Finite-Key Analysis of Quantum Key Distribution with Characterized Devices Using Entropy Accumulation

Ian George[*1,2], Jie Lin[*1], Thomas van Himbeeck[*1,3], Kun Fang[1,4], and Norbert Lütkenhaus[1]

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

[2]Department of Electrical & Computer Engineering, University of Illinois, Urbana, Illinois 61801, USA

[3]Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada

[4]School of Data Science, The Chinese University of Hong Kong, Shenzhen, Guangdong, 518172, China

The Entropy Accumulation Theorem (EAT) was introduced to significantly improve the finite-size rates for device-independent quantum information processing tasks such as device-independent quantum key distribution (QKD). A natural question would be whether it also improves the rates for device-dependent QKD. In this work, we provide an affirmative answer to this question. We present new tools for applying the EAT in the device-dependent setting. We present sufficient conditions for the Markov chain conditions to hold as well as general algorithms for constructing the needed min-tradeoff function. Utilizing Dupuis' recent privacy amplification without smoothing result, we improve the key rate by optimizing the sandwiched Rényi entropy directly rather than considering the traditional smooth min-entropy. We exemplify these new tools by considering several examples including the BB84 protocol with the qubit-based version and with a realistic parametric downconversion source, the six-state four-state protocol and a high-dimensional analog of the BB84 protocol.

Contents

---

[*]These authors contributed equally to this work

1 Introduction

Quantum key distribution (QKD) protocols [1, 2] enable two legitimate parties (Alice and Bob) to establish shared secret keys in the presence of any eavesdropper (Eve) who has control over the channel connecting the two parties and is only limited by the laws of quantum mechanics. That is, QKD protocols establish an information-theoretically secure shared secret key. The generated secret keys can be used in many cryptographic applications that our modern cybersecurity relies on, such as encryption and authentication. The field of QKD has grown rapidly in the last couple decades. Novel protocols have been proposed and analyzed (see [3, 4, 5] for reviews). Many QKD experiments (e.g. [6, 7]) have been demonstrated to reach increasingly longer distances and/or to achieve higher key bits per second. The maturity of the field can be witnessed by development of commercial prototypes in several companies, successful launch of a QKD satellite in China [8], many ongoing efforts to launch QKD satellites from all over the world [9], and developments of chip-based QKD systems [10, 11, 12].

While currently the field of implementation security (as opposed to protocol security), requiring certification procedures and security proofs with more refined models, captures an increasing amount of attention, there are still challenges to be addressed on the level of protocol security itself. One major technical difficulty is guaranteeing security of the protocol when using finite resources. The security of a novel protocol is often first proved in the asymptotic key limit where Alice and Bob exchange infinitely many signals, since in that regime typically reduction to the identically and independently distributed (i.i.d.) assumption about the individual exchanged signals can be made and statistical fluctuations can be neglected. However, any realistic system can only exchange a finite number of signals. For example, the time interval of low orbiting satellites having line of sight to ground stations is limited to minutes, thus naturally limiting the total number of signals that can be exchanged. The study of security with finite resources is known as finite key analysis. In recent years, finite key analysis against general attacks has been performed for several QKD protocols. One aims to provide security proofs that allow one to generate the most key using the fewest signals and converge to the fundamental asymptotic limit quickly.

Over the past decade, several techniques have been proposed to bridge the gap between asymptotic security and finite key analysis against general attacks. The Quantum de Finetti theorem [13] was first used to achieve this task. While it makes no restrictions on the QKD protocol implemented,[1] the key rate becomes very pessimistic at practical signal block size. The postselection technique [15] was later presented to improve the key rate if the implemented

---

[1]The Quantum de Finetti theorem requires permutation invariance, which in principle entails applying a coordinated random permutation on the state by Alice and Bob. However, it was shown in [14] that the min-entropy after symmetrization lower bounds the original, so the *implemented* protocol does not need the symmetry enforced.

protocol is permutation invariant with respect to any input. Although it gives better performance, the key rate is known to in general remain pessimistic as it scales exponentially in the dimension of Alice and Bob's signals. More recently, the entropy accumulation theorem [16, 17] was developed to offer tighter finite key analysis. It has been successfully applied to prove the security of device-independent (DI) QKD protocols [18, 19].

From the perspective of implementation security, DIQKD is favorable since it requires minimal assumptions on Alice and Bob's devices and thus is immune to most side-channel attacks. Thanks to the entropy accumulation theorem [16] and its application to DIQKD [18], the experimental requirements to implement DIQKD have become within reach of state-of-the-art technologies. Very recently, proof-of-principle experimental demonstrations of DIQKD with positive key rates are reported for extremely short distances [20, 21, 22]. Even if the transmission distance is extended to practical regimes in the near future, a DIQKD system is expected to be more costly since the experimental requirements are still demanding. Beyond the experimental requirements, unlike device-dependent QKD, DIQKD is currently not known to be universally composably secure [23, 19]. This means currently this property must either be sacrificed or a new set of devices must be used each time one establishes a key. As such, while DIQKD has advantages for implementation security and can be implemented, at least over very short distances, device-dependent QKD (i.e. QKD with characterized devices) remains a practical option with different theoretical security guarantees at the moment.[2]

Beyond these limitations, as less assumptions are put on trusted parties' devices, DIQKD key rates are unavoidably lower than a standard device-dependent QKD protocol. On the other hand, with the best practice to countermeasure known side-channel attacks, suitable risk management and use cases, and efforts from standardization, device-dependent QKD remains a vital player for a wide adoption of QKD in the future. Therefore, it is still of great interest to provide as tight as possible key rates for device-dependent QKD. Our goal here is to apply the entropy accumulation theorem to provide better finite key rates of device-dependent QKD.

While concurrent work used the generalised entropy accumulation theorem [24] to establish the security of device-dependent QKD protocols, with a focus on prepare-and-measure protocols when only one signal is in the physical channel at a time [25], the original entropy accumulation theorem has not been applied to determine the key rate for any device-dependent QKD protocol.[3] In this work we focus on applying the original EAT to the analysis to the most general class of entanglement-based protocols we can.[4] There are two major obstacles to overcome in applying the original EAT to device-dependent QKD. The first is to guarantee the Markov condition is satisfied by the protocol. The second challenge is to have a general method to construct the required min-tradeoff function. In this work we address both challenges.

The Markov chain condition in effect guarantees the protocol is well-behaved in what side-information is leaked to Eve during the protocol. This is an important aspect as device-dependent protocols often make use of announcing more information about each signal than DI protocols. In this work, we provide sufficient conditions for satisfying the Markov conditions of the EAT. Specifically, we prove that when Alice and Bob's announcements are determined by POVMs with a simple block-diagonal structure, then the protocol satisfies the Markov chain conditions (see Section 4.2). This block-diagonal structure is satisfied for many practical

---

[2]We note that measurement-device-independent (MDI) QKD also falls in the category of device-dependent QKD since one still makes assumptions on both Alice's and Bob's devices.

[3]In [16] the authors presented how the asymptotic rate was recovered for BB84, but did not present finite-size key lengths.

[4]For entanglement-based protocols, there is no real advantage to using the generalised EAT and so this is largely without loss of generality.

discrete-variable QKD protocols. Moreover, we note that many practical non-sequential protocols will satisfy the Markov chain conditions necessary, but as they aren't sequential, don't satisfy the conditions of [25].

The challenge of developing a general method for constructing a min-tradeoff function has been addressed for the device-independent scenario in a recent work [26]. In concurrent work [25], the construction of a min-tradeoff function has been reduced to asymptotic key rate solvers in the device-dependent setting under the assumption only a single signal is ever in the physical channel at a time. This is analogous to the first algorithm of our numerical method for constructing tight min-tradeoff functions for device-dependent QKD protocols although we only recover the Markov chain conditoins be satisfied. The basic idea of this first algorithm is similar to our existing numerical method for asymptotic key rates [27, 28]. The second algorithm improves on the first one by considering the second-order term in the original EAT. It is based on Fenchel duality. However, unlike the formulation of the objective function in Refs. [27, 28], we present here a different formulation of the objective function for the optimization which has advantages in terms of dimension needed for the numerical optimization as well as a simpler representation of procedures to handle classical postprocessing.

Using the guarantee of our numerical method constructing a min-tradeoff function, we present a general key length bound. It is largely similar to that of Ref. [18], but, building on the recent result that privacy amplification may be characterized using sandwiched Rényi entropies rather than the smooth min-entropy [29], we are able to show we can improve the key rate by optimizing over sandwiched Rényi entropies rather than using the smooth min-entropy bounds. To the best of our knowledge, the only work to use Rényi entropies in establishing the security of QKD is [30]. However, we note that [30] does so by considering the smoothed 2-Rényi entropy. This differs from the ability to analyze the key rate of Rényi entropies directly by establishing a security proof that makes no use of smoothed entropic quantities as is done in this work.[5]

Taking all of these tools together, we apply our method to several examples. The first example is a simple qubit-based BB84 protocol and the second example is the entanglement-based six-state four-state protocol [32]. We use these two examples to demonstrate behaviors of our algorithms. The third one is a high-dimensional analog of the BB84 protocols. We compare these results with the key rates obtained by the postselection technique [15] to show that the EAT can outperform the postselection technique for high-dimensional signals. In the last example, we demonstrate that our method can also work for optical implementations of QKD and in particular, we study the entanglement-based BB84 protocol with a spontaneous parametric downconversion source in a lossy and noisy channel.

Our work here provides a first step along the direction of applying EAT to general device-dependent QKD protocols. Currently, we limit ourselves to entanglement-based protocols in exchange for the generality of protocol which we can consider. To handle prepare-and-measure protocols, one needs to be able to incorporate the source-replacement scheme [33], but it remains unclear how to do this while satisfying the Markov chain conditions of the original EAT. In [25], source-replacement is used by circumventing the Markov chain conditions by using the generalised EAT and assuming truly sequential implementation of the rounds in the protocol. As noted previously, the demand of a truly sequential implementation is not practical in general. It remains a technical challenge how to relax this condition and prove security for prepare and measure protocols.

The rest of the paper is organized as follows. In Section 2.1, we summarize our notational

---

[5]We remark that the smoothed 2-Rényi entropy was also considered for analyzing the large deviation regime of privacy amplification by Hayashi [31].

conventions and in Section 2.2, we review the security definition of QKD. In Section 3, we review the entropy accumulation theorem and adapt the theorem to the device-dependent setting. We do this first in the case where side information is all seeded randomness, as was the case in previous works. We then provide sufficient conditions for satisfying the Markov chain conditions necessary to apply the EAT without relying on all side-information being randomly seeded. This is important as many device-dependent QKD protocols make announcements which depend on the outcome of the measurement. In Section 4, we describe the generic protocol to which our method is applicable, protocols where all quantum signals are exchanged prior to any classical communication and all communication acts on a single 'round' of quantum communication. We also provide the assumptions on public announcements. In Section 5, we then apply the EAT to this family of protocols and obtain a key length formula. In Section 6, we discuss how to construct min-tradeoff functions numerically and present two numerical algorithms for obtaining a nearly tight min-tradeoff function. In Section 7, we apply our method to several examples. We then conclude in Section 8. We leave technical details to appendixes.

2 Preliminaries

We discuss the notational convention and some useful definitions in Section 2.1. We then review the security definition of QKD in Section 2.2.

2.1 Notation

We briefly summarize the notation which we use throughout this work.

General notations	Descriptions
$A, B, C, \cdots$	Quantum systems and their associated Hilbert spaces
$\|A\|, \|B\|, \|C\|, \cdots$	Dimension of the Hilbert spaces
A_1^n	Shorthand for $A_1 A_2 \cdots A_n$
$[n]$	The set of natural numbers from 1 to n
$\mathcal{I}$	Identity map
f	A min-tradeoff function
$\boldsymbol{f}$	A vector that is used to construct the min-tradeoff function f
$\mathbf{1}$	A vector of all ones

EAT statement	Descriptions
P_i	Public information in the EAT statement
S_i	Secret information in the EAT statement
T_i	Test flag variable
X_i	Test result register in the EAT statement
E	Eve's system
Ω	An event
$\rho[\Omega]$	Probability of $\Omega \subset \mathcal{X}$ for ρ_{XA} (See main text in Section 2.1)
$\mathsf{freq}()$	Frequency of a given event
$\boldsymbol{q}$	A probability vector
$\mathbb{P}(\mathcal{X})$	The probability vector space with events from $\mathcal{X}$
$\mathrm{D}(A)$	The set of quantum states on Hilbert space A

Table 1: Overview of notational conventions.

For consistency, we at times use the notation for quantum states conditioned on an event

6

from previous works [16, 17]. Let $\mathcal{X}$ be a finite alphabet, $X \cong \mathbb{C}^{|\mathcal{X}|}$. Then a classical-quantum (CQ) state may be written as $\rho_{XA} = \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes \rho_{A,x}$ where the quantum part of this decomposition is generally called the conditional state. Given an event $\Omega \subset \mathcal{X}$, the probability of the event is $\rho[\Omega]$, which may be calculated by $\rho[\Omega] := \sum_{x \in \Omega} \text{Tr}[\rho_{A,x}]$. Lastly, the state conditioned on the event is given by $\rho_{XA|\Omega} = \frac{1}{\rho[\Omega]} \sum_{x \in \Omega} \rho_{A,x}$. Note that a conditioned state is therefore re-normalized.

We will also require various entropies which we also introduce here. We use the notation of [16, 17]. We refer to [34] for further background, but note that the notation differs in that work.

For $\alpha \in (0,1) \cup (1,\infty)$, define the minimal divergence by

$$D_\alpha(\rho||\sigma) := \begin{cases} \frac{1}{\alpha-1} \log \frac{\|\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\|_\alpha^\alpha}{\text{Tr}(\rho)} & \text{if } \alpha < 1 \text{ or if } \alpha > 1 \text{ and } \text{supp}(\rho) \subseteq \text{supp}(\sigma) \\ +\infty & \text{otherwise} \end{cases},$$

where $\|\cdot\|_p$ is the Schatten p-norm for $p \geq 1$ and the definition is extended to all $p > 0$. For any $\rho \in \text{D}(A \otimes B)$, $\sigma \in \text{D}(B)$, define

$$H_\alpha(\rho_{AB}||\sigma_B) := -D_\alpha(\rho_{AB}||\mathbb{1}_A \otimes \sigma_B).$$

We then define $H_\alpha(A|B)_{\rho_{AB}} := H_\alpha(\rho_{AB}||\rho_B)$ and $H_\alpha^\uparrow(A|B)_\rho := \sup_{\sigma_B} -D_\alpha(\rho_{AB}||\mathbb{1}_A \otimes \sigma_B)$. We refer to both these classes of entropies as sandwiched Rényi entropies. We may also recall the smooth min-entropy defined by

$$H_{\min}^\varepsilon(A|B)_{\rho_{AB}} := \max_{\tilde{\rho} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}},$$

where $H_{\min}(A|B)_{\rho_{AB}} := -\log(\min\{\text{Tr}(Y) : \rho_{AB} \leq \mathbb{1}_A \otimes Y_B \})$, $\mathcal{B}^\epsilon(\rho_{AB}) := \{\tilde{\rho}_{AB} \geq 0 : \text{Tr}(\tilde{\rho}_{AB}) \leq 1 \& P(\tilde{\rho}_{AB}, \rho_{AB}) \leq \varepsilon\}$, and P is the purified distance [35, 34]. Throughout this work, log is referred to $\log_2$.

2.2 QKD security definition

We provide a short review of the ε-security framework of QKD [13, 36]. A QKD protocol is ε-secure if for any input state, the output state $\rho_{S_A S_B E}$ conditioned on that the protocol does not abort (and thus subnormalized) satisfies

$$\frac{1}{2}\|\rho_{S_A S_B E} - \pi_{S_A S_B} \otimes \rho_E\|_1 \leq \varepsilon, \tag{1}$$

where $\pi_{S_A S_B} = \sum_{s \in \mathcal{S}} \frac{1}{|\mathcal{S}|} |s\rangle\langle s| \otimes |s\rangle\langle s|$, and $\mathcal{S}$ is the space of keys that could be generated from the protocol. The security parameter ε quantifies the amount of deviation of the real protocol from an ideal protocol. In an ideal QKD protocol, Alice and Bob are supposed to obtain an identical key, which is the correctness requirement; The key is supposed to be distributed from a uniform distribution among all possible keys and that Eve knows no information about the key, which is the secrecy requirement. This security definition in terms of trace distance has an operational interpretation: If a distinguisher is given either the real or the ideal protocol as a black box with an equal *a priori* probability and the goal is to verify which protocol the black box implements, then the probability that this distinguisher can guess correctly by looking at output states of the black box is at most $\frac{1}{2}(1 + \varepsilon)$. We note that in the case of aborting, both protocols output a trivial key symbol.

In Eq. (1), we use subnormalized states. Equivalently, if we define in terms of normalized output states $\tilde{\rho}_{S_A S_B E} = \rho_{S_A S_B E}/\text{Tr}(\rho_{S_A S_B E})$ and $\tilde{\rho}_E = \rho_E/\text{Tr}(\rho_E)$ where $\text{Tr}(\rho_{S_A S_B E}) = $

$\text{Tr}(\rho_E) := \text{Pr}(\text{accept})$ denotes the probability that the protocol does not abort, then Eq. (1) can be written as

$$\frac{1}{2} \text{Pr}(\text{accept}) \|\tilde{\rho}_{S_A S_B E} - \pi_{S_A S_B} \otimes \tilde{\rho}_E\|_1 \leq \varepsilon \ . \tag{2}$$

It is often convenient to discuss the secrecy requirement and correctness requirement separately since the correctness requirement is usually guaranteed by the error correction and error verification steps of a QKD protocol. A key is ε_{sec}-secret if

$$\frac{1}{2} \|\rho_{S_A E} - \pi_{S_A} \otimes \rho_E\|_1 \leq \varepsilon_{\text{sec}} \ , \tag{3}$$

where $\pi_{S_A} = \sum_{s \in \mathcal{S}} \frac{1}{|\mathcal{S}|} |s\rangle\langle s|$. A QKD protocol is ε_{cor}-correct if the joint probability that the protocol does not abort and that Bob's key is different from Alice's key is at most ε_{cor}. By the triangle inequality of the trace norm, it is easy to see that if the QKD protocol is ε_{cor}-correct and it generates ε_{sec}-secret keys, then the protocol is ε-secure with $\varepsilon = \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}$.

3   The Entropy Accumulation Theorem

In this section we review the Entropy Accumulation Theorem (EAT) [16, 17] which is the unifying technical tool of this work. The EAT is motivated as follows. Fundamentally, the formal property of secrecy using a process with a finite number of rounds is characterized by the smooth min-entropy [13]. Unfortunately, the smooth min-entropy is a functional that is difficult to calculate directly for large systems. It therefore follows that one wishes to determine tight bounds on the smooth min-entropy of a given process via a reduction that is computationally feasible. The EAT accomplishes this task for well-behaved sequential processes. The idea of the EAT is that, under some reasonable behavior, one can bound the smooth min-entropy of the finite-length process by the worst-case accepted asymptotic behavior along with some correction terms.

However, in this work we find empirically that a recent work that characterizes secrecy using the sandwiched Rényi entropies $H_\alpha^\uparrow$ [29] can lead to improved key rates. As such, rather than presenting results in terms of smoothed entropies in the main text, we present them in terms of $H_\alpha^\uparrow$ entropies. For completeness and perhaps intuition, in Appendix D, we present all results in terms of smooth entropies. We now present the formal statement of the EAT along with relevant definitions after which we elaborate on the intuition and relation to the rest of this work.

3.1   Formal statement

To formally state the EAT, we review some definitions first [16, 17] (See Figure 1 for a visualization).

Definition 1 (EAT Channels). *EAT channels are Completely Positive Trace-Preserving (CPTP) maps*

$$\mathcal{M}_i : R_{i-1} \to S_i P_i X_i R_i \tag{4}$$

where for all $i \in \{1, \cdots n\}$, R_i are quantum systems (with $R_n \cong \mathbb{C}$ the trivial register) and where S_i, P_i, and X_i for $i \in \{1, \cdots n\}$ are classical systems taking values in $\mathcal{S}, \mathcal{P}$, and $\mathcal{X}$ respectively.

Furthermore, we assume that X_i is a deterministic function of S_i and P_i. In other words, the EAT channels can be decomposed as

$$\mathcal{M}_i = \mathcal{T}_i \circ \mathcal{M}_i' \tag{5}$$
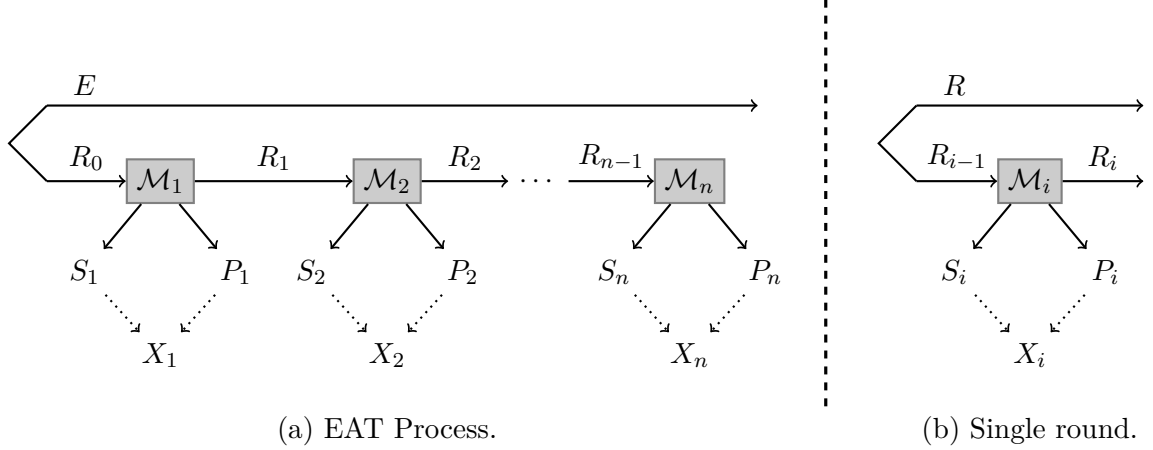
8

(a) EAT Process. (b) Single round.

