* **17**, 41 (1977), <https://cir.nii.ac.jp/crid/1570854175661265024>.
- [87] It would have been cleaner if we could directly “accumulate” $H_\infty^\uparrow$; however, it can be seen that our bounds for the EAT or GEAT scenarios involve H_α rather than $H_\alpha^\uparrow$ in the single-round terms, and therefore, we cannot directly make use of a bound on single-round $H_\infty^\uparrow$ without first converting it to H_2 . (For the Ref. [17] scenario though, the bounds we presented in Sec. VI B are indeed based on single-round $H_\alpha^\uparrow$, which would indeed allow us to directly accumulate min-entropy.) In any case, for the CHSH game, in particular, Ref. [58] showed that the bound in Eq. (148) is, in fact, tight for both H_2 and $H_\infty^\uparrow$, so there is no loss of tightness in considering the former instead for this particular protocol.
- [88] Again, we could instead convert to $H_{\min}^{\varepsilon_s}$ and apply the corresponding privacy amplification theorem (under the current state of results in privacy amplification, this may be necessary if the protocol uses Trevisan’s extractor instead of 2-universal hashing). However, in that case, we find no improvement in $n_{\min}$ over Eq. (150), though we can at least obtain about $n_{\min} = 3 \times 10^{10}$, which is still better than Ref. [46]. The issue basically seems to be that, for security proofs based on our $H_{\min}^{\varepsilon_s}$ bound rather than our $H_\alpha^\uparrow$ bound, one has to pick a “threshold” value ε_a and split the analysis into cases where p_Ω is above or below ε_a ; this introduces additional finite-size corrections, and the resulting ℓ_{key} formula then fails to reduce to Eq. (150) in the $\alpha \rightarrow 2$ limit.
- [89] In fact, another potential question is whether we would actually obtain better $n_{\min}$ values via this von Neumann entropy approach; we leave this question for future work. One point that may be worth highlighting is that, similar to the advantage of Eq. (143) over Eq. (136) in the previous section, working with the collision-entropy bound in Eq. (148) ensures that the optimization for the “first-order term” always returns a strictly positive value, unlike the relaxation to von Neumann entropy via the continuity bound in Eq. (86), which may yield a negative value if α' is not sufficiently close to 1. Hence, it seems likely that the collision-entropy approach will indeed be better for small n , where the optimal Rényi parameters are further from 1.
- [90] D. Tupkary, Ernest Y.-Z. Tan, and N. Lütkenhaus, *Security proof for variable-length quantum key distribution*, *Phys. Rev. Res.* **6**, 023002 (2024).
- [91] M. Christandl, R. König, and R. Renner, *Postselection technique for quantum channels with applications to quantum cryptography*, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [92] S. Nahar, D. Tupkary, Y. Zhao, N. Lütkenhaus, and Ernest Y.-Z. Tan, *Postselection technique for optical quantum key distribution with improved de Finetti reductions*, *PRX Quantum* **5**, 040315 (2024).
- [93] For readers familiar with Ref. [90], we highlight that, in principle, Theorem V.1 in this work could be used to bound the Rényi entropy conditioned on any particular frequency distribution observed on the $\hat{\mathcal{C}}_1^n \hat{\mathcal{C}}_1^n$ registers, which roughly satisfies the requirements for applying the analysis in Ref. [90], *except* that the bound has an explicit dependence on p_Ω . Therefore, a direct calculation along the same lines as in that work would result in the final security parameter being multiplied by the number of possible frequency distributions. This result is somewhat undesirable; however, in principle, it is described by a combinatorial coefficient that “only” increases polynomially in n . This outcome may be tolerable in practice, as suggested by proofs based on the postselection technique that introduce such polynomial factors [91,92], albeit based on the dimensions of the quantum systems rather than the classical outcomes (the approach suggested here would hence be superior to the postselection technique for DI protocols or other contexts where the dimension dependence is improved via this approach).
- [94] We could obtain a similar result by instead using the chain rule from Ref. [42] here to extract a $H_{1/2}^\uparrow(Z_1^n | T_1^n)_{\rho_{\Omega}}$ term, but this would have a (fairly minor) disadvantage of causing a small “higher-order” change in Rényi parameter, comparable to Eq. (64). Note that even with this, our approach would still differ slightly from Ref. [5] due to how we bound the $H_{1/2}^\uparrow(Z_1^n | T_1^n)_{\rho_{\Omega}}$ term in the subsequent steps.
- [95] Furthermore, in our bound the subtracted term simply has the form $\gamma^{\max} n \log |\mathcal{Z}|$, where $\gamma^{\max}$ only needs to be chosen to be sufficiently large for the *honest* IID behavior to accept with high probability. In comparison, the subtracted terms in Refs. [5,29,36,58] were roughly of the form $\gamma n \log |\mathcal{Z}| + O(\sqrt{n})$, where the $O(\sqrt{n})$ term accommodated potential non-IID behavior. It seems likely that the former value is smaller, though we do not aim to prove this rigorously. (We briefly highlight, however, that Ref. [37] introduced an approach in which the subtracted term was also roughly of the form $\gamma^{\max} n \log |\mathcal{Z}|$, though there was still a change of smoothing parameter.)