Figure 1: Diagrammatic depiction of EAT process and theorem. (a) Captures the overall process and (b) is the process captured by the min-tradeoff function (See Definition 2). They are related by the Entropy Accumulation Theorem (Theorem 1). Note that $\mathcal{M}_n$ may be viewed as outputting a trivial register, $R_n \cong \mathbb{C}$, which we have suppressed. The output of the EAT process is $\rho_{S_1^n P_1^n X_1^n E}$, the output registers along with the purification.

where $\mathcal{M}_i' : R_{i-1} \to S_i P_i R_i$ is some CPTP map and where $\mathcal{T}_i : S_i P_i \to S_i P_i X_i$ is a classical operation assigning a value for X_i as a function of S_i and P_i of the form

$$\mathcal{T}_i(W_{S_i P_i}) = \sum_{s \in \mathcal{S},\, p \in \mathcal{P}} (\Pi_{S_i,s} \otimes \Pi_{P_i,p}) W_{S_i P_i} (\Pi_{S_i,s} \otimes \Pi_{P_i,p}) \otimes |t(s,p)\rangle \langle t(s,p)|_{X_i}, \qquad (6)$$

where $\{\Pi_{S_i,s} : s \in \mathcal{S}\}$ and $\{\Pi_{P_i,p} : p \in \mathcal{P}\}$ are families of mutually orthogonal projectors on S_i and P_i, and the function $t : \mathcal{S} \times \mathcal{P} \to \mathcal{X}$ is a deterministic function.

In the above definition, the registers S_i and P_i stand for 'secret' key registers and 'public' announcement registers respectively as this will be the natural interpretations of these registers in the context of cryptography. The X_i register is then a 'testing' register which is a function of the secret and public registers. Note that we consider the particular case of classical systems S_i and P_i, compared to [16, 17, 29] where they can be quantum, as this is sufficient for this work. The main idea of the EAT channels is that they can be composed such as in Figure 1, starting from an initial state $\rho_{R_0 E}^0 \in \mathrm{D}(R_0 \otimes E)$ and applying the EAT maps sequentially to produce the output state

$$\rho_{S_1^n P_1^n X_1^n E} = (\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1 \otimes \mathcal{I}_E)(\rho_{R_0 E}^0). \qquad (7)$$

The most important restriction on this state is that we require it to satisfy the Markov chain conditions:

$$S_1^{i-1} \leftrightarrow P_1^{i-1} E \leftrightarrow P_i \qquad \forall i \in \{1, \ldots, n\}, \qquad (8)$$

where one may recall a quantum Markov chain, denoted $A \leftrightarrow B \leftrightarrow C$, is a quantum state ρ_{ABC} such that the conditional mutual information is zero, i.e. $I(A : C|B) = 0$.[6] It follows the Markov chain conditions are claims about the mutual information between the previous secret

---

[6]There exist other characterizations of quantum Markov chains, though the characterization presented here is sufficient for our exposition. See [37] for further information on quantum Markov chains.

registers and the previous public registers (along with Eve's information) when conditioned on the current public announcement. The reason this is important to the proof of the theorem is that the Markovian behavior restriction guarantees that the process (defined by the sequential application of $\mathcal{M}_i$) does not *a priori* destroy entropy being accumulated in the S_1^n registers. It does this by guaranteeing that, for each $i \in [n]$, the public announcement in round i, P_i, is not correlated to the generated secret information of previous rounds, S_1^{i-1}, when we condition on the side information E and all public announcements up to then P_1^{i-1}.

It is also perhaps useful to preemptively stress that the EAT channels do not have to be a model of the actual implementation, rather they only need to capture the same relationships between the output random variables S_1^n, P_1^n and X_1^n as the actual implementation because the entropy only depends on the random variables. This insight is what allowed the EAT to be used for device-independent information processing where dimensions cannot be bounded.

Definition 2 (Min-tradeoff functions). *An affine function f on the space of probability distributions $\mathbb{P}(\mathcal{X}) = \{\boldsymbol{p} \in \mathbb{R}^{|\mathcal{X}|} : \boldsymbol{p}(x) \geq 0, \sum_x \boldsymbol{p}(x) = 1\}$ is called a min-tradeoff function for the EAT channel $\mathcal{M}_i$ if it satisfies*

$$f(\boldsymbol{q}) \leq \min_{\nu \in \Sigma_i(\boldsymbol{q})} H(S_i | P_i R)_\nu \quad \forall \boldsymbol{q} \in \mathbb{P}(\mathcal{X}), \tag{9}$$

where the minimization is over the set of quantum states compatible with the statistics $\boldsymbol{q}$ that is defined as below:

$$\Sigma_i(\boldsymbol{q}) := \left\{ \nu_{S_i P_i X_i R_i R} = (\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1} R}) : \omega \in \mathrm{D}(R_{i-1} \otimes R) \text{ and } \nu_{X_i} = \boldsymbol{q} \right\}, \tag{10}$$

where R is isomorphic to R_{i-1}.

Remark 1. Note that Ref. [16] considers affine functions. However, because of $\sum_x \boldsymbol{q}(x) = 1$, any affine function on $\mathbb{P}(\mathcal{X})$ can be represented as a linear function. In particular, f can be specified by a vector $\boldsymbol{f} \in \mathbb{R}^{|\mathcal{X}|}$, that is, $f(\boldsymbol{q}) = \boldsymbol{f} \cdot \boldsymbol{q} := \sum_x \boldsymbol{f}(x)\boldsymbol{q}(x)$. We note that this is equivalent to an affine function since for an affine function $f_0' + \boldsymbol{f}' \cdot \boldsymbol{q}$, one can define $\boldsymbol{f}(x) = \boldsymbol{f}'(x) + f_0' \ \forall x \in \mathcal{X}$ such that $f_0' + \boldsymbol{f}' \cdot \boldsymbol{q} = \boldsymbol{f} \cdot \boldsymbol{q}$.

By Definition 2, the min-tradeoff function characterizes the minimum amount of (von Neumann) entropy of the secret information conditioned on the public information and quantum side-information (encoded as the register R) for all probability distributions on the testing register. This encapsulates the notion of the minimum von Neumann entropy being accumulated in a given round. For QKD security proofs, the min-tradeoff function can be seen as the term that bounds Eve's ignorance about the key in the asymptotic regime given by the Devetak-Winter formula [38], and so the min-tradeoff function may be seen as determining the first-order term in a finite-size key distillation protocol.

With these considerations, we can state the EAT with its improved second order term [17].

Theorem 1 (Special Case of Proposition V.3 of [17]). *Consider EAT channels $\mathcal{M}_1, ..., \mathcal{M}_n$ and their output $\rho_{S_1^n P_1^n X_1^n E}$ such that it satisfies the Markov conditions and S_i is a classical register for all $i \in [n]$. Let $h \in \mathbb{R}$, $\alpha \in (1, 2)$, and f be a min-tradeoff function for $\mathcal{M}_1, \ldots, \mathcal{M}_n$. Then, for any event $\Omega \subseteq \mathcal{X}^n$ that implies $f(\mathsf{freq}(X_1^n)) \geqslant h$,[7]*

$$H_\alpha^\uparrow(S_1^n | P_1^n E)_{\rho_{|\Omega}} > nh - n\frac{(\alpha - 1)\ln 2}{2}V^2 - \frac{\alpha}{\alpha - 1}\log\frac{1}{\rho[\Omega]} - n(\alpha - 1)^2 K_\alpha \tag{11}$$

---

[7]Following [16], we say an event $\Omega \subseteq \mathcal{X}^n$ implies $f(\mathsf{freq}(X_1^n)) \geq h$ if for every $x_1^n \in \Omega$, $f(\mathsf{freq}(X_1^n)) \geq h$.

holds for

$$V = \sqrt{\mathsf{Var}(f) + 2} + \log\left(2d_S^2 + 1\right) \tag{12}$$

$$K_\alpha = \frac{1}{6(2-\alpha)^3 \ln 2} 2^{(\alpha-1)(\log d_S + (\mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)))} \ln^3\left(2^{\log d_S + (\mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))} + e^2\right) \tag{13}$$

where

$$\begin{aligned}
\mathsf{Max}(f) &:= \max_{\boldsymbol{q} \in \mathbb{P}(\mathcal{X})} f(\boldsymbol{q}), \\
\mathsf{Min}(f) &:= \min_{\boldsymbol{q} \in \mathbb{P}(\mathcal{X})} f(\boldsymbol{q}), \\
\mathrm{Min}_\Sigma(f) &:= \min_{\boldsymbol{q}: \Sigma_i(\boldsymbol{q}) \neq \emptyset} f(\boldsymbol{q}), \\
\mathrm{Var}(f) &:= \max_{\boldsymbol{q}: \Sigma_i(\boldsymbol{q}) \neq \emptyset} \sum_x \boldsymbol{q}(x) \boldsymbol{f}(x)^2 - \left[\sum_x \boldsymbol{q}(x) \boldsymbol{f}(x)\right]^2
\end{aligned} \tag{14}$$

and $d_S = \max_{i \in [n]} |S_i|$ is the maximum dimension of the systems S_i.

Remark 2. Note that, beyond the Markov chain conditions, the EAT applying to a state depends on the event $\Omega \subseteq \mathcal{X}^n$ implying $f(\mathsf{freq}(X_1^n))$. Letting $\mathcal{Z}$ be a finite alphabet, if one is interested in an event $\Omega' \subseteq \mathcal{Z}^n \times \mathcal{X}^n$ that guarantees such an Ω (i.e. $\Pr[\Omega|\Omega'] = 1$ which denotes the probability of event Ω conditioned on event Ω') then, assuming the conditions for EAT held on generating X_1^n, S_1^n, P_1^n, the EAT will hold for $\rho_{X_1^n S_1^n P_1^n E_{|\Omega'}}$. This has been used implicitly in previous works such as [18], but we stress it here for completeness as we also use it.

It is worth noting the above theorem from [17] is actually an improved version of the original EAT [16]. The improvement is in the the second-order term where the dependency on the gradient of the min-tradeoff function f is eliminated, which for certain applications caused the second-order term to dominate. We note that for a specific choice of α, one can write Eq. (11) in the form $H_\alpha^\uparrow > nh - O(\sqrt{n})$ [17] to clearly separate the first-order and second-order terms. However, we do not state it in this form because, while asymptotically optimal, to get the best finite size bounds we will optimize over the parameter $\alpha \in (1,2)$ as suggested in [17]. It is also noted that the exact from of the expression of K_α here uses the fact that S_i is classical [17, Dicussion after Eq. (22)].

3.2 Applying EAT to device-dependent QKD

3.2.1 Tensor product structure

As noted earlier, the EAT maps in general do not have to be the same maps as the actual process as long as they capture the same relationship between output random variables. In the case of device-independent information processing, this is necessary since one cannot describe the device itself. In contrast, for device-dependent QKD as we consider here, without loss of generality we can let the EAT maps model the guaranteed behavior of the device in each round. It then follows that the EAT maps act on separate quantum systems. Formally, if we let $(Q_i)_{i \in [n]}$ be n quantum systems then we can consider the n rounds of the QKD protocol as n CPTP maps of the form

$$\widetilde{\mathcal{M}}_i : Q_i \to S_i P_i X_i, \tag{15}$$

each acting independently on its own Q_i space. It follows that these maps can be expressed in the notation of the EAT theorem by defining the EAT channels $\mathcal{M}_i : R_{i-1} \to S_i P_i X_i R_i$ as follows:

$$\mathcal{M}_i = \widetilde{\mathcal{M}}_i \otimes \mathcal{I}_{Q_{i+1}^n} \tag{16}$$

where $R_i = \bigotimes_{j=i+1}^n Q_j$ and $\mathcal{I}_{Q_{i+1}^n}$ is the identity map on the registers Q_{i+1}^n. In other words, at round i the EAT channel $\mathcal{M}_i$ effectively only acts on the system Q_i to produce the outputs S_i, P_i, and X_i, but not on the next systems Q_{i+1}^n.

By the fact that the outputs S_i and P_i are classical, we can make another simplification. In this case, the first requirement in Definition 1 of the EAT channels boils down to the requirement that X_i is obtained by applying a deterministic function on S_i and P_i: $x_i = t(s_i, p_i)$. In typical QKD protocols, we can further assume this function is identical for all rounds. Under this assumption, the EAT channels are thus entirely defined by specifying the function t and the POVM elements $\{M_{sp}\}_{s,p}$ such that

$$\widetilde{\mathcal{M}}_i(\rho) = \sum_{s,p} \mathrm{Tr}(\rho M_{sp}) \, |s,p\rangle\langle s,p|_{S_i P_i} \otimes |t(s,p)\rangle\langle t(s,p)|_{X_i} \tag{17}$$

for all $\rho \in \mathrm{D}(Q_i)$. These POVM elements $\{M_{sp}\}_{s,p}$ are uniquely associated to $\widetilde{\mathcal{M}}_i$ and satisfy $M_{sp} \geq 0$ and $\sum_{s,p} M_{sp} = \mathbb{1}$.

Now that we have reduced the scope of the EAT theorem, we still have two challenges to solve. The first challenge is how we can generate the best possible min-tradeoff function. The second is how we guarantee the Markov chain conditions in Eq. (8).

3.2.2 Challenge 1: constructing optimal min-tradeoff functions

It is desirable to have a general procedure (applicable to many protocols) to construct min-tradeoff functions according to Definition 2. In addition to having valid min-tradeoff functions, we would like to find the best possible min-tradeoff function that can produce as tight key rates as possible for each signal block size when it is used in the EAT. In general, the construction of tight min-tradeoff functions is difficult. The difficulty arises from the non-trivial behavior of the conditional von Neumann entropy of the output state of a map (in this case the EAT channel) as a function of the resulting observations. We note that while for certain small-dimensional and theoretically simple QKD protocols, it may be possible to determine the optimal min-tradeoff function from uncertainty relations [16, Section 5.1], the analytic construction of min-tradeoff functions for generic device-dependent protocols is less straightforward, and thus it warrants a numerical method. This issue has also been recognized in the device-independent scenario and been addressed with its own numerical method [26]. In this work, we address this issue in the device-dependent setting and utilize additional structures of device-dependent QKD protocols. In Section 6, we present two algorithms for numerically constructing (almost) tight min-tradeoff functions in the case where one knows the structure of the EAT channels.

3.2.3 Challenge 2: guaranteeing Markov chain conditions

The Markov chain conditions [Eq. (8)] put strong restrictions on the maps $\mathcal{M}_i$'s that can be used with the EAT theorem. Roughly speaking, it states that, from the point of view of the adversary E, the process at round j does not leak information about the secret register(s) S_i of previous rounds $i < j$. In typical device-independent protocols, this restriction on the output state is in a sense trivially satisfied as all public announcements P_i, such as measurement settings, are independently seeded with random numbers. In other words, the probability distribution of the announcement P_i does not depend on the state sent by Eve. Formally, if $\{p\}$ is the set of public announcements in round i and there are n rounds, then the Markov chain conditions trivially hold if $\Pr[p|\rho_i] = \Pr[p] \ \forall \rho_i \in \mathrm{D}(Q_i), \ \forall i \in [n]$, i.e., the distribution over announcements is independent of the state being measured in each round.

However, one advantage of device-dependent QKD over device-independent QKD is its ability to have more complicated public announcement structures. One example is postselection on

detection events in device-dependent QKD. Postselection implicitly requires an announcement. However, since the probability of a detection event depends on the state sent by Eve, the public announcement is not based on independently seeded randomness. A simple argument shows that this is potentially problematic, as it can lead to a violation of the Markov chain conditions, even when the EAT channels act on independent systems. This happens when Eve prepares a pure state $|\phi\rangle_{Q_1^n E} = |\psi\rangle_{Q_1^n} \otimes |\psi'\rangle_E$, entangled between different rounds but not with her quantum memory. In that case, there can be correlations between announcements in one round and the private key register in another round. This could potentially prevent us from applying the EAT even if Eve could only learn from the public announcement. We therefore prove in Section A that the following condition (Definition 3) still guarantees the Markov conditions hold for Eve's optimal attack, which is sufficient for applying the EAT (Theorem 1). We state this result below as Theorem 2.

Definition 3. *Given some quantum-to-classical CPTP map $\mathcal{W} : Q \to SP$ which can be fully specified by a POVM $\{M_{sp} : s \in \mathcal{S},\ p \in \mathcal{P}\}$, we say that the variable P is* weakly dependent *(on the input state) when there exists a decomposition of the input space Q into a direct sum of orthogonal subspaces V^λ, i.e., $Q = \bigoplus_\lambda V^\lambda$, such that*

(a) *the channel $\mathcal{W}$ is block diagonal along V^λ: i.e., its POVM elements are of the form $M_{sp} = \bigoplus_\lambda M_{sp}^{(\lambda)}$ with $M_{sp}^{(\lambda)} \in \mathcal{L}(V^\lambda)$ acting on V^λ;*

(b) *the probability of an announcement P is the same for all states in a given subspace V^λ: i.e., there exist constants $c_{p,\lambda}$'s such that*

$$\mathrm{Pr}_P(p|\rho_\lambda) = c_{p,\lambda}, \quad \textit{for all } \rho_\lambda \in D(V^\lambda) \tag{18}$$

where $\mathrm{Pr}_P(p|\rho_\lambda) := \mathrm{Tr}[M_p \rho_\lambda]$ with $M_p = \sum_s M_{sp}$.

Note that (b) in the definition is equivalent to saying that for each λ and p, $M_p^{(\lambda)} := \sum_s M_{sp}^{(\lambda)} = c_{p,\lambda} \mathbb{1}_{V^\lambda}$ is proportional to the identity. This means that, equivalently, for any $\sigma \in Q$, $\mathrm{Pr}_P(p|\sigma) = c_{p,\lambda} \mathrm{Tr}[\Pi_\lambda \sigma \Pi_\lambda]$, where Π_λ is the projector onto the subspace, i.e. the announcement only depends on a constant and the weight of the state on the subspace, which makes it 'weakly' dependent on the state. For intuition, this is distinct from independently randomly seeded announcements where each announcement has POVM elements of the form $M_p = c_p \mathbb{1}_Q$, which results in the announcement being independent on the state all together. Note the independently randomly seeded case trivially satisfies Definition 3, and so it is a (strictly) special case of weakly dependent announcements.

Here we state that the advantage of weakly dependent announcements is that they guarantee the EAT may be applied.

Theorem 2. *If the announcements P_i of the CPTP maps $\widetilde{\mathcal{M}}_i : Q_i \to S_i P_i X_i$ are weakly dependent, then the result of Theorem 1 may be applied to prove security.*

We give a physical intuition why this theorem would hold and defer the proof to Section A. The POVM being of the block-diagonal form in Definition 3 means the subspace information is knowable to Eve. This is because without loss of generality, Eve should send such block-diagonal states and so she knows the information by implementing a quantum nondemolition (QND) measurement that determines the subspace which she then stores in a secondary register.

Indeed, this idea of Eve having an extra register with the subspace information is how this is proven in Section A. We note equivalently that Eve's purification of such a block-diagonal state includes the subspace information and so it is knowable to Eve from the perspective of purification as well.

4 The Quantum Key Distribution Protocol

In this section we present the class of entanglement-based (EB) QKD protocols for which we prove security. At a high level, there are three related protocols: the QKD protocol for physical implementations (Protocol 1), its equivalent virtual QKD protocol (Protocol 2) for security proof purposes, and the (also virtual) Entropy Accumulation subprotocol (Protocol 3), referred to as the EAT subprotocol, to which we apply the EAT to derive a desired entropic bound. The virtual QKD protocol requires certain properties so that the EAT subprotocol can be applied to its analysis. Of particular importance is that the virtual QKD protocol can be thought of as acting sequentially, i.e. the signals are processed round by round, and that the announcements satisfy the Markov chain conditions in Eq. (8). The necessary properties of the virtual QKD protocol impose necessary structures on the physical implementation of the protocol so that it is equivalent to the virtual QKD protocol, where equivalence is in terms of the (quantum) random variables generated as this is what both the EAT and the security proof more generally consider.

4.1 Physical and virtual protocol description

In this section, we present the physical QKD protocol followed by the virtual QKD protocol to which it is equivalent.

Protocol 1 Physical Device-Dependent Quantum Key Distribution Protocol

Inputs:

$\{M_a^A\}_a, \{M_b^B\}_b$	Alice and Bob's measurement devices (POVMs)
$\mathbf{K}$	Subset of Alice and Bob's public announcements to be kept during sifting
$n \in \mathbb{N}_+$	Number of rounds
$\gamma \in (0, 1]$	Probability of testing
$\mathcal{Q}$	Set of acceptable frequency distributions over $\mathcal{X}$

Protocol:

For $i \in [n]$, do Steps 1 to 4:

1. **State Transmission**: A source (that may be under Eve's control) distributes a state ρ_{Q_i} between Alice and Bob.

2. **Measurements**: Alice and Bob implement their local POVMs $\{M_a^A\}_a$, $\{M_b^B\}_b$ to measure their respective halves of the state and record their outcomes.

3. **Data Partition**: Alice partitions her data into (data that will eventually be) public $\widetilde{A}_i$ and (data that will stay) private $\overline{A}_i$. Likewise, Bob partitions his data into public $\widetilde{B}_i$ and private $\overline{B}_i$.

4. **Testing Designation**: Alice randomly chooses $T_i \in \{0, 1\}$ according to $\Pr(T_i = 1) = \gamma$.

5. **Announcements**: Alice and Bob announce their public data $\widetilde{A}_1^n$ and $\widetilde{B}_1^n$, respectively. Alice then announces T_1^n. For all $i \in [n]$ such that $T_i = 1$, Alice announces $\overline{A}_i$.

14

6. **Parameter Estimation**: For all $i \in [n]$, Bob computes X_1^n according to $X_i = t(\overline{A}_i, \overline{B}_i, \widetilde{A}_i, \widetilde{B}_i)$ if $T_i = 1$ and $X_i = \perp$ otherwise, where t is a deterministic function. Alice and Bob abort the protocol if $\mathsf{freq}(X_1^n) \notin \mathcal{Q}$.

7. **General Sifting**: If $(\widetilde{A}_i, \widetilde{B}_i, T_i) \in \mathbf{K}^C \times \{0\}$, Alice sets the $\overline{A}_i = \perp$, where $\mathbf{K}^C$ is the complement of $\mathbf{K}$.

8. **Key Map**: If $(\widetilde{A}_i, \widetilde{B}_i, T_i) \in \mathbf{K} \times \{0\}$, Alice updates $\overline{A}_i := f_{KM}(\overline{A}_i, \widetilde{A}_i, \widetilde{B}_i)$ where f_{KM} is the key map. This subset of rounds may be denoted as the register $\mathbf{Z}$, Alice's raw key.

9. **Error Correction & Detection:** Using an error correction scheme, Alice and Bob communicate for Bob to construct his guess of Alice's raw key, $\widehat{\mathbf{Z}}$. He then uses a 2-universal hash function to send a hash of his guess to Alice. This detects if the correction worked. If it did not, they abort. Otherwise, they continue.

10. **Privacy Amplification:** Using a family of 2-universal hash functions, Alice and Bob perform privacy amplification to achieve the desired secrecy.

A few remarks are necessary. First, we have implicitly required that the announcement structure of the protocol be round by round. This announcement structure is necessary to move to our virtual protocol as we need a protocol that is sequential for the majority of the steps. Second, we have required no announcements be made until all of the measurement data have been obtained. This is important as it avoids Eve altering her actions depending on announcements. This requirement makes the protocol equivalent to the one where Eve distributes the whole n-round state (for which she may hold a purification) at the beginning and then only gains additional information via Alice's and Bob's announcements. The latter will be the necessary structure for the virtual protocol. Third, we have required the function t in Step 6 to be deterministic. This is a condition needed to apply the Entropy Accumulation Theorem [see Eq. (6)], but it does not seem limiting for standard protocols.

We note that requiring the testing be done round by round specifically differs from standard practice in device-dependent QKD security proofs [13] which perform fixed-length parameter estimation. Fixed-length parameter estimation is when, before the protocol is executed, it is decided that m of the n signals will be used for parameter estimation. Then, rather than having Steps 4 and 6 of Protocol 1, the protocol would include Alice uniformly choosing a bit string from the set of bit strings of length n and Hamming weight m which determines which rounds to test. This is not necessarily a large gap if one considers testing probability γ such that $\gamma n = m$, as a Bernoulli variable converges to its mean quickly. However, for rigor, after proving the security of Protocol 2, which is equivalent to the security of Protocol 1, in Section 5.2.1, we present how to convert statements of security on this probabilistic round-by-round testing protocol to statements of security on the fixed length testing protocol without introducing any looseness.

Lastly, we note that we need the extra assumption beyond being round by round that the announcements satisfy the Markov conditions. More technically, the announcement structure will have to be such that the virtual QKD protocol would satisfy the Markov chain conditions in Eq. (8) in the case that Alice did not announce her fine-grained data $\overline{A}_i$ when the round i is a testing round, i.e., $T_i = 1$. Since Alice does announce her fine-grained data during testing rounds, we stress why this works preemptively. If Alice's fine-grained data $\overline{A}_i$ is announced publicly, it could threaten the Markov chain conditions by leaking too much information if Eve sends states that are correlated across rounds. However, this fine-grained data is needed by Bob to compute X_i on testing rounds, so we require Alice to announce this data. We therefore need a way to address this. In the security proof, we start with the conditional entropy of Alice's raw

key which, among other registers, is conditioned on Eve knowing the fine-grained data Alice announces during testing rounds. By applying entropic chain rules, we are able to convert to a conditional entropy term corresponding to the case in which Alice kept all fine-grained data private. In this case, the Markov conditions hold by restrictions on the announcement structure we require. The final technical issue is that physically X_i needs to be computed using $\overline{A}_i$ and $\overline{B}_i$. It follows that if neither party has both registers, there is no physical process to compute X_i. However, this is not an issue as the EAT subprotocol is virtual (that is, there is no need to implement this protocol in practice) and only needs to generate the same (quantum) random variables as the real process. Therefore we construct a sequence of protocols where the security claim on the physical protocol holds by the equivalence to the security of the virtual protocol whose security relies on a virtual EAT subprotocol. We also note for intuition that there is a penalty to the key rate by announcing the $\overline{A}_i$ in the aforementioned chain rules, which is not a part of the virtual EAT subprotocol. We discuss the specific assumptions on the announcement structure to guarantee the Markov chain conditions hold in Section 4.2 after presenting the virtual QKD protocol.

We now present the virtual QKD protocol. Given the discussion above, we note that the difference from the physical QKD protocol is that announcements, sifting, generation of the test round data (but not aborting based on the test data), and the key map are all implemented round by round. Beyond this conversion of many steps to being performed sequentially, the virtual QKD protocol is the same as the physical one. This is what will allow the protocols to be equivalent.

Protocol 2 Virtual Device-Dependent Quantum Key Distribution Protocol

Inputs:

$\{M_a^A\}_a, \{M_b^B\}_b$	Alice and Bob's measurement devices (POVMs)
$\mathbf{K}$	Subset of Alice and Bob's public announcements to be kept during sifting
$n \in \mathbb{N}_+$	Number of rounds
$\gamma \in (0, 1]$	Probability of testing
$\mathcal{Q}$	Set of acceptable frequency distributions over $\mathcal{X}$

Protocol:

0. **State Transmission:** Eve distributes the n states, which may be entangled in an arbitrary manner, such that the total state is of the form $\rho_{Q_1^n E}$.

   For $i \in [n]$, do Steps 1 to 6:

1. **Measurements**: Alice and Bob implement their local POVMs $\{M_a^A\}_a$, $\{M_b^B\}_b$ to measure their respective halves of the state and record their outcomes.

2. **Data Partition and Announcement:** Alice partitions her data into public $\widetilde{A}_i$ and private $\overline{A}_i$. Likewise, Bob partitions his data into public $\widetilde{B}_i$ and private $\overline{B}_i$. Then they announce their public data.

3. **Testing Designation**: Alice randomly chooses $T_i \in \{0, 1\}$ according to $\Pr(T_i = 1) = \gamma$.

4. **General Sifting**: If $(\widetilde{A}_i, \widetilde{B}_i, T_i) \in \mathbf{K}^C \times \{0\}$, Alice sets the $\overline{A}_i = \perp$. Denote

$$\mathcal{S} = \{i \in [n] : (\widetilde{A}_i, \widetilde{B}_i, T_i) \in \mathbf{K}^C \times \{0\}\}$$

   so that $\overline{A}_{\mathcal{S}}$ denotes the registers of discarded rounds.

5. **Key Map**: If $(\widetilde{A}_i, \widetilde{B}_i, T_i) \in \mathbf{K} \times \{0\}$, Alice updates $\overline{A}_i := f_{KM}(\overline{A}_i, \widetilde{A}_i, \widetilde{B}_i)$ where f_{KM} is the key map. This subset of rounds may be denoted as the register $\mathbf{Z}$, Alice's raw key.

6. **Statistical Tests**:

    - If $T_i = 1$, Alice announces $\overline{A}_i$ publicly. Using this, Bob generates X_i using a deterministic function t such that $X_i = t(\overline{A}_i, \overline{B}_i, \widetilde{A}_i, \widetilde{B}_i)$.
    - If $T_i = 0$, Bob sets $X_i = \perp$.

    Denote $\mathcal{T} = \{i \in [n] : T_i = 1\}$. Then the registers Alice announces are $\overline{A}_{\mathcal{T}}$.

7. **Parameter Estimation**: Alice and Bob abort the protocol if $\mathsf{freq}(X_1^n) \notin \mathcal{Q}$.

8. **Error Correction and Parameter Estimation**: Do Steps 9 and 10 of Protocol 1.

We note that both Protocols 1 and 2 assume Alice establishes the key. However, if Bob were to establish the key, this merely switches the roles of Alice and Bob in Protocol 1 and Protocol 2. Thus, this setting is not a restriction. Furthermore, we emphasize we still require that testing be determined in a round-by-round manner as the EAT is an i.i.d. reduction for sequential processes, which was discussed earlier.

The only remaining assumption to make explicit is the ability to guarantee the Markov chain conditions hold from the announcement structure.

4.2 Assumptions on public announcements

To verify the applicability of the EAT for a given protocol, we need to verify that the conditions from Theorem 2 are satisfied. This puts some restrictions on the type of protocols that can be included in our security proof and more specifically on the type of announcements and postselection that we can do.

Theorem 2 says that the partitioned announcements can have some dependence on the state, but only in a limited way. It can only depend on the subspace V^λ in which the state lies. The underlying reason for this is that for block diagonal measurements, we can assume without loss of generality that Eve sends a state $\rho_{Q_1^n E}$ where each state in register Q_i is block diagonal and so she already holds that information in her purification. We therefore do not give her new information about the state by leaking $\widetilde{A}_i$ and $\widetilde{B}_i$. Recall that announcements being independent of the input state is a particular case of this setting as explained in Section 3.2.3.

To summarize, we make the following assumption throughout this work, which guarantees we can apply Theorem 1 by Theorem 2 so long as we guarantee the conditions stated in Definition 3 are satisfied.

> **Assumption 1.** *The measurements and subsequent announcement structure of Alice and Bob guarantee that the partitioned data $\widetilde{A}_i$'s and $\widetilde{B}_i$'s are weakly dependent (Definition 3).*

Example (optical discrete-variable protocols): The generalization from independently seeded announcements to weakly dependent announcements is crucial in the case of discrete-variable protocols. In those protocols, we typically perform postselection in the case of loss to remove the no-detection events from the raw data. However, postselection implies that each party needs to publicly announce if they have a detection or not (in addition to announcing the basis choice for protocols like BB84). This announcement is potentially problematic because the detection probability depends on the state; i.e., states with more photons have a higher probability of being detected. However, we can use the fact that the measurements by single-photon detectors commute with the total photon number operators N. In other words, Alice's

(or Bob's) optical space can be decomposed in subspaces, each of which has a given total photon number n_a (or n_b), as $Q_A = \oplus_{n_a=0}^{\infty} V_A^{n_a}$ (or $Q_B = \oplus_{n_b=0}^{\infty} V_B^{n_b}$), and the measurement device's POVM elements are block diagonal along the subspaces $V_A^{n_a}$ (or $V_B^{n_b}$).

Let's take BB84 as an example. Assuming that the basis choice is independently seeded, we only need to verify that the probability of a detection is the same for all states with the given basis choice x and the same total photon number $N_A = n_a$. That is, for each total photon number n_a and basis choice x, there exists some constant c_{x,n_a} such that the probability of detection conditioned on sending a state from the basis x in the subspace $V_A^{n_a}$ is

$$\Pr(\text{detection } |x, \rho_{n_a}) = c_{x,n_a}, \text{ for all } \rho_{n_a} \in \mathrm{D}(V_A^{n_a}). \tag{19}$$

Likewise, we have a similar requirement for Bob's detectors. This requirement needs to hold for both Alice's and Bob's detectors.

We remark that this property holds for the BB84 passive-detection setup using identical (imperfect) single-photon detectors (See Section 7.4).

Remark 3. As mentioned in the introduction, [25] uses the generalised EAT [24] to establish security for prepare-and-measure protocols by assuming the protocol only has one signal in the physical channel at at time, i.e. is truly a sequential protocol. The assumption in [25] is so that they can satisfy the 'no-signalling' condition for the generalised EAT. In [24] it is shown how the original EAT's Markov chain conditions imply the 'no-signalling' condition. Thus, the set of protocols we consider here all can also be covered by the generalised EAT too. However, as explained in [25], the only advantage of the generalised EAT for device-dependent QKD is to apply to prepare-and-measure protocols, which requires the truly sequential assumption, which then does not include most of the protocols considered in Protocol 1. That is to say, our class of entanglement-based protocols can be analysed by the generalised EAT, but this does not seem to provide an advantage over the original EAT, and if one considers prepare-and-measure protocols, our class of protocols is too general to be addressed by the generalised EAT.

4.2.1 Completeness of a QKD Protocol

A protocol that generates a secret key but always aborts on the honest implementation is not practically useful. Completeness measures the probability the protocol will not abort on the honest implementation.[8]

Definition 4. *A QKD protocol is called ε_{QKD}^C-complete if the probability of aborting the entire protocol is at most ε_{QKD}^C. Similarly, any subprotocol P is ε_P^C-complete if that subprotocol aborts with probability at most ε_P^C.*

Clearly one may bound the QKD protocol's completeness $\varepsilon_{\mathrm{QKD}}^{\mathrm{C}}$ via the union bound of the completeness of each subprotocol as has been done previously, e.g. [39]. The completeness of error correction is a function of the specific implementation, so we omit a discussion on this. Therefore, the major concern is the completeness of parameter estimation. It is both intuitive and well-known that as the set of accepted statistics increases, the probability of aborting the protocol can only decrease for any input, but the key length is likely to also decrease. We provide simple bounds for completeness that are relevant for any protocol that satisfies Protocol 2.

Proposition 3. Following the notation of Protocol 2, let $\sigma = \mathcal{E}(\rho)$ be the state after the honest preparation, ρ, and (possibly noisy) transmission channel $\mathcal{E}$, which we assume to be

---

[8]This has also been referred to as robustness [13].

memoryless between transmissions. Let p be the probability distribution of joint outcomes of Alice and Bob's measurements on σ in testing rounds. Let the set of accepted statistics be $\mathcal{Q} := \{f \in \mathbb{P}(\mathcal{X}) : \|p - f\|_1 \leq \xi_t\}$ where $\xi_t \in (0, 1]$. Then the completeness of the parameter estimation subprotocol when $\varepsilon_{\mathrm{PE}}^{\mathrm{C}}$ satisfies the upper bound

$$\varepsilon_{\mathrm{PE}}^{\mathrm{C}} \leq 2\exp\left(-2m'(\gamma - \gamma')^2\right) + \exp\left(-m'\left(\frac{t^2}{2\ln 2} - |\mathcal{X}|\frac{\log(m'+1)}{m'}\right)\right),$$

where $\gamma' < \gamma$ and $m' := \lfloor \gamma'n \rfloor$. Moreover, this goes to zero as n goes to infinity.

Proof. First, for any fixed number of tests m, the probability of aborting, $\varepsilon_{\mathrm{PE\!-\!m}}^{\mathrm{C}}$, is bounded as

$$\varepsilon_{\mathrm{PE\!-\!m}}^{\mathrm{C}} \leq \min\left\{1, \exp\left(-m\left(\frac{t^2}{2\ln 2} - |\mathcal{X}|\frac{\log(m+1)}{m}\right)\right)\right\},$$

which is a straightforward implication of Pinsker's inequality [40, Lemma 11.6.1] and the law of large numbers via method of types [40, Theorem 11.2.1] as noted in [41]. Then we have

$$\begin{aligned}
\varepsilon_{\mathrm{PE}}^{C} &= \sum_{k' \in [n]} \Pr[k' \text{ test rounds}]\varepsilon_{\mathrm{PE}|k'}^{\mathrm{C}} \\
&\leq \Pr[\# \text{ of test rounds} < m'] + \varepsilon_{\mathrm{PE}|m'}^{\mathrm{C}} \\
&\leq \Pr[\text{fraction of rounds that are tests} \geq \gamma - \gamma'] + \varepsilon_{\mathrm{PE}|\lfloor\gamma'n\rfloor}^{\mathrm{C}} \\
&\leq 2\exp\left(-2\lfloor\gamma'n\rfloor(\gamma - \gamma')^2\right) + \varepsilon_{\mathrm{PE}|\lfloor\gamma'n\rfloor}^{\mathrm{C}},
\end{aligned}$$

where the first inequality is choosing to group the probabilities by some m', the second is using $m' := \gamma'n$ for some $\gamma' < \gamma$, and the final equality Hoeffding's inequality for independent Bernoulli random variables. $\qed$

5 Security of Device-Dependent QKD from EAT

In this section we present the security of the considered QKD protocols (Protocol 1). We stress that our security proof is for coherent attacks. Recall Protocol 1 does not assume anything about the state distribution but guarantees announcements are after all measurements. It is therefore equivalent to Protocol 2 where $\rho_{Q_1^n E}$ is an arbitrary state and announcements are made round-by-round. Recall that for an i.i.d. collective attack,[9] one would assume $\rho_{Q_1^n E} = \sigma_{QR}^{\otimes n}$ so that Eve sends n copies of the state σ_Q for which she holds a purification σ_{QR} to Alice and Bob. However, we do not make this assumption here in the security proof.

5.1 Entropy rate of EAT process

As discussed previously, we aim to apply the EAT to analyze the virtual QKD protocol (Protocol 2) which is equivalent to the physical QKD protocol (Protocol 1) in terms of security.

---

[9]Collective attacks are usually defined (e.g. [3]) by assuming that Eve interacts with each signal with a new ancillary state using the same unitary operation (which also includes mixed-unitary channels). Under this definition, collective attacks and i.i.d. assumption can be treated as synonymous for many protocols (as long as the protocol structure allows for the i.i.d. behavior). Some authors seem to generalize the definition to allow time-dependent unitary operations to include, for example, channels with a slowly rotating reference frame. This generalized definition would be non-i.i.d. collective attacks. For this reason, we use the terminology of i.i.d. collective attacks to emphasize the i.i.d. assumption.

However, we cannot directly use the EAT to analyze the virtual protocol. Specifically, the QKD protocol only accumulates entropy[10] until parameter estimation. As such, our interest is in the entropy accumulated given some event passes, namely that parameter estimation passes. Therefore, the security proof is broken into two parts. First, one proves the entropy accumulation rate on a 'subprotocol' that is nearly (for technical reasons) equivalent to that of Steps 0 to 7 of Protocol 2. After this, one proves the security of the virtual protocol by relating it back to the subprotocol. In this subsection, we present the EAT subprotocol (Protocol 3) and its entropy accumulation rate. Then in the next subsection we present the secure key length of the QKD protocol (Theorem 5). A similar proof for a device-independent QKD protocol was given in [18]. However, that proof relied on a particular structure of the protocol which simplifies the analysis but is not as general as the protocol we consider here. In particular, the parameter estimation was done on the error corrected bit string instead of on the raw measurement results, like we do here. This allows us to use all the available measurement information to bound the key rate.

Protocol 3 Device-Dependent Entropy Accumulation Subprotocol

Inputs: Same as Protocol 2
Protocol: Run Steps 0 to 7 of Protocol 2, except in Steps 4 and 6, Bob assigns $\overline{B}_i = \perp$ (i.e. if $T_i = 0$, then $\overline{B}_i = \perp$), and in Step 6 Alice *does not* announce $\overline{A}_i$ when $T_i = 1$. Regardless, $X_i = t(\overline{A}_i, \overline{B}_i, \widetilde{A}_i, \widetilde{B}_i)$ can be calculated the same as before.

It is worth noting that in principle the EAT does not rely on knowing all of the steps of the protocol explicitly. It just requires the existence of EAT channels that output (quantum) random variables that are the same as the real process. This is why we are not concerned about X_i being computed locally. Here we described the procedure per round largely the same as in Protocol 2, because when we use our numerical algorithms to construct the min-tradeoff function (Section 6), we use our knowledge of a way to implement the process to construct the EAT channels explicitly. We also note for this reason, this protocol can handle QKD protocols in which one party's public announcement is conditioned upon the other, so long as one can prove the resulting output random variables still satisfy the required Markov conditions.

With the protocol defined, we may use the EAT to bound the entropy accumulated. We first state the relabeling from the registers used in the EAT statement in Section 3 and ones used in Protocol 3:

$$S_i \leftrightarrow \overline{A}_i \overline{B}_i$$
$$P_i \leftrightarrow \widetilde{A}_i \widetilde{B}_i T_i$$
$$X_i \leftrightarrow X_i$$
$$Q_i \leftrightarrow A_i B_i$$
$$R_i \leftrightarrow R_i$$
$$E \leftrightarrow E \ .$$

With these conversions, we state the sandwiched Rényi entropy rate of the entropy accumulation subprotocol (Protocol 3).

Theorem 4. *Consider the entropy accumulation protocol defined in Protocol 3 and assume the Assumption 1 is satisfied. Let $\Omega = \{x_1^n \in \mathcal{X}^n : \mathsf{freq}(x_1^n) \in \mathcal{Q}\}$ and ρ be the output of the*

---

[10]In the main text we consider the sandwiched Rényi entropy. In Section D we consider smooth min-entropy. In both cases the main point is that some entropic quantity accumulates, so we just use entropy without a qualifier to refer to both cases.

protocol. Let h such that $f(\boldsymbol{q}) \geq h$ for all $\boldsymbol{q} \in \mathcal{Q}$ where f is the min-tradeoff function generated by either Algorithm 1 or Algorithm 2. Then for any $\varepsilon_{\mathrm{EA}} \in (0, 1)$, either the protocol aborts with probability greater than $1 - \varepsilon_{\mathrm{EA}}$, or

$$H_\beta^\uparrow(\overline{A}_1^n \overline{B}_1^n | \widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega}} > nh - n\frac{(\beta-1)\ln 2}{2}V^2 - \frac{\beta}{\beta-1}\log\frac{1}{\varepsilon_{\mathrm{EA}}} - n(\beta-1)^2 K_\beta \qquad (20)$$

where $\beta \in (1, 2)$ by Theorem 1.