- [96] While $\mathcal{N}_j$ performs a pinching channel on $\hat{\mathcal{C}}_1^{j-1} \hat{\mathcal{C}}_1^{j-1}$ in contrast to $\mathcal{M}_j$, which acts as an identity on those registers, it does not make a difference for states produced by applying those channels in sequence because $\mathcal{N}_{j-1} \circ \dots \circ \mathcal{N}_1[\omega^0]$ is always already classical on $\hat{\mathcal{C}}_1^{j-1} \hat{\mathcal{C}}_1^{j-1}$. Similarly, the second

- and third steps performed by $\mathcal{N}_j$ do not disturb the classical registers they act on.
- [97] In this step, let us take $\tilde{E}$ to be of large enough dimension to be a purifying register for the input registers in the $\mathcal{N}_j$ scenario as well, which can be achieved without loss of generality by expanding its dimension as necessary.
- [98] For strict technical accuracy in the following steps, these conditional states should be interpreted to still include the registers $\tilde{C}_1^{j-1}\hat{C}_1^{j-1}$, though with those registers simply taking the fixed value $\tilde{c}_1^{j-1}\hat{c}_1^{j-1}$.
- [99] While the QES $f_{|\tilde{c}_1^{j-1}\hat{c}_1^{j-1}|}$ depends on $\tilde{c}_1^{j-1}\hat{c}_1^{j-1}$, its value is fixed by the initial choices in the theorem, not by the state.
- [100] Pedantically, to ensure there are no issues involving the dependence of the summation domain in Eq. (B28) on ω , we should first note that we can extend the summation domain to the full alphabet $\tilde{\mathcal{C}} \times \hat{\mathcal{C}}$ without changing the value of $G_{\alpha', \alpha'', \nu^\omega}(\mathbf{f})$ (in this case, there are no divergence terms in the sum, so we do not encounter any technical issues).
- [101] An alternative approach for the purposes of our analysis would be to simply restrict the alphabet of the registers $\tilde{\mathcal{C}}\hat{\mathcal{C}}$ to $\mathcal{C}_{\mathcal{M}}$ rather than $\tilde{\mathcal{C}} \times \hat{\mathcal{C}}$ since the values outside $\mathcal{C}_{\mathcal{M}}$ will never occur and thus have no “physical relevance.” However, this approach would result in the slightly unpleasant side effect that the resulting alphabet is not guaranteed to have a Cartesian-product form.
- [102] An alternative option is as follows: Since the mapping $\omega \rightarrow \nu_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}^\omega$ is a quantum-to-classical channel, one can show that it must be of the form $\omega \rightarrow \sum_{\tilde{c}\hat{c}} \text{Tr}_{\Gamma_{\tilde{c}\hat{c}}\omega}[\tilde{c}\hat{c}]\langle\tilde{c}\hat{c}|\rangle$ for some POVM elements $\Gamma_{\tilde{c}\hat{c}}$; furthermore, we must have $\Gamma_{\tilde{c}\hat{c}} \neq 0$ for all $\tilde{c}\hat{c} \notin \mathcal{C}_{\mathcal{M}}$. Thus, we can show that any full-support $\omega_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}$ yields a distribution $\nu_{\tilde{\mathcal{C}}\hat{\mathcal{C}}}^\omega$ with full support on $\mathcal{C}_{\mathcal{M}}$ (at least assuming countable dimensions; the argument should generalize further in some fashion but we do not consider this here), giving the desired result.
- [103] Here, we did not simply try to apply Slater’s condition to the original constrained optimization in Eq. (109) because it would require the existence of some ω in the relative interior of the effective domain of $G_{\alpha, \nu^\omega}^*(\lambda)$ (i.e., the domain on which it takes finite values), which is more subtle in the infinite-dimensional case. However, for the finite-dimensional case, in our above proof of the finiteness of $J_{\hat{\alpha}}$, we argued that $G_{\alpha, \nu^\omega}^*(\lambda)$ is finite over all full-support ω , and hence any full-support ω yields such an interior point.
- [104] However, this proof method still does not immediately certify dual attainment, despite using Slater’s condition, because, when transforming the optimizations, we only focused on preserving the optimal value rather than other properties such as dual attainment. We leave a more extensive analysis of such aspects for future work, if it should become important.
- [105] For the $\tilde{c}\hat{c} \notin \mathcal{C}_{\mathcal{M}}$ terms, there is no need to include any “ δ tolerances” here because zero-probability events (on a finite alphabet) would never occur. There is a technical issue that the supporting alphabets induced by $\mathcal{M}_j$ versus $\mathcal{M}$ might be different, in principle, but we do not expect this situation to arise in practice.