Proof. We simply check that everything we have done satisfies the requirements of EAT.

1. As we assume the protocol satisfies Assumption 1 which implies that Theorem 2 holds for the protocol, the output state ρ satisfies the Markov conditions in Eq. (8).

2. By our definition of how we compute the test register X_i, the testing map $\mathcal{T}_i$ is of the form in Eq. (6) of Definition 1.

3. By our construction of the min-tradeoff function (Algorithm 1 or Algorithm 2), we have a min-tradeoff function and the value h in the statement of the theorem above satisfies the requirements to be h in the statement of Theorem 1.

Thus we have satisfied the requirements of the EAT and can apply it. $\qquad\square$

Remark 4. The statement of Theorem 4 requires that either the EAT protocol aborts with a probability greater than $1 - \varepsilon_{\mathrm{EA}}$ or else the entropy bound holds. In the language of Renner's PhD thesis [13], this theorem says either ρ is $\varepsilon_{\mathrm{EA}}$-securely filtered by the EAT protocol or the entropy bound holds. This explains the replacement of the failure probability of parameter estimation, which appeared in Renner's original coherent-attack security proofs [13], with the term $\varepsilon_{\mathrm{EA}}$ in the statement of ε-security.

5.2 Security of QKD protocol

We can now present the key length for a QKD protocol using the EAT without introducing any smoothing. We note this depends on the construction of a max-tradeoff entropy accumulation theorem for the sandwiched Rényi entropy $H_\delta^\uparrow$, which we provide in Section B.

Theorem 5. *Consider any QKD protocol which follows Protocol 1 and satisfies Assumption 1. Let $\varepsilon_{\mathrm{sec}}, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{acc}} \in (0, 1]$ such that $\varepsilon_{\mathrm{acc}} \geq \varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{EC}}$. Let h such that $f(\boldsymbol{q}) \geq h$ for all $\boldsymbol{q} \in \mathcal{Q}$ where f is the min-tradeoff function generated by Algorithm 1 or Algorithm 2.*

Let $\beta \in (1, 2)$, $\delta \in (1/2, 1)$ and $\alpha = \frac{-\beta+\delta}{-1+2\delta-\beta\delta}$. The QKD protocol is $\varepsilon_{\mathrm{acc}}$-secure for key length

$$\begin{aligned}
\ell \leq &nh - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} - n\frac{(\beta-1)\ln 2}{2}V^2 - n(\beta-1)^2 K_\beta - n\gamma\log|\mathcal{A}\times\mathcal{B}| \\
&+ \frac{\beta-\delta}{(\beta+1)(1-\delta)}\log(\varepsilon_{\mathrm{acc}}) + \frac{\alpha}{\alpha-1}\log(\varepsilon_{\mathrm{sec}}) + 1
\end{aligned} \qquad (21)$$

where

$$V = \sqrt{\mathrm{Var}(f) + 2} + \log\left(2d_S^2 + 1\right)$$

$$K_\beta = \frac{1}{6(2-\beta)^3 \ln 2} 2^{(\beta-1)(\log d_S + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))} \ln^3\left(2^{\log d_S + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2\right)$$

where $\mathcal{A}$ and $\mathcal{B}$ are the alphabets of private outcomes for Alice's and Bob's announcements excluding the symbol $\perp$, respectively, $d_S = (|\mathcal{A}|+1)(|\mathcal{B}|+1)$, $\mathrm{leak}_{\varepsilon_{\mathrm{EC}}}$ is the amount of information leakage during the error correction step.

Proof. See Section B. □

Remark 5. In the proof of Theorem 5 in Section B there is another parameter, η, to optimize over. At the end of the proof, we make a natural choice for this parameter. As a result, the parameter η is not stated in the above theorem.

Remark 6. While not necessary, it seems natural to set $\varepsilon_{\mathrm{acc}} = \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{sec}}$. As shown in the proof of Theorem 5, the optimal choice of security parameters will always have $\varepsilon_{\mathrm{acc}} \geq \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{sec}}$. In principle, one has no control over the input states, so it is necessary to prove the security for many states, which would require $\varepsilon_{\mathrm{acc}}$ to be small. The scaling term of $\log(\varepsilon_{\mathrm{acc}})$ in the theorem is small unless (β, δ) is near $(2, 1)$, which is clearly suboptimal as the V and K_β correction terms increase linearly and exponentially in β respectively. Moreover, δ is effectively free as $\alpha \in [1, 1.5]$ always. As such, it is reasonable to set $\varepsilon_{\mathrm{acc}} = \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{sec}}$ as this results in the strongest security claim without changing $\varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{sec}}$ and, one would expect, obtains similar key rates assuming $\varepsilon_{\mathrm{acc}}, \varepsilon_{\mathrm{sec}}, \varepsilon_{\mathrm{EC}}$ were not originally significantly different orders.

Remark 7. As noted in Section 3, by specific choice of parameters in using the EAT, the resulting bound on the entropy can scale as $nh - O(\sqrt{n})$. As such, with suitable choices of β and δ, Theorem 5 gives the the key length that scales as $\ell(n) \leq nh - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} - O(\sqrt{n})$. If the min-tradeoff function is chosen appropriately, the key rate will reach the asymptotic key rate in the infinite-key limit.

5.2.1 Fixed number of test rounds

We have just proven the security of Protocol 1 by proving the security of Protocol 2 with the help of entropy accumulation subprotocol (Protocol 3). However, traditionally device-dependent QKD protocols use fixed-length testing instead of probabilistic round-by-round testing. This leaves us with two options. First, the device-dependent QKD protocol could be altered to do the parameter estimation round by round as is described in Protocol 2. In this case, one can use the result of Theorem 5 directly. However, if one wishes to use Theorem 5 and apply it to QKD protocols with fixed-length testing, one must connect the failure probability of Protocol 2 to the failure probability of the device-dependent QKD protocol actually implemented. Here we state the relation between the two failure probabilities in the case that T_i is an independent Bernoulli random variable (e.g. determined by seeded randomness). This can then be used to calculate secure key length using Theorem 5 for protocols with fixed-length testing as explained beneath the following theorem. In Section C, we present the derivation of this result. We note that, given the proof method, this result is exact rather than a bound.

Theorem 6. *Let $\rho_{Q_1^n E}^{in} \in \mathrm{D}(Q_1^n E)$ be the input to the protocol. Let ρ^{out} denote the output of Protocol 1 but with fixed-length parameter estimation on the input state $\rho_{Q_1^n E}^{in}$. Let ρ_{EAT}^{out} denote the output of the EAT protocol where for each round the probability of testing is γ. Let Ω be the event of not aborting on parameter estimation, which to be the same in both protocols, can only accept when there are m tests. Then $\rho_{EAT}^{out}[\Omega] = 2^{-nh(\gamma)}\binom{n}{m}\rho^{out}[\Omega]$. Furthermore, $\rho_{|\Omega}^{out} = \rho_{EAT|\Omega}^{out}$. (See Section 2.1 to recall notation.)*

Proof. See Section C. □

In proving security, one wishes to consider the set of inputs ρ^{in} which will be accepted except with probability ε in the testing. In EAT this probability is $\varepsilon_{\mathrm{EA}}$ and in fixed-length testing we will say this is $\varepsilon_{\mathrm{PE}}$. That is, one would like to consider the set of ρ^{in} such that $\rho^{out}[\Omega] \geq \varepsilon_{\mathrm{EA}}$ (resp. $\varepsilon_{\mathrm{PE}}$). The above theorem tells us how the set of ρ^{in} that satisfy these conditions changes when going between the considered fixed-length setting and probabilistic round-by-round testing. In other words, if one wishes to consider a protocol with a fixed-length testing that considers all input states that are not $\varepsilon_{\mathrm{PE}}$-filtered, it suffices to calculate the secure key length of the EAT with $\varepsilon_{\mathrm{EA}} = 2^{-nh(\gamma)}\binom{n}{m}\varepsilon_{\mathrm{PE}}$. As Theorem 6 is tight, this completely closes the gap in this setting. Note, however, that this approach does make the second-order term in Theorem 5 scale closer to that of the first-order term. That is, considering that $\log(\bar{\varepsilon}\rho[\Omega])$ is replaced with $\log(\bar{\varepsilon}\varepsilon_{\mathrm{EA}})$ in applying Theorem 1 for Theorem 4, we see $\log(\bar{\varepsilon}\rho^{out}_{EAT}[\Omega]) \geq \log(\bar{\varepsilon}\varepsilon_{\mathrm{PE}}) + \log\left(\frac{e^2}{\sqrt{2\pi}}\sqrt{\gamma(1-\gamma)n}\right)$, as is shown in Section C.[11] This means that the correction term scales as $O(\sqrt{n}\log(\sqrt{n}))$ rather than $O(\sqrt{n})$, which may suggest this is not the ideal way to merge fixed-length testing and the ideas from EAT.

6 Construction of (Near-)Optimal Min-Tradeoff Functions

The QKD key rates obtained by the EAT method crucially depend on the choice of min-tradeoff function. For any given block size, it is desirable to choose the min-tradeoff function that maximizes the key rate among all valid min-tradeoff functions. In the infinite-key limit, we would like to choose a min-tradeoff function such that the key rate obtained by the EAT method reproduces the expected asymptotic key rate. We also would like to make our method as general as possible so that it can be applied to a large family of protocols. Our framework can be used whenever the EAT maps have the specific tensor product form as explained in Section 3.2. Our first approach is to use the numerical framework for asymptotic QKD rate calculation [28] to construct min-tradeoff functions (via a similar two-step procedure). As will be explained in depth later, the important observation here is that the dual problem of the linearization of the original optimization problem gives us the desired min-tradeoff functions. The linearization is a semidefinite program (SDP) and thus its dual problem can be efficiently solved. This method is conceptually simple and can give us a family of valid min-tradeoff functions. We then optimize the choice of min-tradeoff functions when we evaluate the key rate in the finite-key regime using this algorithm. On the other hand, the generation of each individual min-tradeoff function by this approach takes into account only the first-order information in the key rate expression. It is typically the case that the min-tradeoff function that gives the highest first-order term does not give the optimal finite-key rate when lower-order terms are included. This motivates us to derive the second algorithm that also considers the second-order terms. With the aid of Fenchel duality, we show that the second algorithm can also be written in terms of convex optimization.

As a starting point, we review the asymptotic key rate optimization formulation in [28]. We present our first algorithm that utilizes the essential idea of [28] in Section 6.2 and then discuss the second algorithm in Section 6.3.

---

[11]One may verify this is the appropriate direction of bound as we are interested in the δ term of Theorem 5, and if $y \geq x$, then $n\beta - \sqrt{1-z-y} \geq n\beta - \sqrt{1-z-x}$, so the bound on the key length has only decreased.

6.1 Review of asymptotic key rate optimization

To construct min-tradeoff functions, we establish the intimate relation that exists between the problem of generating a good min-tradeoff function for a given protocol and the problem of computing asymptotic key rates in QKD. It is shown [28, 42] that the latter problem can be rewritten as a convex optimization problem. The main idea is that, given a map $\widetilde{\mathcal{M}}_i : Q_i \to S_i P_i X_i$ (from an input quantum system to the key, public announcement and testing registers), the function $r_\infty(\boldsymbol{q})$ gives the worst-case conditional entropy compatible with the given statistics $\boldsymbol{q}$. Explicitly, it is the result of the following convex optimization problem:

$$r_\infty(\boldsymbol{q}) = \underset{\rho_{QR}}{\text{minimize}} \quad W(\rho_{QR})$$
$$\text{subject to} \ \ \text{Tr}[\rho_Q M_x] = \boldsymbol{q}(x) \tag{22}$$
$$\rho_{QR} \geq 0$$

where the objective function

$$W(\rho_{QR}) := H(S_i|P_iR)_{\widetilde{\mathcal{M}}_i \otimes \mathcal{I}_R(\rho_{QR})} \tag{23}$$

is defined as the conditional entropy of the state obtained by applying the map $\widetilde{\mathcal{M}}_i \otimes \mathcal{I}_R$ to the state ρ_{QR} which is a purification of ρ_Q, and the constraints come from the POVM elements $M_x := \sum_{s,p:t(s,p)=x} M_{sp}$ associated to the map $\text{Tr}_{S_iP_i} \circ \widetilde{\mathcal{M}}_i$. Here we use register R to refer to Eve's register in a single round as depicted in Figure 1. The objective function can be written in terms of these POVM elements and without needing to optimize over the R register directly as Proposition 1 shows.

Proposition 1. *Let $\{M_{sp} : s,p\}$ be Alice and Bob's joint POVM which is regrouped according to the public information p and the value of the final key s. Let $M_p = \sum_s M_{sp}$. Then for $\rho \in \text{D}(Q)$,*

$$W(\rho_{QR}) = \sum_{s,p} H\left(\mathcal{K}_{sp}(\rho_Q)\right) - \sum_p H\left(\mathcal{K}_p(\rho_Q)\right) \tag{24}$$

where $\mathcal{K}_{sp}(\rho) := K_{sp}\rho K_{sp}^\dagger$ with $K_{sp} = \sqrt{M_{sp}}$, and $\mathcal{K}_p(\rho) := K_p\rho K_p^\dagger$ with $K_p = \sqrt{M_p}$. We note the subscripts highlight that the optimization does not depend on the R register.

Proof. See Section E. □

To solve the convex optimization problem in Eq. (22), numerical algorithms typically require the gradient information of the objective function. The gradient of W for $\rho > 0$ is given as

$$\nabla W(\rho) = -\sum_{s,p} \mathcal{K}_{sp}^\dagger\left(\log \mathcal{K}_{sp}(\rho)\right) + \sum_p \mathcal{K}_p^\dagger\left(\log \mathcal{K}_p(\rho)\right), \tag{25}$$

where $\mathcal{K}_{sp}^\dagger$ denotes the adjoint map of $\mathcal{K}_{sp}$ and can be written as $\mathcal{K}_{sp}^\dagger(\rho) := K_{sp}^\dagger\rho K_{sp}$. Similarly, $\mathcal{K}_p^\dagger$ is the adjoint map of $\mathcal{K}_p$. When ρ is singular, this gradient is not well-defined. We can use the same perturbation technique used in [28] for the quantum relative entropy formulation to define the gradient for every $\rho \geq 0$. In particular, we denote the depolarizing channel with a depolarizing probability p by $\mathcal{D}_p$, which is defined as

$$\mathcal{D}_p(\rho) = (1-p)\rho + p\,\text{Tr}(\rho)\frac{\mathbb{1}}{d}, \tag{26}$$

where d is the dimension of the Hilbert space relevant for ρ. We denote the perturbed version of the objective function as $W_\epsilon(\rho)$ with a perturbation ϵ, which is defined as

$$W_\epsilon(\rho) = \sum_{s,p} H\left(\mathcal{K}_{sp}^\epsilon(\rho)\right) - \sum_p H\left(\mathcal{K}_p^\epsilon(\rho)\right), \tag{27}$$

where $\mathcal{K}_{sp}^\epsilon = \mathcal{D}_\epsilon \circ \mathcal{K}_{sp}$ and $\mathcal{K}_p^\epsilon = \mathcal{D}_\epsilon \circ \mathcal{K}_p$. In Section E, we also discuss the continuity of our objective function under this small perturbation. In particular, we have

$$|W(\rho) - W_\epsilon(\rho)| \le \eta_\epsilon \quad \text{with} \quad \eta_\epsilon = (|S|+1)|P|\epsilon(d-1)\log\frac{d}{\epsilon(d-1)}, \tag{28}$$

where $|S|$ and $|P|$ denote the size of alphabets for S_i and P_i, respectively.

6.2 An algorithm derived from the asymptotic numerical optimization

Algorithm 1 for finding a min-tradeoff function has the same spirit as the algorithm for finding the asymptotic key rate in Ref. [28]. We prove it provides a valid min-tradeoff function in Proposition 2. In Proposition 3, we show that each construction of min-tradeoff function gives us tight asymptotic key rate for the observed statistics $\boldsymbol{q}_0$ that we use in the construction.

Algorithm 1 Algorithm for constructing the min-tradeoff functions based on the asymptotic key rate method

---

Inputs:

$\boldsymbol{q}_0$ A given probability distribution in $\mathbb{P}(\mathcal{X})$
$\{M_x : x \in \mathcal{X}\}$ Bipartite POVM used for testing

Output:

   $\boldsymbol{y}^\star$ A vector in $\mathbb{R}^{|\mathcal{X}|}$ which defines a min-tradeoff function by $f_\epsilon(\boldsymbol{q}) := \langle \boldsymbol{q}, \boldsymbol{y}^\star \rangle - \eta_\epsilon$.

Algorithm:

1. Consider the convex optimization $r_\epsilon(\boldsymbol{q}_0) := \min_{\rho \in \Sigma_i(\boldsymbol{q}_0)} W_\epsilon(\rho)$ with the true optimal solution ρ^{opt}. Solve the optimization (e.g. by Frank-Wolfe algorithm) and obtain a near-optimal solution $\rho_\epsilon^\star$ with the perturbation error $\epsilon \in (0, 1/(e(d-1))]$ determined by the algorithm.

2. Let $W_\epsilon^{\text{lin}}(\rho) := W_\epsilon(\rho_\epsilon^\star) + \text{Tr}[\nabla W_\epsilon(\rho_\epsilon^\star) \cdot (\rho - \rho_\epsilon^\star)]$ be the linearization of the function W_ϵ at the point $\rho_\epsilon^\star$. It can be equivalently written as

$$W_\epsilon^{\text{lin}}(\rho) = \text{Tr}[O_\epsilon \rho] \quad \text{with} \quad O_\epsilon := \left(W_\epsilon(\rho_\epsilon^\star) - \text{Tr}\left[\nabla W_\epsilon(\rho_\epsilon^\star) \cdot \rho_\epsilon^\star\right]\right)\mathbb{1} + \nabla W_\epsilon(\rho_\epsilon^\star). \tag{29}$$

Since $W_\epsilon(\rho)$ is a convex function in ρ, we know that $W_\epsilon^{\text{lin}}(\rho) \le W_\epsilon(\rho), \forall \rho$, and $W_\epsilon^{\text{lin}}(\rho_\epsilon^\star) = W_\epsilon(\rho_\epsilon^\star)$.

3. Consider the SDP $\min_{\rho \in \Sigma_i(\boldsymbol{q}_0)} W_\epsilon^{\text{lin}}(\rho)$ whose dual SDP is given by

$$\max_{y} \langle \boldsymbol{q}_0, \boldsymbol{y} \rangle \quad \text{subject to} \quad \sum_{x \in \mathcal{X}} \boldsymbol{y}(x) M_x \le O_\epsilon, \; \boldsymbol{y} \in \mathbb{R}^{|\mathcal{X}|}. \tag{30}$$

Solve the dual program and obtain an optimal solution $\boldsymbol{y}^\star$.

4. Construct the min-tradeoff function by $f_\epsilon(\boldsymbol{q}) := \langle \boldsymbol{q}, \boldsymbol{y}^\star \rangle - \eta_\epsilon$.

Remark 8. Note that the first term of O_ϵ in Eq. (29) always vanishes, i.e., $W_\epsilon(\rho_\epsilon^\star) - \text{Tr}\left[\nabla W_\epsilon(\rho_\epsilon^\star) \cdot \rho_\epsilon^\star\right] = 0$ for any $\rho_\epsilon^\star$. This can be shown by expanding the definitions.

Remark 9 (Strong duality for SDP in Eq. (30)). Let $\lambda_{\min}$ be the smallest eigenvalue of O_ϵ. It follows that $(\lambda_{\min} - 1)\mathbb{1} < O_\epsilon$. Since $\sum_x M_x = \mathbb{1}$, $(\lambda_{\min} - 1, \lambda_{\min} - 1, \cdots, \lambda_{\min} - 1)$ is a strictly feasible solution for Eq. (30). As long as $\Sigma_i(\boldsymbol{q}_0)$ is non-empty, the Slater's condition is satisfied [43, Theorem 1.18]. Thus, the strong duality holds for the SDP in Eq. (30). This means that the dual problem in Eq. (30) gives the same optimal value as the primal problem which is $\min_{\rho \in \Sigma_i(\boldsymbol{q}_0)} W_\epsilon^{\text{lin}}(\rho)$.

Remark 10. Note that the min-tradeoff function constructed by Algorithm 1 depends on the input choice of $\boldsymbol{q}_0 \in \mathbb{P}(\mathcal{X})$. In the end we need to optimize over $\boldsymbol{q}_0$ to get the best key rate (similar to [18, Eq. (32)]).

In the following we show that the function constructed in Algorithm 1 is indeed a valid min-tradeoff function.

Proposition 2 (Correctness). *Let $\epsilon \in (0, 1/(e(d'-1))]$ and assume that $\sum_i \boldsymbol{y}^\star(i)\Gamma_i \leq O_\epsilon$ is satisfied. Then f_ϵ constructed from Algorithm 1 is a valid min-tradeoff function.*

Proof. To check whether f_ϵ is a valid min-tradeoff function, according to Definition 2, one needs to check that f_ϵ is an affine function and it satisfies Eq. (9). It is clear that f_ϵ is a real-valued affine function by construction. It remains to check Eq. (9). For any $\boldsymbol{q} \in \mathbb{P}(\mathcal{X})$ and any $\rho \in \Sigma_i(\boldsymbol{q})$, it holds

$$f_\epsilon(\boldsymbol{q}) = \langle \boldsymbol{q}, \boldsymbol{y}^\star \rangle - \eta_\epsilon = \sum_i \boldsymbol{y}^\star(i)\boldsymbol{q}(i) - \eta_\epsilon \tag{31}$$

$$= \sum_i \boldsymbol{y}^\star(i)\,\text{Tr}[\rho\Gamma_i] - \eta_\epsilon \tag{32}$$

$$= \text{Tr}\left[\left(\sum_i \boldsymbol{y}^\star(i)\Gamma_i\right)\rho\right] - \eta_\epsilon \tag{33}$$

$$\leq \text{Tr}[O_\epsilon \rho] - \eta_\epsilon \tag{34}$$

$$= W_\epsilon^{\text{lin}}(\rho) - \eta_\epsilon \tag{35}$$

$$\leq W_\epsilon(\rho) - \eta_\epsilon \tag{36}$$

$$\leq W(\rho), \tag{37}$$

where the second line follows by the assumption that $\rho \in \Sigma_i(\boldsymbol{q})$, the third line follows by the linearity of trace, the fourth line follows by the assumption that $\boldsymbol{y}^\star$ satisfying the constraint $\sum_i \boldsymbol{y}^\star(i)\Gamma_i \leq O_\epsilon$, the fifth line follows by definition of W_ϵ^{lin}, the sixth line follows as W is a convex function and W_ϵ^{lin} is a linearization of W, and the last line follows by the continuity bound in Eq. (28). Minimizing over all $\rho \in \Sigma_i(\boldsymbol{q})$, we have

$$f_\epsilon(\boldsymbol{q}) \leq r(\boldsymbol{q}) := \min_{\rho \in \Sigma_i(\boldsymbol{q})} W(\rho). \tag{38}$$

As this holds for any $\boldsymbol{q} \in \mathbb{P}(\mathcal{X})$, we conclude that f_ϵ is a valid min-tradeoff function. $\qquad\square$

Proposition 3 (Tightness). *Let $\epsilon \in (0, 1/(e(d'-1))]$ and assume that $\Sigma_i(\boldsymbol{q}_0)$ is non-empty and the first step of Algorithm 1 is solved exactly, i.e., $\rho_\epsilon^\star = \rho^{\text{opt}}$. Then $\lim_{\epsilon \to 0^+} f_\epsilon(\boldsymbol{q}_0) = r(\boldsymbol{q}_0)$.*

Proof. Since $\rho_\epsilon^\star$ is the minimizer of W_ϵ over the convex set $\Sigma_i(\boldsymbol{q}_0)$, by [28, Lemma 2 and Eq. (86), equivalently Eq. (95)], we know that $\min_{\rho \in \Sigma_i(\boldsymbol{q}_0)} \text{Tr}[\nabla W_\epsilon(\rho_\epsilon^\star) \cdot (\rho - \rho_\epsilon^\star)] = 0$. Thus $\min_{\rho \in \Sigma_i(\boldsymbol{q}_0)} W_\epsilon^{\text{lin}}(\rho) = W_\epsilon(\rho_\epsilon^\star) = r_\epsilon(\boldsymbol{q}_0)$. Moreover, since $\Sigma_i(\boldsymbol{q}_0)$ is non-empty, by Remark 9 the strong duality of Eq. (30) holds. Then we have $f_\epsilon(\boldsymbol{q}_0) + \eta_\epsilon = \langle \boldsymbol{q}_0, \boldsymbol{y}^\star \rangle = \min_{\rho \in \Sigma_i(\boldsymbol{q}_0)} W_\epsilon^{\text{lin}}(\rho) = r_\epsilon(\boldsymbol{q}_0)$. This implies $\lim_{\epsilon \to 0^+} f_\epsilon(\boldsymbol{q}_0) = \lim_{\epsilon \to 0^+} r_\epsilon(\boldsymbol{q}_0) = r(\boldsymbol{q}_0)$. $\square$

6.3 An alternative algorithm that uses second-order information

To apply Algorithm 1 in the finite-key rate calculation, we need to optimize the choice of min-tradeoff functions by heuristically picking different starting points. As such, while the previous algorithm will reproduce the asymptotic key rate in the infinite-key limit, it may behave poorly in the small block-size regime if the optimization over the starting point $\boldsymbol{q}_0$ is not done properly. This limitation motivates us to design a new algorithm that considers the effect of the choice of min-tradeoff function on second-order correction terms when constructing the min-tradeoff function. While ideally we would look at the key length expression in Theorem 5 and collect all terms that depend on the choice of min-tradeoff function f for our new objective function, this would involve an additional optimization over the choices of β and δ. This is because the terms V and K_β depend on both the min-tradeoff function f and the choice of β, and there are constant terms that depend on both β and δ. In principle, one could optimize the min-tradeoff function f and two parameters β and δ simultaneously to obtain the best possible key rate. However, because such a joint optimization is challenging, we choose to consider a simpler scenario that we now explain.

As we will claim the Rényi entropy key length obtains better key lengths than the smooth min-entropy key length, we build an algorithm that should behave best for the smooth min-entropy key length, Theorem 15 [see Eq. (109)], which already has one fewer free parameters than in Theorem 5. To simplify further, we follow [17] in fixing a specific choice of α that leads to a simplified statement of the EAT [17, Theorem V.2, Eq. (28)]. Again using the fact that S_i is classical, and dividing relevant terms by the number of signals, n, we have the following candidate for the objective function to use to to generate a near-optimal min-tradeoff function:

$$\mathcal{L}(f) := f(\boldsymbol{q}_0) - \frac{1}{\sqrt{n}} c(f) - \frac{1}{n} c'(f), \tag{39}$$

where $c(f)$ and $c'(f)$ are defined as

$$c(f) = \sqrt{2\ln(2)}\Big[\log\Big(2d_S^2 + 1\Big) + \sqrt{2 + \text{Var}(f)}\Big]\sqrt{1 - 2\log(\bar{\varepsilon}\rho[\Omega])},$$

$$c'(f) = \frac{35[1 - 2\log(\bar{\varepsilon}\rho[\Omega])]}{[\log\big(2d_S^2 + 1\big) + \sqrt{2 + \text{Var}(f)}]^2} 2^{\log(d_S) + \text{Max}(f) - \text{Min}_\Sigma(f)} \ln^3\Big(2^{\log d_S + \text{Max}(f) - \text{Min}_\Sigma(f)} + e^2\Big). \tag{40}$$

For a general min-tradeoff function f, $\text{Var}(f)$ can be upper bounded by a function of $\text{Max}(f)$ and $\text{Min}(f)$ as

$$\text{Var}(f) \leq \frac{1}{4}[\text{Max}(f) - \text{Min}(f)]^2. \tag{41}$$

We note that in the application of EAT to security proofs of QKD protocols (see Theorem 15), one replaces $\rho[\Omega]$ by ε_{acc} and uses $\bar{\varepsilon}/4$ in the place of $\bar{\varepsilon}$. We also note while the term $c'(f)$ has a complicated dependence on the min-tradeoff function f, its contribution to the key rate is much smaller than the first two terms of Eq. (39) due to the $1/n$ dependence. Therefore, for simplicity of our method, we ignore the $c'(f)$ term in our objective function for the purpose of constructing min-tradeoff function. We make another simplification in the $c(f)$ term by dropping the term

related to $\log(2d_S^2 + 1)$ since it does not depend on the min-tradeoff function. With all these simplifications, we would like to consider the following objective function:

$$
\begin{aligned}
\tilde{\mathcal{L}}(f) &:= f(\boldsymbol{q}_0) - \frac{1}{\sqrt{n}}\sqrt{2\ln(2)}\sqrt{1 - 2\log(\varepsilon_{\mathrm{acc}}\bar{\varepsilon}/4)}\sqrt{2 + \frac{1}{4}[\mathsf{Max}(f) - \mathsf{Min}(f)]^2} \\
&= f(\boldsymbol{q}_0) - \frac{2}{\sqrt{n}}\sqrt{\ln(2)}\sqrt{1 - 2\log(\varepsilon_{\mathrm{acc}}\bar{\varepsilon}/4)}\sqrt{1 + \frac{1}{8}[\mathsf{Max}(f) - \mathsf{Min}(f)]^2}.
\end{aligned}
\tag{42}
$$

Since a min-tradeoff function f can be fully specified by a vector $\boldsymbol{f}$, it is the case that $\mathsf{Max}(f) = \max(\boldsymbol{f}) := \max_x \boldsymbol{f}(x)$ and similarly, $\mathsf{Min}(f) = \min(\boldsymbol{f}) := \min_x \boldsymbol{f}(x)$ (see Eq. (14) for definitions). This leads to the following optimization problem

$$
\begin{aligned}
&\underset{\boldsymbol{f}}{\text{maximize}} \quad \boldsymbol{f} \cdot \boldsymbol{q}_0 - c_0\sqrt{1 + c_1^2[\max(\boldsymbol{f}) - \min(\boldsymbol{f})]^2} \\
&\text{subject to} \quad \sum_x \boldsymbol{f}(x)\,\mathrm{Tr}(\rho M_x) \le W(\rho) \ \forall \rho \in \mathrm{D}(Q_i),
\end{aligned}
\tag{43}
$$

where c_0, c_1 are two constants to be set for generality, and $\{M_x\}$ is the POVM used for testing. In particular, the set of values, $c_0 = 2\sqrt{\ln 2}\sqrt{1 - 2\log(\varepsilon_{\mathrm{acc}}\bar{\varepsilon}/4)}/\sqrt{n}$, $c_1 = \frac{1}{2\sqrt{2}}$, correspond to the optimization of Eq. (42). We emphasize that in deriving this simplified expression, we have made a heuristic choice. As we will show later, any vector $\boldsymbol{f}$ returned by this optimization gives a valid min-tradeoff function. This means that our heuristic choice does not affect the correctness of a min-tradeoff function. However, it might give sub-optimal min-tradeoff functions that lead to looser key rates. We note that it is possible to make further improvements, particularly for optimizing the min-tradeoff function for Theorem 5.

The reason that we introduce two constants c_0 and c_1 is to make our algorithm general enough to allow the construction of crossover min-tradeoff function (which is defined later in Definition 6) as well as the normal min-tradeoff function in the statements of EAT. If our algorithm is used to find a crossover min-tradeoff function g, which can be used to reconstruct a min-tradeoff function f by Eqs. (52) and (53), then $\mathsf{Var}(f)$ is upper bounded by $\frac{1}{\gamma}[\mathsf{Max}(g) - \mathsf{Min}(g)]^2$ according to Eq. (57). Moreover, $g(\boldsymbol{q}') = f(\boldsymbol{q})$ for every $\boldsymbol{q} \in \mathbb{P}(\mathcal{X})$, where $\boldsymbol{q}'$ is renormalized after removing the position corresponding to the $\perp$ symbol from $\boldsymbol{q}$. Thus, it is the case that the problem for finding a crossover min-tradeoff function still has the form of Eq. (43). For crossover min-tradeoff functions, these two constants take the following values: $c_0 = 2\sqrt{\ln 2}\sqrt{1 - 2\log(\varepsilon_{\mathrm{acc}}\bar{\varepsilon}/4)}/\sqrt{n}$, $c_1 = 1/\sqrt{2\gamma}$.

The optimization problem in Eq. (43) has an infinite number of constraints that we cannot really handle since the constraint needs to be held for every density operator. However, we can use the Fenchel duality (see Section F.2) to show it is the dual problem of some primal problem that we can actually solve. Let $\{M_x : x \in \mathcal{X}\}$ denote the relevant bipartite POVM of a protocol. Section F.3 presents a detailed derivation of the primal-dual problem relation including strong duality. The primal problem corresponding to Eq. (43) is

$$
\begin{aligned}
&\underset{\rho,\boldsymbol{\xi}}{\text{minimize}} \quad W(\rho) - \sqrt{c_0^2 - \Big[\sum_x \boldsymbol{\xi}(x)\Big]^2/(4c_1^2)} \\
&\text{subject to} \quad \mathrm{Tr}(\rho) = 1 \\
&\qquad\qquad\quad -\boldsymbol{\xi}(x) \le \mathrm{Tr}(\rho M_x) - \boldsymbol{q}_0(x) \le \boldsymbol{\xi}(x) \\
&\qquad\qquad\quad \sum_x \boldsymbol{\xi}(x) \le 2c_0 c_1 \\
&\qquad\qquad\quad \rho \ge 0 \ , \ \boldsymbol{\xi} \in \mathbb{R}^{|\mathcal{X}|} \ .
\end{aligned}
\tag{44}
$$

We note that the primal problem in Eq. (44) is very similar to the primal problem in the asymptotic case in Eq. (22), but the difference is that the state ρ is not required to reproduce the statistics $\boldsymbol{q}_0$ exactly. Instead there is a penalty term in the objective function when $\text{Tr}[\rho M_x] \neq \boldsymbol{q}_0(x)$ and the additional constraint ensures that the penalty term is well-defined. We also note that one may need to use the perturbed version of W. The same perturbation procedure used for Algorithm 1 is applicable here for the function W. For simplicity of the presentation, we ignore the perturbation here.

To solve the primal problem in Eq. (44), it is often useful to use the gradient information. As the gradient of $W(\rho)$ is already discussed in the previous algorithm (including necessary perturbation), we just write the derivative of $\sqrt{c_0^2 - \left[\sum_j \boldsymbol{\xi}(j)\right]^2 / (4c_1^2)}$ with respect to $\boldsymbol{\xi}(k)$ here as

$$\frac{\partial}{\partial \boldsymbol{\xi}(k)} \sqrt{c_0^2 - \left(\sum_j \boldsymbol{\xi}(j)\right)^2 / (4c_1^2)} = -\frac{1}{4c_0^2 c_1^2} \frac{1}{\sqrt{1 - [\sum_j \boldsymbol{\xi}(j)]^2 / (4c_0^2 c_1^2)}} \sum_j \boldsymbol{\xi}(j) . \tag{45}$$

We can follow a similar two-step procedure as in [28] to solve the primal problem in Eq. (44). In the first step, we try to obtain a near-optimal solution $\rho^\star$ and in the second step, we solve the dual problem of the linearization of the objective function at the point $\rho^\star$. The dual problem of the linearization at a point $\rho^\star \in \text{D}(Q_i)$ is

$$\begin{aligned}
\underset{\boldsymbol{f}}{\text{maximize}} \quad & \boldsymbol{f} \cdot \boldsymbol{q}_0 - c_0 \sqrt{1 + c_1^2 [\max(\boldsymbol{f}) - \min(\boldsymbol{f})]^2} \\
\text{subject to} \quad & \sum_x \boldsymbol{f}(x) M_x \leq \nabla W(\rho^\star) .
\end{aligned} \tag{46}$$

We rewrite this problem as an SDP by introducing slack variables u, v, t:

$$\begin{aligned}
\underset{\boldsymbol{f}, u, v, t}{\text{maximize}} \quad & \boldsymbol{f} \cdot \boldsymbol{q}_0 - t \\
\text{subject to} \quad & \sum_x \boldsymbol{f}(x) M_x \leq \nabla W(\rho^\star) \\
& v\boldsymbol{1} \leq \boldsymbol{f} \leq u\boldsymbol{1} \\
& \begin{pmatrix} t - c_0 & c_0 c_1 (u - v) \\ c_0 c_1 (u - v) & t + c_0 \end{pmatrix} \geq 0 .
\end{aligned} \tag{47}$$

We now present our second algorithm for constructing min-tradeoff function in Algorithm 2.

Algorithm 2 The second algorithm for constructing min-tradeoff functions

Inputs:

$\boldsymbol{q}_0$	A given probability distribution in $\mathbb{P}(\mathcal{X})$
c_0, c_1	Two constants related to the EAT correction terms
$\{M_x : x \in \mathcal{X}\}$	Bipartite POVM used for testing

Output:

   $\boldsymbol{y}^\star$ A vector in $\mathbb{R}^{|\mathcal{X}|}$ which defines a min-tradeoff function by $f(\boldsymbol{q}) := \langle \boldsymbol{q}, \boldsymbol{y}^\star \rangle$.

Algorithm:

1. Use either the Frank-Wolfe method or an interior-point method to solve Eq. (44) and obtain a nearly optimal solution $\rho^\star$.

2. Solve the dual SDP problem of the linearization at the point $\rho^\star$ in Eq. (47) to obtain $\boldsymbol{y}^\star = \boldsymbol{f}$.

Our next task is to show that Algorithm 2 constructs a valid min-tradeoff function.

Proposition 4 (Correctness). *Assuming that $\sum_x \boldsymbol{f}(x) M_x \leq \nabla W(\rho^\star)$ is satisfied, the min-tradeoff function f constructed from $\boldsymbol{f} = \boldsymbol{y}^\star$ returned by Algorithm 2 is a valid min-tradeoff function.*

Proof. From the assumption $\sum_x \boldsymbol{f}(x) M_x \leq \nabla W(\rho^\star)$, it follows that for any $\rho \in \mathrm{D}(Q_i)$,

$$\sum_x \boldsymbol{f}(x) \operatorname{Tr}(\rho M_x) \leq \operatorname{Tr}(\rho \nabla W(\rho^\star)) \leq W(\rho), \tag{48}$$

where the last inequality follows from the linearization of the function W at the point $\rho^\star$ since W is a convex function. We note that this is exactly the condition for a valid min-tradeoff function since the left-hand side is the min-tradeoff function evaluated at the statistics produced by a state ρ and the right-hand side is the conditional entropy evaluated at the state ρ. As this inequality is true for any state, it follows that $f(\boldsymbol{q}) \leq \min_{\nu \in \Sigma_i(\boldsymbol{q})} H(S_i | P_i R)_\nu$ for every $\boldsymbol{q} \in \mathbb{P}(\mathcal{X})$ such that $\Sigma_i(\boldsymbol{q}) \neq \emptyset$. We also note that if $\Sigma_i(\boldsymbol{q}) = \emptyset$, the minimum on the right-hand side of Eq. (9) is defined as ∞ [16] so that $f(\boldsymbol{q}) \leq \min_{\nu \in \Sigma_i(\boldsymbol{q})} H(S_i | P_i R)_\nu = \infty$ is still satisfied in this case. $\qquad\square$

Remark 11. Due to the numerical precision of any solver, $\sum_x \boldsymbol{f}(x) M_x \leq \nabla W(\rho^\star)$ may not be exactly satisfied. In implementation, we relax this constraint by $\sum_x \boldsymbol{f}(x) M_x + \epsilon \mathbb{1} \leq \nabla W(\rho^\star)$ for some small ϵ that is slightly larger than the solver precision. By doing so, we make the value $f(\boldsymbol{q})$ smaller than it could be if there were no numerical precision issue. Thus, the correctness is guaranteed even when one takes into account of the numerical precision.

Remark 12. By taking into account some second-order correction terms in the objective function, as we will see later, Algorithm 2 can produce similar or better key rates than Algorithm 1 *without* optimizing the initial choice of $\boldsymbol{q}_0 \in \mathbb{P}(\mathcal{X})$, which can save computational time. Moreover, it is also possible to optimize the choice of $\boldsymbol{q}_0$ with this algorithm and choose the best one among all selected choices of $\boldsymbol{q}_0$. In addition, as we mentioned previously, this algorithm can be further improved since we made several simplifications and ignored some second-order correction terms. While it is possible to do so, adding back more terms will definitely make the optimization problem more complicated and thus a more sophisticated problem formulation is potentially needed. We leave any potential improvement for a future work.

6.4 Crossover min-tradeoff function

In practice, the number of testing rounds is typically chosen to be a small fraction of the total signals sent in the QKD protocol. When the number of test rounds becomes sufficiently smaller than the total number of signals, the original version of the EAT (Proposition 8) is generally dominated by the second-order term because it scales inversely with the testing probability γ. A solution for this issue is given in Ref. [17], where authors of [17] present the 'crossover min-tradeoff function', which may be used to induce a proper min-tradeoff function that does not generally become dominated by the second-order term when testing probability γ is small. For this reason, it is often advantageous to construct the crossover min-tradeoff function first and then reconstruct a normal min-tradeoff function from the crossover version. We review the definitions from [17] for completeness of our presentation and refer to [17, Section V.A] for further discussion.

Definition 5 (Channel with infrequent sampling). *A channel with testing probability $\gamma \in [0,1]$ is an EAT channel $\mathcal{M}_{i,Q_i \to S_i P_i X_i}$ such that $\mathcal{X} = \mathcal{X}' \cup \{\perp\}$ and that can be expressed as*

$$\mathcal{M}_{i,Q_i \to S_i P_i X_i}(\cdot) = \gamma \mathcal{M}^{\text{test}}_{i,Q_i \to S_i P_i X_i}(\cdot) + (1-\gamma)\mathcal{M}^{\text{gen}}_{i,Q_i \to S_i P_i}(\cdot) \otimes |\perp\rangle\langle\perp|_{X_i}, \tag{49}$$

where $\mathcal{M}^{\text{test}}_i$ never outputs the symbol $\perp$ on X_i.

In our case $\mathcal{M}^{\text{gen}}_{i,Q_i \to S_i P_i}$ is given by the protocol description where $S_i = \overline{A}_i$ and $P_i = \widetilde{A}_i\widetilde{B}_i$. The testing map $\mathcal{M}^{\text{test}}_{i,Q_i \to S_i P_i X_i}$ is given by $S_i = \overline{A}_i\overline{B}_i$ and $P_i = \widetilde{A}_i\widetilde{B}_i$ as per Protocol 3.