- [106] The data-processing inequality for Petz entropies is usually only stated for $\alpha \in (0, 2]$; here, we extend it to $\alpha = 0$ by noting that, by definition, the value of $\tilde{D}_0$ is given by the $\alpha \rightarrow 0$ limit, and thus we indeed have $\tilde{D}_0(\rho\|\sigma) - \tilde{D}_0(\mathcal{E}[\rho]\|\mathcal{E}[\sigma]) = \lim_{\alpha \rightarrow 0} (\tilde{D}_\alpha(\rho\|\sigma) - \tilde{D}_\alpha(\mathcal{E}[\rho]\|\mathcal{E}[\sigma])) \geq 0$.
- [107] Qualitatively, this condition states that V_j does not signal from E_{j-1} to $R_j\tilde{C}_j\hat{C}_jF_j$. Also note that the choice of Stinespring dilation can be arbitrary here due to isometric equivalence of purifications.
- [108] Formally, this means we suppose that E_j is isomorphic to $\tilde{C}_jT_jE_{j-1}$, so we can define an “identity channel” $\text{id}_{\tilde{C}_jT_jE_{j-1} \rightarrow E_j}$ and say that $\mathcal{M}_j$ has the form $\text{id}_{\tilde{C}_jT_jE_{j-1} \rightarrow E_j} \circ \tilde{\mathcal{M}}_j$ for some $\tilde{\mathcal{M}}_j: R_{j-1} \rightarrow S_j\tilde{C}_j\hat{C}_jT_jR_j$.
- [109] For instance, it seems potentially useful to instead consider $H_{\tilde{\beta}}(D_jS_j\tilde{C}_j|\tilde{C}_1^{j-1}\hat{C}_1^{j-1}R_jF_1^jG_1^j\tilde{E})_{\nu}$ in Eq. (E12) and then try to lower bound it with $\min_{\tilde{c}_1^{j-1}\hat{c}_1^{j-1}} H_{\tilde{\beta}}(D_jS_j\tilde{C}_j|R_jF_1^jG_1^j\tilde{E})_{\nu_{|\tilde{c}_1^{j-1}\hat{c}_1^{j-1}|}}$, but the issue is that $\tilde{C}_1^{j-1}\hat{C}_1^{j-1}$ might not be classical in the state $\nu_{D_jS_j\tilde{C}_j\tilde{C}_1^{j-1}\hat{C}_1^{j-1}R_jF_1^jG_1^j\tilde{E}}$, and hence $\nu_{|\tilde{c}_1^{j-1}\hat{c}_1^{j-1}|}$ is less easily defined.
- [110] A. Marwah and F. Dupuis, *Smooth min-entropy lower bounds for approximation chains*, *Commun. Math. Phys.* **405**, 211 (2024).
- [111] Strictly speaking, that result is only stated for $\beta \in (0, \infty)$, but we can first suppose that $\alpha > 1/2$ so that $\beta < \infty$; then, to obtain our desired result for $\alpha = 1/2$, we can take the $\alpha \rightarrow 1/2$ limit at the end, exploiting continuity of the sandwiched Rényi divergences with respect to α (Corollary 4.2 of Ref. [30] together with the fact that convex functions are continuous on the interior of their domain).
- [112] N. Datta, *Min- and max-relative entropies and a new entanglement monotone*, *IEEE Trans. Inf. Theory* **55**, 2816 (2009).
- [113] Technically, for $\beta > 1$ (i.e., $\alpha < 1$), we have $\text{supp}(\rho_{A_1C}) \subseteq \text{supp}(\mathbb{I}_{A_1} \otimes \sigma_C)$ since, by definition, the state σ satisfies $D_\beta(\rho_{A_1C}\|\mathbb{I}_{A_1} \otimes \sigma_C) \leq D_\beta(\rho_{A_1C}\|\mathbb{I}_{A_1} \otimes \rho_C) < +\infty$. From the definition of ν_{A_1C} , it can then be seen that, in fact, $\text{supp}(\rho_{A_1C})$ and $\text{supp}(\nu_{A_1C})$ are equal in this case; thus, the implication indeed holds in both directions, and we obtain the equality $H_\infty(A_2|A_1C)_\nu = H_\infty(A_2|A_1C)_\rho$. However, this argument seems less straightforward to generalize to the $\beta < 1$ regime, where $D_\beta(\rho_{A_1C}\|\mathbb{I}_{A_1} \otimes \sigma_C) < +\infty$ does not imply $\text{supp}(\rho_{A_1C}) \subseteq \text{supp}(\mathbb{I}_{A_1} \otimes \sigma_C)$; in fact, in that regime, we generally have $\text{supp}(\sigma_C) \subseteq \text{supp}(\rho_C)$ instead (Sec. III B in Ref. [32]).