Definition 6 (Crossover min-tradeoff function). *Let $\mathcal{M}_i$ be a channel with testing probability γ as defined above. The crossover min-tradeoff function for $\mathcal{M}_i$ is an affine function $g : \mathbb{P}(\mathcal{X}') \to \mathbb{R}$ satisfying*

$$g(\boldsymbol{q}') \leq \min_{\nu \in \Sigma'_i(\boldsymbol{q}')} H(S_i|P_i R)_\nu \quad \forall \boldsymbol{q}' \in \mathbb{P}(\mathcal{X}'), \tag{50}$$

where the set of quantum states

$$\Sigma'_i(\boldsymbol{q}') := \left\{ \nu_{S_i P_i X_i R} = (\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{Q_i R}) : \omega \in \mathrm{D}(Q_i \otimes R) \,\&\, [(\mathcal{M}^{\text{test}}_i \otimes \mathcal{I}_R)(\omega_{Q_i R})]_{X_i} = \boldsymbol{q}' \right\}. \tag{51}$$

We note that the difference between the crossover min-tradeoff function and the original min-tradeoff function defined in Definition 2 is that we only require the testing rounds to give the correct frequency distribution.

For each $x \in \mathcal{X}$, let $\delta_x \in \mathbb{P}(\mathcal{X})$ denote the frequency distribution with $\delta_x(x) = 1$ and $\delta_x(x') = 0$ for all other $x' \in \mathcal{X}$ such that $x' \neq x$. The crossover min-tradeoff function g automatically defines a min-tradeoff function $f : \mathbb{P}(\mathcal{X}) \to \mathbb{R}$ by [17]:

$$f(\delta_x) = \mathsf{Max}(g) + \frac{1}{\gamma}[g(\delta_x) - \mathsf{Max}(g)] \quad \forall x \in \mathcal{X}' \tag{52}$$

$$f(\delta_\perp) = \mathsf{Max}(g). \tag{53}$$

Moreover, we have the relations [17]:

$$\mathsf{Max}(f) = \mathsf{Max}(g) \tag{54}$$

$$\mathsf{Min}(f) = (1 - \frac{1}{\gamma})\mathsf{Max}(g) + \frac{1}{\gamma}\mathsf{Min}(g) \tag{55}$$

$$\mathsf{Min}_\Sigma(f) \geq \mathsf{Min}(g) \tag{56}$$

$$\mathsf{Var}(f) \leq \frac{1}{\gamma}[\mathsf{Max}(g) - \mathsf{Min}(g)]^2. \tag{57}$$

6.5 Procedure for key rate calculation

We now provide an instruction for the finite-key length ℓ calculation using Algorithm 1 and Theorem 5.

1. We first pick a frequency distribution $\boldsymbol{q}_0$ and then apply Algorithm 1 to construct a crossover min-tradeoff function g. By solving the dual SDP of the linearized problem, the algorithm returns us a list of dual variables, which are coefficients of the min-tradeoff function g.

2. We construct the min-tradeoff function f needed for EAT by Eq. (52) and Eq. (53), and then compute $\min_{\boldsymbol{q} \in \mathcal{Q}} f(\boldsymbol{q})$ to get the first-order term h.

3. We evaluate $\mathsf{Max}(g)$, $\mathsf{Min}(g)$ by simply taking the max and min of coefficients.

4. We apply Theorem 5 with the relations in Eqs. (54) to (57) to obtain a lower bound. To do so, we optimize the choice of β and δ in Theorem 5 using MATLAB built-in `fmincon` function. This optimization gives us the optimal second-order correction terms for the given choice of min-tradeoff function.

5. We repeat this process with a different frequency distribution $\boldsymbol{q}_0$ to generate a different min-tradeoff function. We optimize the choice of min-tradeoff functions in a simple heuristic way by picking several different $\boldsymbol{q}_0$'s.

Similarly, we can use Algorithm 2 and Theorem 5. The procedure is similar to the above except that we do not need to optimize the initial choice $\boldsymbol{q}_0$ (although one can still do it if it can give a better choice of the min-tradeoff functions). To apply Theorem 15, we also have a similar procedure except that we optimize the choice of α in the statement of Theorem 15 with MATLAB built-in `fminbnd` function.

7 Examples

We first present examples with announcements based on only seeded randomness and then consider an example with more sophisticated announcements. In the first example, we apply our method to the entanglement-based BB84 protocol with an ideal entangled photon source. In the second example, we provide a finite key analysis of six-state four-state protocol [32]. We use both these two examples to demonstrate the effectiveness of our method, compare performances of two algorithms and compare two versions of the EAT (smoothed min-entropy versus sandwiched Rényi entropy). In the third example, we then show the key rates of high-dimensional protocols with two mutually unbiased bases (MUBs), i.e. analogs of BB84 using qudit systems. We show that for these protocols the Entropy Accumulation Theorem can outperform the postselection technique [15]. In the last example, we show the key rates of the entanglement-based BB84 with a realistic entangled photon source.

In all examples, for the purpose of illustration, we make the following choices in the numerics. We set $\bar{\varepsilon} = \varepsilon_{\mathrm{PA}} = \varepsilon_{\mathrm{EC}} = \varepsilon_{\mathrm{EA}} = \frac{1}{4} \times 10^{-8}$. To apply Theorem 5, we set $\varepsilon_{\mathrm{sec}} = \bar{\varepsilon} + \varepsilon_{\mathrm{PA}}$ and $\varepsilon_{\mathrm{acc}} = \varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{EC}}$. To apply Theorem 15, we set $\varepsilon_{\mathrm{acc}} = \bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}$. This results in both cases using the same value of $\varepsilon_{\mathrm{acc}}$ and thus providing the same security guarantee (namely, guaranteeing the same $\varepsilon_{\mathrm{acc}}$-secure key). In all examples, to estimate the cost of error correction $\mathrm{leak}_{\varepsilon_{\mathrm{EC}}}$, we set $\mathrm{leak}_{\varepsilon_{\mathrm{EC}}} = n f_{\mathrm{EC}} H(Z|\hat{Z}) + \log(2/\varepsilon_{\mathrm{EC}})$, where f_{EC} is the inefficiency of an error correction code and $H(Z|\hat{Z})$ is the von Neumann entropy of Alice's key (in a single round) conditioned on Bob's guess $\hat{Z}$. In the simulation, we set $f_{\mathrm{EC}} = 1.16$ for all examples.

We also remark that our implementation allows us to define the acceptance set $\mathcal{Q}$ (see Protocol 1) as $\mathcal{Q} = \{F \in \mathbb{P}(\mathcal{X}) : \left\| F - \bar{F} \right\|_1 \leq \xi_t\}$, where $\bar{F}$ is the expected frequency distribution in an honest implementation and ξ_t is the acceptance threshold. As mentioned in Section 4.2.1, key rates should decrease as the ξ_t grows. We present an example of this scaling for qubit-based BB84 in Section 7.1 and in other examples we specify the choice for ξ_t we have chosen.

We highlight that we optimize both β and δ in the statement of Theorem 5 when we use the key-length expression from this theorem. Similarly, we optimize the choice of α in the statement of Theorem 15 when using it. As discussed previously, this optimization is done with MATLAB's `fmincon` function for the former case and `fminbnd` function for the latter case.

7.1 Qubit-based BB84

We apply our method to analyze a simple entanglement-based BB84 example based on the qubit implementation to compare different EAT statements, two algorithm variants for the construction of min-tradeoff functions, and study the scaling of the rate as a function of the size of our acceptance set. We assume that Alice's system and Bob's system are qubits and do not consider loss for this example.

7.1.1 Protocol description and simulation

We consider the following setup for this protocol:

(1) Alice chooses the Z basis with a probability p_z and the X basis with a probability $1-p_z$. Bob chooses to measure in the Z basis with a probability p_z and in X basis with a probability $1-p_z$.

(2) Key-generation rounds are where they both choose Z basis. The testing rounds are where they both choose X basis. They discard rounds with mismatched basis choices.

(3) They perform parameter estimation before error correction. For parameter estimation, we use the phase error POVM $\{E_X, \mathbb{1}-E_X\}$ where E_X is the X-basis error operator. This corresponds to statistics $\{e_x, 1-e_x\}$ where e_x is the X-basis error rate.

We note that in this protocol setup, the testing probability γ is given by the probability that both Alice and Bob choose the X basis, that is, $\gamma = (1-p_z)^2$. The sifting factor for the key rate is p_z^2. We consider an efficient version of BB84 [44] by choosing p_z to be close to 1. This also corresponds to infrequent testing in our setup. We remark that since basis choices are made based on seeded random numbers and they are chosen independently in each round, their announcements trivially satisfy the Markov condition.

In our simulation, we use the depolarizing channel to model noises. The simulated state that we use to calculate the observed statistics is

$$\rho^{\mathrm{sim}} = (1 - \frac{3}{2}Q)\left|\Phi^+\right\rangle\!\!\left\langle\Phi^+\right| + \frac{Q}{2}(\left|\Phi^-\right\rangle\!\!\left\langle\Phi^-\right| + \left|\Psi^+\right\rangle\!\!\left\langle\Psi^+\right| + \left|\Psi^-\right\rangle\!\!\left\langle\Psi^-\right|), \tag{58}$$

where $\left|\Phi^+\right\rangle, \left|\Phi^-\right\rangle, \left|\Psi^+\right\rangle$ and $\left|\Psi^-\right\rangle$ are Bell states, and Q is the quantum bit error rate. The statistics $\boldsymbol{q}_0$ that we need to give as an input to the min-tradeoff function construction algorithm is then given by $\boldsymbol{q}_0(j) = \mathrm{Tr}(\rho^{\mathrm{sim}}M_j)$ for Alice and Bob's joint POVM $\{M_j\}$.

7.1.2 Results

When applying Algorithm 1 to the finite-key rate calculation, we optimize the min-tradeoff functions by choosing different $\boldsymbol{q}_0 = (Q, 1-Q)$ where Q is searched over the interval $[0.005, 0.07]$ with a step size 0.005. For each min-tradeoff function generated from a particular value of Q, we calculate the key rate, which is the key length ℓ divided by the total number of signals n. We then choose the maximum key rate among all possible choices of min-tradeoff functions generated in this way. This way of coarse-grained search over $\boldsymbol{q}_0$ is a heuristic approach to optimize the choice of min-tradeoff functions. We find these choices of $\boldsymbol{q}_0$ in general give us good results. However, a more sophisticated optimization over $\boldsymbol{q}_0$ might potentially improve the results presented here.

For Algorithm 2, we use the interior-point method from MATLAB's `fmincon` function for the first step and then use CVX for the linearized dual problem. We note that we can also use the
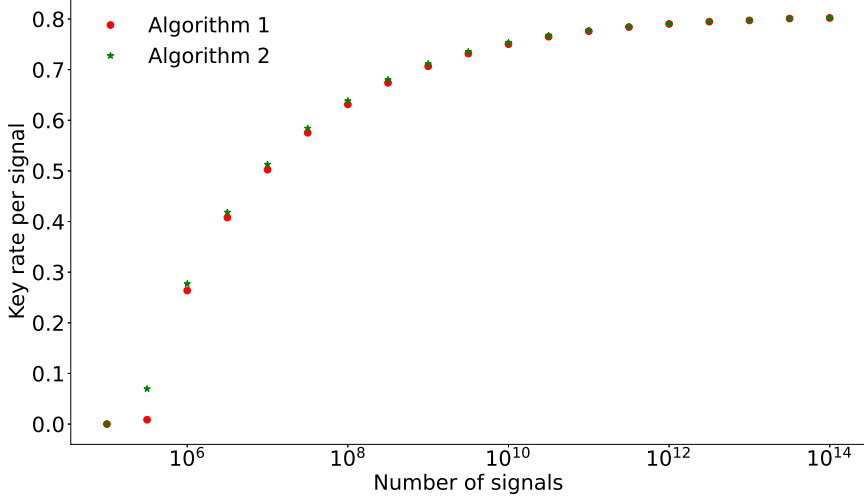
Figure 2: Key rate versus the number of signals for the qubit BB84 protocol to compare two algorithms for the generation of min-tradeoff functions. The quantum bit error rate is set to $Q = 0.01$ in the simulation, and $\zeta_t = 0.005$ for defining the acceptance set $\mathcal{Q}$. The red circle marker corresponds to Algorithm 1 while the green star marker corresponds to Algorithm 2. The key rate formula is based on Theorem 5. Other protocol parameters are optimized as described in the main text.

Frank-Wolfe algorithm for the first step instead of the and the interior-point method. When we do so, results are similar (slightly worse) for this example.

For both algorithms, we optimize p_z by optimizing $\gamma = (1 - p_z)^2 = 10^{-k}$ where k is chosen from the interval $[2, 4]$ with a step size of 0.1. For block sizes larger than or equal to 10^{10}, we allow p_z to be closer to 1 by searching k in the interval $[3, 7]$ with a step size of 0.2. Again, those choices are heuristic and could be potentially improved. Nevertheless, they are sufficient for our purpose.

In Figure 2, we compare the key rates obtained from these two algorithms with Theorem 5. Interestingly, both algorithms give similar results while Algorithm 2 seems to be slightly better in terms of the smallest number of signals for nonzero key rates. Intuitively, we expect Algorithm 2 to behave better as it takes into account some second-order correction terms, while Algorithm 1 only looks for the min-tradeoff function that gives the highest leading-order term. As we perform an optimization of the choice of min-tradeoff function by different initial q_0's for Algorithm 1, we observe that the optimal finite key rate from Algorithm 1 is often given by a min-tradeoff function that does not give the highest value for the leading-order term. Due to the optimization of q_0, the running time of Algorithm 1 is much longer than that of Algorithm 2.

In Figure 3, we compare key rates given by Theorems 5 and 15 when we use Algorithm 2. One can see that Theorem 5 gives better key rates. This confirms our conjecture that the EAT based on the sandwiched α-Rényi entropy is tighter than the EAT based on the smooth min-entropy for lower-order correction terms. The intuition for this is that the Entropy Accumulation Theorem for smooth entropies is first derived in terms of H_α sandwiched Rényi entropies and then converted to statements about smooth entropies [16, 17]. It follows that avoiding the conversion to smooth entropies should only improve the key rate.

In Figure 4, we compare the key rate as a function of the size of the acceptance set, which is relevant when designing practical protocols where there exists a tradeoff between completeness and key rate. In Figure 4(a), it appears that the fluctuation of key rate per signal is minimal for smaller number of signals and then separates as the signal length grows. In Figure 4(b), the key
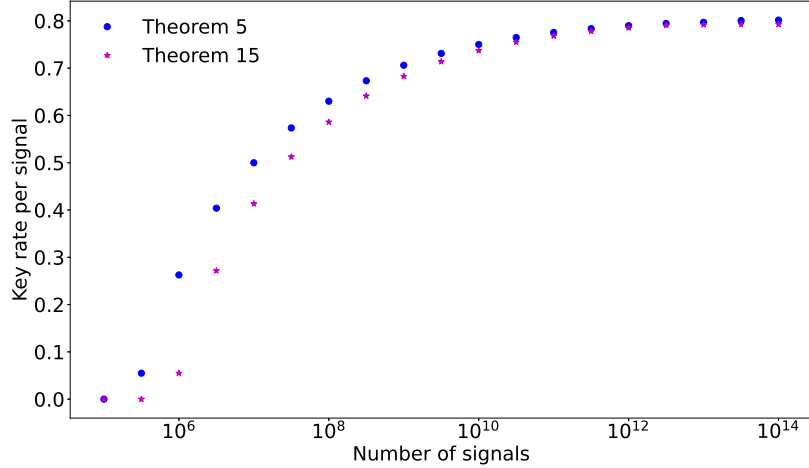
Figure 3: Key rate versus the number of signals for the qubit BB84 protocol to compare different second-order correction terms using Algorithm 2. The quantum bit error rate is set to $Q = 0.01$ in the simulation, and $\zeta_t = 0.005$ for defining the acceptance set $\mathcal{Q}$. The blue circle marker corresponds to the key rate formula given in Theorem 5 [29] while the magenta star marker corresponds to the key rate formula from Theorem 15 [17].

rate per signal is normalized to the case $\zeta_t = 0$ to look at this behaviour more closely. In this case we indeed see that at sufficiently large block size the fraction between each change in ζ_t is relatively constant. However, at the smaller block sizes, there seems to be less of a fluctuation between they key rates. It is possible this has to do with the relevance of the second-order term in small block sizes, but it also may be a property of our algorithm. The ability to investigate such properties with our numerics may be useful in designing protocols with small block size.

7.2 Six-state four-state protocol

Another interesting example is the six-state four-state protocol [32]. In the free space implementation of QKD protocols with the polarization encoding, there is naturally one axis that is stable against turbulence while other axes are slowly drifting. The idea of reference-frame-independent QKD [45] was motivated to address this issue and it was shown that such a protocol can be robust to slow drifts. The basic idea is that if the reference frame drift can be described by a unitary rotation, by using the information from an additional basis, one can effectively undo this unitary rotation. Here we consider the six-state four-state protocol [32] which has the reference-frame-independent feature. In particular, we consider the entanglement-based version and assume Alice and Bob have qubits. We do not consider losses in this example.

7.2.1 Protocol and simulation

We analyze the entanglement-based version of the six-state four-state protocol [32] assuming that Alice and Bob each receive a qubit in each round for simplicity of calculation. In this protocol, Alice measures the state in one of the X, Y and Z bases according to the probability distribution $((1-p_z)/2, (1-p_z)/2, p_z)$, while Bob measures in one of X and Z bases with the probability distribution $(1-p_z, p_z)$. Similarly to the previous qubit BB84 example, when both Alice and Bob choose the Z basis, this round is used for key generation. When Alice chooses X or Y basis and Bob chooses X basis, this round is used for parameter estimation. All other rounds are discarded. We consider an efficient version by setting p_z to be close to 1. In the
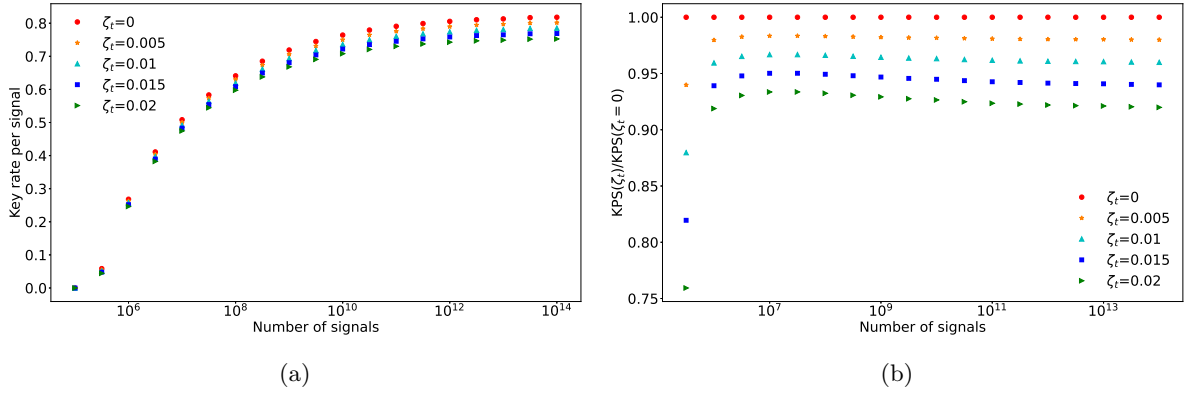
Figure 4: (a) Key rate versus the number of signals for the qubit BB84 protocol for different 'sizes' of acceptance set controlled by parameter ζ_t. (b) The fraction of the key rate per signal (KPS) at $\zeta_t = 0$ achieved for other values of ζ_t. In both subplots, the quantum bit error rate is set to $Q = 0.01$ in the simulation. Other protocol parameters as described in the main text.

testing step of the protocol, we use the POVM that contains error rates in the XX and YX bases.

For the simulation, we assume the Z basis is free of misalignment. The misalignment happens in the X-Y plane of the Bloch sphere. Thus, on top of the qubit depolarizing channel, we also apply a unitary rotation along the Z axis to Bob's qubit in order to model the misalignment. We choose the angle of rotation to be $11°$ in the simulation. The state used to obtain the observed statistics from this simulation is

$$\rho^{\text{sim}} = (\mathbb{1}_A \otimes e^{i\theta\sigma_Z})\rho^{\text{dp}}(\mathbb{1}_A \otimes e^{-i\theta\sigma_Z}), \tag{59}$$

where σ_Z is the Pauli-Z matrix, θ is the angle of rotation and ρ^{dp} is the state given in Eq. (58) (that is, the simulated state in the qubit-based BB84 example).

7.2.2 Results

In the application of Algorithm 1 to the finite-key rate calculation, we optimize the min-tradeoff functions by choosing different $\boldsymbol{q}_0$'s. We adopt a heuristic approach to optimize the choice of min-tradeoff functions. Each $\boldsymbol{q}_0$ is created by choosing a different depolarizing probability Q, which is searched over the interval $[0.005, 0.07]$ with a step size 0.005. It is a heuristic choice that serves our purpose. For each min-tradeoff function generated from a particular value of Q, we calculate the key rate and then choose the maximum key rate among them. For Algorithm 2, we use same procedure as for the qubit BB84 example in Section 7.1 including the optimization over the choice of p_z.

In Figure 5, we compare two algorithms for the min-tradeoff function construction. For this plot, similar to qubit-based BB84 example, we perform additional initial point $\boldsymbol{q}_0$ optimization for Algorithm 1 while we do not optimize $\boldsymbol{q}_0$ for Algorithm 2. Like Figure 2, both algorithms give similar key rates.

In Figure 6, we compare key rates for Theorems 5 and 15 and observe the same behavior as the qubit-based BB84 example in Figure 3. As explained in the qubit-based BB84 example in Figure 3, this behavior is not surprising since the sandwiched Rényi entropy was used in the middle step of the proofs of Theorems 1 and 11 in Refs. [16, 17] before converting to the smooth min-entropy by an additional inequality. One would expect that bypassing the smooth min-entropy gives tighter key rates due to the removal of an inequality.
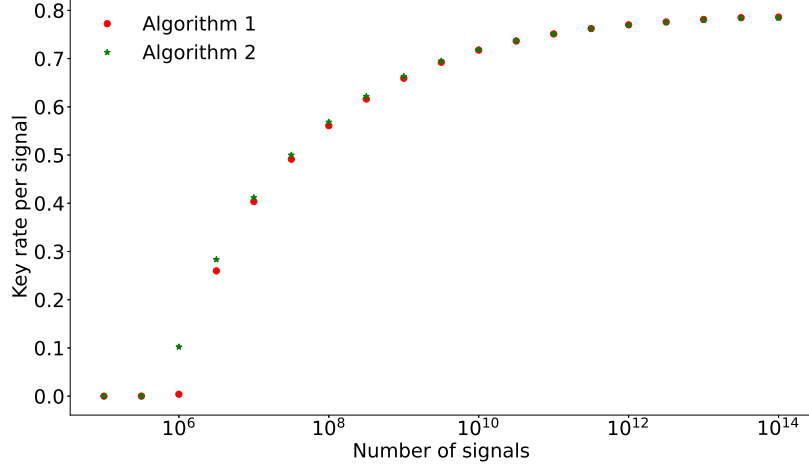
36

Figure 5: Key rate versus the number of signals for the six-state four-state protocol with two algorithms. The quantum bit error rate is set to $Q = 0.01$ in the simulation, and $\zeta_t = 0.005$ for defining the acceptance set $\mathcal{Q}$. This plot is obtained by using the key rate formula given in Theorem 5 [29]. The red circle marker corresponds to the min-tradeoff function construction by Algorithm 1 while the green star marker corresponds to the min-tradeoff function construction by Algorithm 2.

7.3 High-dimensional 2-MUB protocol

To demonstrate an advantage of our approach in the EAT framework, we analyze an interesting family of protocols which are the high-dimensional analog of the BB84 protocol. In BB84, two mutually unbiased bases (MUBs) are used. We consider qudit systems with 2 MUBs. We compare our calculation with the postselection technique [15] combined with the numerical approach of [42]. We use this example to demonstrate that EAT can give better key rates compared to the postselection technique [15], especially when the dimension $\dim(\mathcal{H}_{AB})$ in the protocol is large. The key idea is that the reduction via the post-selection technique involves a security parameter scaling exponentially in the dimension, which leads to a correction to the key length. This correction term does not arise when applying the EAT. While perhaps intuitive, it is unclear how to prove this results in an advantage at all blocklengths and all dimensions and, to the best of our knowledge, this is the first work that has discussed this difference in security proof methods or numerically investigated them.

7.3.1 Protocol and simulation

To properly define the protocol setup, recall that the discrete Weyl operators are defined as

$$U_{jk} = \sum_{s=0}^{d-1} \omega^{sk} |s+j\rangle\langle s| \tag{60}$$

for $j, k \in \{0, 1, \ldots, d-1\}$ where $\omega = e^{2\pi i/d}$ is a dth root of unity. We note that U_{01} is the generalized Pauli-Z matrix and U_{10} is the generalized Pauli-X matrix. We define the qudit version of Z and X operators as $Z := U_{01}$ and $X := U_{10}$. The generalized Bell states are

$$|\Phi_{jk}\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} \omega^{sk} |s, s+j\rangle = \mathbb{1} \otimes U_{jk} |\Phi_{00}\rangle. \tag{61}$$

In the 2-MUB protocol, Alice measures in the eigenbasis of either U_{01} or U_{10}. Bob similarly measures in the eigenbasis of either U_{01}^* or U_{10}^*. The eigenbasis of the operator $Z := U_{01}$ is
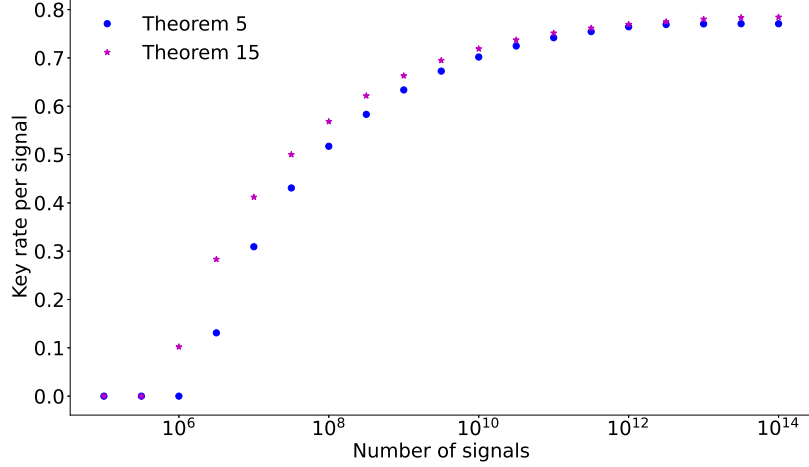
37

Figure 6: Key rate versus the number of signals for the six-state four-state protocol with different second-order correction terms. The quantum bit error rate is set to $Q = 0.01$ in the simulation, and $\zeta_t = 0.005$ for defining the acceptance set $\mathcal{Q}$. This plot is obtained by using Algorithm 2. The red circle marker corresponds to the key rate formula given in Theorem 5 [29] while the green star marker corresponds to the key rate formula from Theorem 15 [17].

the computational basis $\{|s\rangle : 0 \leq s \leq d - 1\}$. The eigenbasis of the operator $X := U_{10}$ is $\{|\psi_j^X\rangle : 0 \leq j \leq d - 1\}$ where

$$|\psi_j^X\rangle := \sum_{s=0}^{d-1} \frac{\omega^{-js}}{\sqrt{d}} |s\rangle . \tag{62}$$

They each choose to measure in the Z basis with the probability p_z and choose to measure in the X basis with the probability $1 - p_z$. In the classical phase, Alice and Bob announce their basis choices and discard rounds with mismatched bases. We allow an asymmetric basis choice, i.e., setting p_z close to 1. In this protocol, all public announcements are based on seeded randomness. For simplicity of calculation, the testing rounds are those when they both choose X basis and the key generation rounds are rounds when they both choose Z basis.

It is interesting to note that the state $|\Phi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_s |s, s\rangle$ is invariant under any $U_{jk} \otimes U_{jk}^*$. In an honest implementation, the source is supposed to prepare the state $|\Phi_{00}\rangle$, and then to distribute one half to Alice and the other half to Bob. If the quantum channel is ideal, then they are supposed to obtain perfectly correlated results just like the qubit case.

Following the reasoning of [46, 47], Alice's and Bob's joint density operator can be taken as diagonal in the generalized Bell basis:

$$\rho_{AB}^{\mathrm{BG}} = \sum_{j,k} \lambda_{jk} |\Phi_{jk}\rangle\langle\Phi_{jk}| , \tag{63}$$

where

$$\lambda_{jk} = \frac{1}{d} \Big(\sum_s q_{1s}^{(sj-k \bmod d)} + q_{01}^{(j)} - 1 \Big) \tag{64}$$

with $q_{jk}^{(i)}$ being the ith entry of the error vector $\boldsymbol{q}_{jk}$. See also [48] for a detailed discussion. For our purpose of simulating the frequency distribution $\boldsymbol{q}_0$ needed for Algorithm 1 or Algorithm 2, we take the simulation state ρ_{AB}^{sim} used to generate the full statistics as $\rho_{AB}^{\mathrm{sim}} = \rho_{AB}^{\mathrm{BG}}$.

We follow the simulation in [48] by considering the following observation for error vector $\boldsymbol{q}_{jk}$ in each basis U_{jk}, which is based on the natural generalization of the qubit depolarizing channel

38

with a depolarizing probability Q:

$$\boldsymbol{q}_{jk}(Q) := \{1 - Q, Q/(d-1), \dots, Q/(d-1)\}. \tag{65}$$
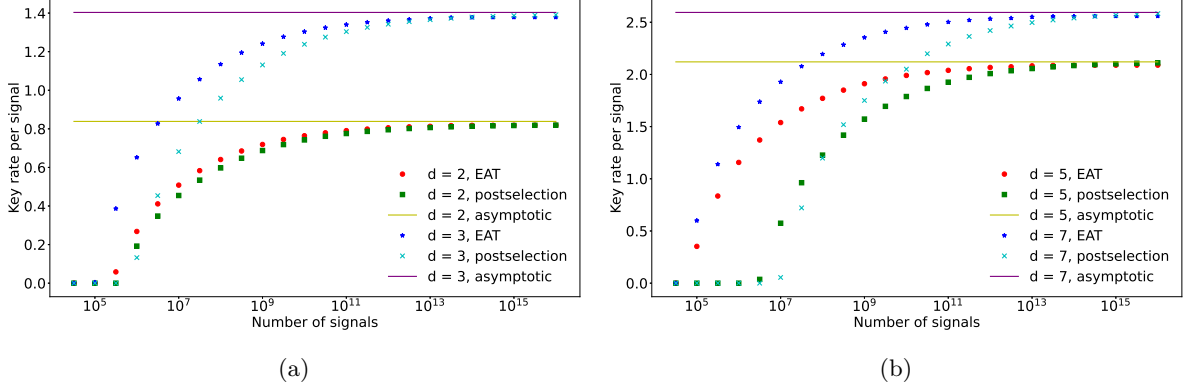
7.3.2 Results

Figure 7: 2-MUB protocols with qudits for various values of dimension d. The depolarizing probability is set to $Q = 0.01$ in the simulation. The calculation is done with Algorithm 2 and the finite-key rate formula is from Theorem 5 [29]. The calculation of postselection technique is done using the numerical approach of [42] in combination of [15]. For simplicity in implementing the post-selection technique code, we use $\zeta_t = 0$ in these plots. The asymptotic key rate formula is given in [33, 48].

In Figure 7, we compare our results using Theorem 5 [29] with results obtained by the postselection technique [15] for 2-MUB protocols in dimensions $d = 2, 3, 5$ and 7. For simplicity in implementation of the post-selection technique, we use $\zeta_t = 0$ in this simulation, which we stress means the protocol is $\sim$ 1-complete at reasonable block sizes (See Definition 4) and thus not practical.[12] We note that 2-MUB protocols exist in any dimensions $d \geq 2$ and our proof method can work for any dimension. Here, we restrict to prime dimensions due to our choice of data simulation method. For both EAT and the postselection technique, we optimize the probability of choosing Z basis. The probability of testing is set to $\gamma = (1 - p_z)^2$. We optimize the probability of choosing Z-basis in the same way as in the qubit-based BB84 example.

It can be seen that both EAT and postselection technique can approach the expected asymptotic key rate in the infinite-key limit. Also, our method based on EAT outperforms the postselection technique for 2-MUB protocols in any dimensions. We also observe that for larger dimensions, our method can give much higher key rate than the postselection technique for small block sizes. This makes our method attractive since small block sizes are of particular interests for experimental implementations.

In the same plot, we also show the asymptotic key rate for 2-MUB protocol. The asymptotic key rate formula is given in [33, 48]. Both our method and the postselection technique can approach the asymptotic key rate for sufficiently large block size. We also note that for block size larger than 10^{17}, there seems to be a small constant deviation from the asymptotic key rate in both postselection technique and our method. This deviation is mainly due to our optimization over p_z, which is done by choosing a set of values. The asymptotic key rate formula that we use assumes that we can set p_z to be arbitrarily close to 1 such that the sifting factor is 1. On the other hand, numerical optimization over p_z in our method cannot take p_z too

---

[12]This is not to imply the post-selection technique cannot be used more generally.

close to one. The reason for our EAT method is that our testing probability is set to be $(1-p_z)^2$. When the testing probability is small, the variance of the min-tradeoff function, $\mathsf{Var}(f)$, becomes large as shown in Eq. (57). Since $\mathsf{Var}(f)$ shows up in the second-order correction term, for a fixed block size, there is always a limit on how small the testing probability γ can be before we start to lose key rates due to its adverse effect on the second-order correction term. For a fair comparison between our EAT approach and the postselection technique, we also use the same optimization of p_z in the calculation with the postselection technique.

7.4 BB84 with a realistic spontaneous parametric downconversion source

We consider an example where the Markov chain conditions are not simply based on seeded randomness. This example considers an optical implementation of entanglement-based BB84. The photon-pair source is a spontaneous parametric downconversion source where there is a non-negligible probability that the source emits vacuum or more than one photon pair. Due to photon loss during the transmission and non-unity detector efficiencies, there are no-detection events. In the protocol, Alice and Bob announce these events and discard the corresponding rounds. We need to verify that this type of announcements do not violate the Markov chain conditions.

7.4.1 Protocol and simulation method

In this protocol, a type-II parametric down-conversion (PDC) source emits a state with polarization encoding [49, 50] which is

$$|\Psi\rangle = (\cosh(\chi))^{-2} \sum_{n=0}^{\infty} \sqrt{n+1} \tanh^n(\chi) |\Phi_n\rangle \tag{66}$$

where $|\Phi\rangle_n$ is the state of an n-photon pair which can be written as

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m |n-m, m\rangle_a |m, n-m\rangle_b. \tag{67}$$

The average number of photon pairs generated by one pump pulse is 2λ, where $\lambda = \sinh(\chi)$. In this protocol, Alice and Bob each have a set of single-photon detectors. We consider the BB84 detector setup with a passive basis choice; that is, each measurement setup consists of an initial 50/50 beam splitter and each output port of this beam splitter is directed to a polarizing beam splitter with two single-photon detectors. We assume Alice's two detectors have the same detector efficiency η_A and the same dark count probability Y_{0A}. Similarly, we assume that Bob's two detectors have the same detector efficiency η_B and the same dark count probability Y_{0B}. Using the similar choice as in other examples, whenever Alice and Bob choose X-basis, the round is used for testing. The key generation round is when they both choose Z-basis. Their probabilities of choosing Z basis are p_{zA} and p_{zB}, respectively. The probability of testing is set to $\gamma = (1 - p_{zA})(1 - p_{zB})$.

Our simulation is based on [50]. In this simulation, there are three main contributions to quantum bit error rate: (i) background counts of detectors, which are random noises with $e_0 = 1/2$; (ii) intrinsic detector error e_d, which is the probability that a photon enters the erroneous detector and is used to characterized the alignment and stability of optical system between Alice's and Bob's detection systems; (iii) errors due to multiphoton-pair states: (a) Alice and Bob may detect different photon pairs and (b) double clicks from detectors. Alice and Bob assign a random bit for each double-click event in order to use the squashing model [51, 52].

In particular, the overall gain, Q_λ, as a function of the average number of photons, λ, in each mode, dark counts and detector efficiencies is given by [50, Eq. (9)]

$$Q_\lambda = 1 - \frac{1 - Y_{0A}}{(1 + \eta_A \lambda)} - \frac{1 - Y_{0B}}{(1 + \eta_B \lambda)} + \frac{(1 - Y_{0A})(1 - Y_{0B})}{(1 + \eta_A \lambda + \eta_B \lambda - \eta_A \eta_B \lambda)^2}. \tag{68}$$

The overall quantum bit error rate (E_λ) is given by [50, Eq. (10)]

$$E_\lambda Q_\lambda = e_0 Q_\lambda - \frac{2(e_0 - e_d)\eta_A \eta_B \lambda(1 + \lambda)}{(1 + \eta_A \lambda)(1 + \eta_B \lambda)(1 + \eta_A \lambda + \eta_B \lambda - \eta_A \eta_B \lambda)}. \tag{69}$$

To reduce the number of free parameters in the protocol setup, we set $p_{zA} = p_{zB} = p_z$ and the testing probability is set to $\gamma = (1 - p_z)^2$. We optimize the choice of p_z in the same way as in Section 7.1.

7.4.2 Assumption on announcements

We need to verify for Markov chain conditions that the probability of a detection event only depends on the total photon number, but not on the particular n-photon state. We show that this holds when Alice's (Bob's) detectors consist of two single-photon detectors with an identical detection efficiency η_A (η_B), and a basis-independent dark count probability Y_{0A} (Y_{0B}). We note that the measurement performed by Bob (Alice) is block diagonal in the total photon number basis, as is the case in all discrete-variable protocols.

Under our assumption about the detectors, we can treat all the imperfections of detectors as a part of the quantum channel and then assume ideal detectors in our analysis. Doing so only strengthens Eve's power. After assigning double-click events to random bits, we note that the measurement setup in this protocol admits a squashing model [51, 52]. In our analysis, we can use the effective qubit measurement for Alice (Bob) as the target measurement. This target measurement acts on the Hilbert space that consists of a one-dimensional vacuum space and a two-dimensional qubit space. In particular, the announcement about detection and no-detection corresponds to the POVM $\{M_{\text{det}}, M_{\text{no-det}}\}$, which is defined as

$$M_{\text{det}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ M_{\text{no-det}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{70}$$

where they are represented in the basis $\{|\text{vac}\rangle, |0\rangle, |1\rangle\}$. Here, $|\text{vac}\rangle$ is the vacuum state and $|0\rangle, |1\rangle$ are the computational basis states of a qubit. Clearly, this POVM is weekly dependent according to Definition 3. Thus, this announcement is allowed in applying Theorem 5.

7.4.3 Results

In Figure 8, we show the key rate of this protocol for different distances (L in kilometers) between Alice and Bob. We assume that the source is located in the middle and at an equal distance from Alice and Bob. We choose detector efficiencies $\eta_A = \eta_B = 0.8$ and dark counts $Y_{0A} = Y_{0B} = 10^{-7}$ for the simulation in this plot.[13] We also set the intrinsic detector error e_d as 1%. On the one hand, we can see that our method works for optical implementations from this figure. On the other hand, as the distance between Alice and Bob increases, the

---

[13]This choice of detector parameters may be realized by superconducting nanowire single-photon detectors. However, the purpose here is to demonstrate that our method can handle some imperfections and loss. Our method also has limitations in the amount of loss it can handle.
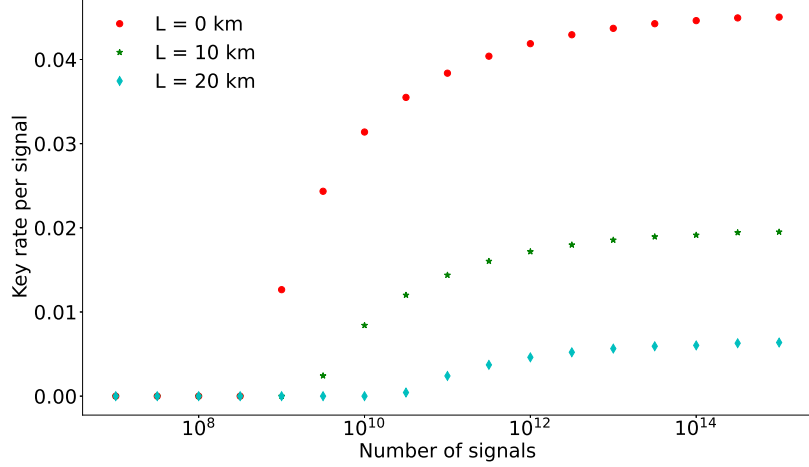
Figure 8: Key rate per signal sent versus the number of signals for BB84 with a spontaneous parametric downconversion source for various distances between Alice and Bob. This plot is obtained with Algorithm 1 and Theorem 5. The acceptance set threshold $\zeta_t = 0.005$ is used for defining the acceptance set $\mathcal{Q}$. Parameters are specified in the main text.

minimal number of signals for positive key rate also increases significantly, and the key rate drops quickly. In our key rate expression from Theorem 5 (also from Theorem 15), the term $-n\gamma \log(|\mathcal{A}|)$ decreases the key length and becomes more problematic for this protocol since the entropy only accumulates in rounds where both Alice and Bob successfully detected photons. However, this term does not scale with the probability of detection. For long distances, this seems to suggest that the cost for parameter estimation is higher than the entropy accumulated from rounds with successful detection. Unfortunately, this counter-intuitive effect comes from the limitation of our proof method in dealing with parameter estimation registers. We hope that a better approach to handle the information leakage from the parameter estimation step can be found in the future to significantly improve the key rate.

8 Discussion and Conclusion

In this work, we have adapted the EAT to entanglement-based device-dependent QKD protocols. To do so, we introduced new tools. First, we constructed new sufficient conditions on the public announcements of the protocol to guarantee the Markov conditions necessary for the EAT. These conditions capture the intuition that if Eve would always know some information for each round of the protocol, then announcing that information cannot change the security. The interesting point is that this guarantees the Markov conditions on Eve's optimal attack.

Second, we proposed two variants of a numerical algorithm to construct min-tradeoff functions, both of which are efficient and one which considers second-order effects. Both methods build off of previous work [27, 28], but the ability to construct min-tradeoff functions that take into account second-order correction information is novel and we expect it could be useful in other settings. We note this second-order correction algorithm relies on using Fenchel duality, which to the best of our knowledge has not been used in quantum information theory previously.

Third, we derived our key length bound (Theorem 5) using Dupuis' privacy amplification for sandwiched Rényi entropies $H_\alpha^\uparrow$ [29]. In that work, Dupuis demonstrates one can obtain simpler error exponents for privacy amplification using the Rényi version of the EAT along with his Rényi leftover hashing lemma [29, Theorem 9] than if one were to apply the smooth

min-entropy leftover hashing lemma [13]. Here we have shown an alternative advantage: by avoiding the conversion of the Rényi EAT into smooth min-entropy terms, we can tighten our bound on the key rate.

We then apply our methods to several examples. First, we applied it to ideal qubit-based BB84 and six-state four-state protocols where we show the application of both our min-tradeoff construction algorithms and that using our Rényi entropy rate improves the finite-size key rate to considering the smooth min-entropy rate, at least in the current proof method. We next considered the high-dimensional two mutually unbiased bases protocols which exemplified an improvement in the key rate over the postselection technique [15], an alternative proof method for coherent-attack security which is limited in how it scales with respect to the dimension of Alice and Bob's quantum states. This confirms that there is a regime in which the postselection technique is "loose", further suggesting the importance of the application of the EAT. Lastly, we demonstrate our method for an optical implementation. This example demonstrates that our method is also applicable to practical protocols instead of restricting to theoretically simple ones. On the other hand, due to unsatisfactory results in small block sizes, we also observe that the EAT currently appears to require more improvements in handling loss and noise in order to have good key rates for experimentally feasible block sizes.

Given these results, it is natural to consider where improvements might be made or further avenues to explore. First and foremost, we note that we were restricted to considering entanglement-based protocols, as we need the entanglement-based protocol framework to use our algorithms. In previous work [42], this has not been limiting as we could use the source-replacement scheme [53, 33] to convert prepare-and-measure protocols to entanglement-based ones. However, it is not clear how the source-replacement scheme interacts with the Markov chain requirements for EAT. This has been partially resolved in concurrent work [24, 25]. Second, we have seen that while the EAT scales well in terms of the dimension of the states, it seems limited by loss and noise. In particular, the ability to handling high loss parameter regime is of particular interest for realistic implementations. As such, a natural question is whether the EAT can be more robust to loss and noise, at least in the device-dependent setting. We note follow-up work [54] has numerical results that show the (generalised) EAT scales worse in loss than for i.i.d. collective attacks. This mathematically makes sense as coherent attacks are more general. However, to the best of our knowledge, no example of such an attack separating the cases is known, so an optimistic researcher could still hope for further improvements.

Acknowledgments

References

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE. DOI: https://doi.org/10.1016/j.tcs.2014.05.025.

[2] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6): 661, 1991. DOI: https://doi.org/10.1103/PhysRevLett.67.661.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301, 2009. DOI: https://doi.org/10.1103/RevModPhys.81.1301.

[4] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92(2):025002, 2020. DOI: https://doi.org/10.1103/RevModPhys.92.025002.

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12:1012–1236, 2020. DOI: https://doi.org/10.1364/AOP.361502.

[6] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121(19):190502, 2018. DOI: https://doi.org/10.1103/PhysRevLett.121.190502.

[7] Xiao-Tian Fang, Pei Zeng, Hui Liu, Mi Zou, Weijie Wu, Yan-Lin Tang, Ying-Jie Sheng, Yao Xiang, Weijun Zhang, Hao Li, Zhen Wang, Lixing You, Hao Chen Ming-Jun Li, Yu-Ao Chen, Qiang Zhang, Cheng-Zhi Peng, Xiongfeng Ma, Teng-Yun Chen, and Jian-Wei Pan. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics*, 14(7):422–425, 2020. DOI: https://doi.org/10.1038/s41566-020-0599-8.

[8] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017. DOI: https://doi.org/10.1038/nature23655.

[9] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Inf.*, 3(1):1–13, 2017. DOI: https://doi.org/10.1038/s41534-017-0031-5.

[10] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson. Chip-based quantum key distribution. *Nat. Commun.*, 8(1):13984, 2017. DOI: https://doi.org/10.1038/ncomms13984.

[11] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S Yu, J Wu, W. Ser, L. C. Kwek, and A. Q. Liu. An integrated silicon photonic chip

platform for continuous-variable quantum key distribution. *Nat. Photonics*, 13(12):839–842, 2019. DOI: https://doi.org/10.1038/s41566-019-0504-5.

[12] Kejin Wei, Wei Li, Hao Tan, Yang Li, Hao Min, Wei-Jun Zhang, Hao Li, Lixing You, Zhen Wang, Xiao Jiang, Teng-Yun Chen, Sheng-Kai Liao, Cheng-Zhi Peng, Feihu Xu, and Jian-Wei Pan. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X*, 10(3):031030, 2020. DOI: https://doi.org/10.1103/PhysRevX.10.031030.

[13] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Inforemation*, 6:1–127, 2005. DOI: https://doi.org/10.1142/S0219749908003256.

[14] Valerio Scarani and Renato Renner. Security bounds for quantum cryptography with finite resources. In Y. Kawano and M. Mosca, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 85–95, Berlin, Heidelberg, 2008. Springer. DOI: https://doi.org/10.1007/978-3-540-89304-2˙8.

[15] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, 2009. DOI: https://doi.org/10.1103/PhysRevLett.102.020504.

[16] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Commun. Math. Phys.*, 379:867–913, 2020. DOI: https://doi.org/10.1007/s00220-020-03839-5.

[17] Frédéric Dupuis and Omar Fawzi. Entropy accumulation with improved second-order term. *IEEE Trans. Inf. Theory*, 65:7596–7612, 2019. DOI: https://doi.org/10.1109/TIT.2019.2929564.

[18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications*, 9(1):459, 2018. DOI: https://doi.org/10.1038/s41467-017-02307-4.

[19] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *SIAM J. Comput.*, 48(1):181–225, 2019. DOI: https://doi.org/10.1137/18M1174726.

[20] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J-D. Bancal. Experimental quantum key distribution certified by bell's theorem. *Nature*, 607:682–686, 2022. DOI: https://doi.org/10.1038/s41586-022-04941-5.

[21] Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff, Rene Schwonnek, Florian Fertig, Sebastian Eppelt, Valerio Scarani, Charles C. W. Lim, and Harald Weinfurter. A device-independent quantum key distribution system for distant users. *Nature*, 607:687–691, 2022. DOI: https://doi.org/10.1038/s41586-022-04891-y.

[22] Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, Ming-Han Li, Yang Liu, Jingyun Fan, Feihu Xu, Qiang Zhang, and Jian-Wei Pan. Toward a photonic demonstration of device-independent quantum key distribution. *Phys. Rev. Lett.*, 129:050502, Jul 2022. DOI: https://doi.org/10.1103/PhysRevLett.129.050502.

[23] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110:010503, Jan 2013. DOI: https://doi.org/10.1103/PhysRevLett.110.010503.

[24] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, page 844–850. IEEE, oct 2022. DOI: https://doi.org/10.1109/focs54457.2022.00085.

[25] Tony Metger and Renato Renner. Security of quantum key distribution from generalised

entropy accumulation. *Nature Communications*, 14(1), August 2023. ISSN 2041-1723. DOI: https://doi.org/10.1038/s41467-023-40920-8.

[26] Peter Brown, Hamza Fawzi, and Omar Fawzi. Computing conditional entropies for quantum correlations. *Nat. Commun.*, 12:575, 2021. DOI: https://doi.org/10.1038/s41467-020-20018-1.

[27] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nat. Commun.*, 7:11712, 2016. DOI: https://doi.org/10.1038/ncomms11712.

[28] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77, 2018. DOI: https://doi.org/10.22331/q-2018-07-26-77.

[29] Frédéric Dupuis. Privacy amplification and decoupling without smoothing. *IEEE Transactions on Information Theory*, 69(12):7784–7792, 2023. DOI: https://doi.org/10.1109/TIT.2023.3301812.

[30] Silvestre Abruzzo, Hermann Kampermann, Markus Mertz, and Dagmar Bruß. Quantum key distribution with finite resources: Secret key rates via Rényi entropies. *Physical Review A*, 84(3), September 2011. ISSN 1094-1622. DOI: https://doi.org/10.1103/physreva.84.032321.

[31] Masahito Hayashi. Large deviation analysis for quantum security via smoothing of Rényi entropy of order 2. *IEEE Transactions on Information Theory*, 60(10):6702–6732, October 2014. ISSN 1557-9654. DOI: https://doi.org/10.1109/TIT.2014.2337884.

[32] Ramy Tannous, Zhangdong Ye, Jeongwan Jin, Katanya B. Kuntz, Norbert Lütkenhaus, and Thomas Jennewein. Demonstration of a 6 state-4 state reference frame independent channel for quantum key distribution. *Appl. Phys. Lett.*, 115:211103, 2019. DOI: https://doi.org/10.1063/1.5125700.

[33] Agnes Ferenczi and Norbert Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85:052310, 2012. DOI: https://doi.org/10.1103/PhysRevA.85.052310.

[34] Marco Tomamichel. *Quantum Information Processing with Finite Resources*. Springer International Publishing, 2016. DOI: https://doi.org/10.1007/978-3-319-21891-5. All equation numbers and theorem numbers cited in this work refer to the fourth arXiv version of this cited work: `https://arxiv.org/abs/1504.00233v4`.

[35] Marco Tomamichel. *A Framework for Non-Asymptotic Quantum Infomration Theory*. PhD thesis, ETH Zürich, Zürich, Switzerland, 2012. URL `https://arxiv.org/abs/1203.2142`.

[36] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*, 2014. DOI: https://doi.org/10.48550/arXiv.1409.3525.

[37] David Sutter. Approximate quantum Markov chains. In *Approximate Quantum Markov Chains*, pages 75–100. Springer, 2018. DOI: https://doi.org/10.1007/978-3-319-78732-9_5.

[38] Igor Devetak and Andreas Winter. Distillation of secret key entanglement from quantum states. *Proc. R. Soc. A*, 461:207–235, 2005. DOI: https://doi.org/10.1098/rspa.2004.1372.

[39] Rotem Arnon-Friedman. *Device-Independent Quantum Information Processing: A Simplified Analysis*. Springer Nature, 2020. DOI: https://doi.org/10.1007/978-3-030-60231-4.

[40] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory, Second Edition*. John Wiley & Sons, 2005. ISBN 0471241954. DOI: https://doi.org/10.1002/047174882X.

[41] Ian George. Numerical finite key analysis. Master's thesis, University of Waterloo, 2020.

[42] Ian George, Jie Lin, and Norbert Lütkenhaus. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Phys. Rev. Research*, 3:013274, 2021. DOI: https://doi.org/10.1103/PhysRevResearch.3.013274.

[43] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, Cambridge, UK, 2018. ISBN 1107180562. DOI: https://doi.org/10.1017/9781316848142.

[44] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.*, 18:133–165, 2005. DOI: https://doi.org/10.1007/s00145-004-0142-y.

[45] Anthony Laing, Valerio Scarani, John G. Rarity, and Jeremy L. O'Brien. Reference-frame-independent quantum key distribution. *Phys. Rev. A*, 82(3):012304, 2010. DOI: https://doi.org/10.1103/PhysRevA.82.012304.

[46] Barbara Kraus, Nicolas Gisin, and Renato Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501, 2005. DOI: https://doi.org/10.1103/PhysRevLett.95.080501.

[47] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332, 2005. DOI: https://doi.org/10.1103/PhysRevA.72.012332.

[48] Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82(3):030301(R), 2010. DOI: https://doi.org/10.1103/PhysRevA.82.030301.

[49] Pieter Kok and Samuel L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61(4):042304, 2000. DOI: https://doi.org/10.1103/PhysRevA.61.042304.

[50] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, 2007. DOI: https://doi.org/10.1103/PhysRevA.76.012307.

[51] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008. DOI: https://doi.org/10.1103/PhysRevLett.101.093601.

[52] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus. Squashing models for detectors and applications to quantum key distribution protocols. *Phys. Rev. A*, 89:012325, 2014. DOI: https://doi.org/10.1103/PhysRevA.89.012325.

[53] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004. DOI: https://doi.org/10.1103/PhysRevLett.92.217903.

[54] Lars Kamin, Amir Arqand, Ian George, Norbert 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, Jun 2025. DOI: https://doi.org/10.1103/PRXQuantum.6.020342.

[55] Frédéric Dupuis. Chain rules for quantum Rényi entropies. *Journal of Mathematical Physics*, 56(2):022203, 2015. DOI: https://doi.org/10.1063/1.4907981.

[56] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017. DOI: https://doi.org/10.22331/q-2017-07-14-14.

[57] Dan Romik. Stirling's approximation for n!: the ultimate short proof? *The American Mathematical Monthly*, 107(6):556–557, 2000. DOI: https://doi.org/10.1080/00029890.2000.12005235.

[58] Jonathan Borwein and Adrian S. Lewis. *Convex Analysis and Nonlinear Optimization: Theory and Examples*. Springer-Verlag, New York, USA, 2006. DOI: https://doi.org/10.1007/978-0-387-31256-9.

A A Sufficient Condition for the Markov Chain Condition

In this section, we prove Theorem 2 from the main text which gives sufficient conditions for ensuring the Markov chain conditions hold on the optimal attack. We note the statement in this section (Proposition 5) includes an additional equivalent condition which is quick to verify and so may be of use.

Recall that we consider EAT channels with a special tensor product structure. We consider n CPTP maps $\widetilde{\mathcal{M}}_i : Q_i \to S_i P_i X_i$ acting in tensor product on the n independent systems $\{Q_i\}_i$. The maps are defined by the POVM $\{M_{sp}\}$ such that

$$\widetilde{\mathcal{M}}_i(\rho) = \sum_{s,p} \mathrm{Tr}[\rho M_{sp}] |s,p\rangle\langle s,p|_{S_i P_i} \otimes |t(s,p)\rangle\langle t(s,p)|_{X_i} . \tag{71}$$

From these we define the corresponding EAT channels $\mathcal{M}_i : R_{i-1} \to R_i S_i P_i X_i$ acting on the quantum systems $R_i = Q_{i+1}^n$, as $\mathcal{M}_i = \widetilde{\mathcal{M}}_i \otimes \mathcal{I}_{Q_{i+1}^n}$ (see main text for further details). In this case, it is simple to prove that the output state of the protocol $\rho_{S_1^n P_1^n X_1^n E} = \mathcal{M}_1 \circ \cdots \circ \mathcal{M}_n \otimes \mathcal{I}_E(\rho_{R_0 E})$ takes on the simple form

$$\rho_{S_1^n P_1^n X_1^n E} = \bigotimes_{i=1}^n \widetilde{\mathcal{M}}_i \otimes \mathcal{I}_E(\rho_{Q_1^n E}) \tag{72}$$

where $R_0 = Q_1^n$.

We now want to prove the following proposition.

Proposition 5. *Let $\{M_{sp} : s \in \mathcal{S}, p \in \mathcal{P}\}$ be the POVM associated to a given quantum-to-classical CPTP map $\widetilde{\mathcal{M}}_i : Q_i \to S_i P_i X_i$ and let $M_p := \sum_s M_{sp}$ correspond to the POVM elements of the map $\mathrm{Tr}_{S_i X_i} \circ \widetilde{\mathcal{M}}_i : Q_i \to P_i$. If either condition (A) or condition (B) below holds for each CPTP map $\widetilde{\mathcal{M}}_i$, then without loss of generality the optimal attack by an eavesdropper is of a block-diagonal form such that the Markov chain conditions, Eq. (8), hold and so the EAT may be applied (Theorem 1).*

(A) *There exists a decomposition $Q_i = \bigoplus_\lambda V^\lambda$ of the space Q_i into orthogonal subspaces $\{V^\lambda\}_\lambda$ such that*

   (1) *For all $(s,p) \in \mathcal{S} \times \mathcal{P}$, M_{sp} is block diagonal: $M_{sp} = \bigoplus_\lambda M_{sp}^{(\lambda)}$, where $M_{sp}^{(\lambda)}$ acts on the subspace V^λ.*

   (2) *For all $p \in \mathcal{P}$, M_p is block diagonal and proportional to the identity in each subspace: there exist constants $m_p^\lambda \in [0,1]$ such that $M_p = \bigoplus_\lambda m_p^\lambda \mathbb{1}_{V^\lambda}$, where $\mathbb{1}_{V^\lambda}$ is the identity operator on V^λ.*

(B) *For all $s \in \mathcal{S}$, $p, p' \in \mathcal{P}$, M_{sp} and $M_{p'}$ commute: $[M_{sp}, M_{p'}] = 0$.*

Furthermore, (A) and (B) are equivalent.

Remark 13. The statement of Theorem 2 just states condition (A) in Proposition 5 under the name of 'weakly dependent' (Definition 3), which is of primary interest. While equivalent, condition (B) is stated here as it could be of use when one knows the measurement operators, as it is then easy to check condition (B) to determine if Proposition 5 may be applied.

One way to prove the EAT theorem applies under condition (A) or condition (B) would be to show the output state in Eq. (72) satisfies the Markov chain conditions, but this does not work in general. Instead, we show that we can assume the initial state is of a certain block diagonal form without loss of generality due to the block diagonal structure of the EAT channels (Lemma 1).

Then we show that this block diagonal form satisfies the Markov chain conditions (Proof of Proposition 5), and, as assuming this form was without loss of generality, this is sufficient. The reduction to a quantum state with block-diagonal structure is well-known in discrete-variable QKD where the measurement operators that model single-photon detectors are block diagonal in the total photon number basis. In such a setting, this block diagonal structure implies Eve's optimal attack includes implementing a QND measurement on the total number of photons before sending out the states, thereby resulting in the state being block-diagonal without loss of generality. One may view Lemma 1 and Proposition 5 as a generalization of such a method, but with the further insight that such structure implies the Markov chain conditions hold.

Lemma 1. *Let each $\widetilde{\mathcal{M}}_i$ be a quantum-to-classical CPTP map whose associated POVM elements are block diagonal; i.e., for each i there exists a decomposition $Q_i = \bigoplus_\lambda V^\lambda$ such that $M_{sp} = \bigoplus_\lambda M_{sp}^{(\lambda)}$ with $M_{sp}^{(\lambda)}$ acting on V^λ. Then for any initial state $\rho_{Q_1^n E}$, there exists another state $\nu_{Q_1^n E'}$ such that*

(1) the state $\nu_{Q_1^n E'}$ has the block diagonal form

$$\nu_{Q_1^n E \Lambda_1^n} = \sum_{\boldsymbol{\lambda}=(\lambda_1,\cdots\lambda_n)} \rho_{Q_1^n E}(\boldsymbol{\lambda}) \otimes |\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda}|_{\Lambda_1^n} , \tag{73}$$

where Eve's registers $E' = (E, \Lambda_1, \cdots \Lambda_n)$ are composed of a quantum memory E and n classical registers Λ_i indicating the subspace, so that, for all $\boldsymbol{\lambda}$, the state $\mathrm{Tr}_E[\rho_{Q_1^n E}(\boldsymbol{\lambda})]$ is defined on $V^{\boldsymbol{\lambda}} := \bigotimes_i V^{\lambda_i}$, and

(2) the output states $\nu_{S_1^n P_1^n X_1^n E'}$ and $\rho_{S_1^n P_1^n X_1^n E}$ are related by

$$\mathrm{Tr}_{\Lambda_1^n}[\nu_{S_1^n P_1^n X_1^n E \Lambda_1^n}] = \rho_{S_1^n P_1^n X_1^n E} . \tag{74}$$

Proof. To construct the state $\nu_{Q_1^n E'}$ from the state $\rho_{Q_1^n E}$, we consider the dephasing map $\Delta_i : Q_i \to Q_i \Lambda_i$

$$\Delta_i(\rho) = \sum_\lambda P_\lambda \rho P_\lambda \otimes |\lambda\rangle\langle\lambda|_{\Lambda_i} , \tag{75}$$

where P_λ is a projector on the subspace V^λ. This map Δ_i projects the state onto each subspace V^λ without affecting the coherence inside the subspace V^λ and writes the result in Λ_i. We then define $\nu_{Q_1^n E'} := \nu_{Q_1^n E \Lambda_1^n} := \left(\bigotimes_i \Delta_i \otimes \mathcal{I}_E\right)(\rho_{Q_1^n E})$. The state $\nu_{Q_1^n E \Lambda_1^n}$ is indeed of the form Eq. (73), as required.

Because of the block diagonal structure of the maps $\widetilde{\mathcal{M}}_i$, it is simple to see that the dephasing map does not affect the measurement statistics. We can observe that the maps Δ_i and $\widetilde{\mathcal{M}}_i$ are related by $\mathrm{Tr}_{\Lambda_i} \circ \widetilde{\mathcal{M}}_i \circ \Delta_i = \widetilde{\mathcal{M}}_i \circ \mathrm{Tr}_{\Lambda_i} \circ \Delta_i = \widetilde{\mathcal{M}}_i$. Consequently, we have

$$\mathrm{Tr}_{\Lambda_1^n}[\nu_{S_1^n P_1^n X_1^n E \Lambda_1^n}] = \mathrm{Tr}_{\Lambda_1^n} \circ \left(\bigotimes_i \widetilde{\mathcal{M}}_i \otimes \mathcal{I}_{E\Lambda_1^n}\right) \circ \left(\bigotimes_i \Delta_i \otimes \mathcal{I}_E\right)(\rho_{Q_1^n E}) \tag{76}$$

$$= \left(\bigotimes_i \widetilde{\mathcal{M}}_i \otimes \mathcal{I}_E\right)(\rho_{Q_1^n E}) \tag{77}$$

$$=: \rho_{S_1^n P_1^n X_1^n E}. \tag{78}$$

$\square$

Proof of Proposition 5. Let $\rho_{Q_1^n E}$ be some initial state used in the EAT (Theorem 1). We assume that the maps $\widetilde{\mathcal{M}}_i$ satisfy the condition (A) instead of the Markov chain conditions. Let us show that the Markov chain conditions follow from this condition.

Using the block diagonal structure of condition (A), we can use Lemma 1 to show that there exists a block diagonal state $\nu_{Q_1^n E'}$ with the same passing probability $\nu[\Omega] = \rho[\Omega]$, which satisfies $H_{\min}^{\epsilon}(S_i^n|P_i^n E)_{\rho_{|\Omega}} \geq H_{\min}^{\epsilon}(S_i^n|\tilde{P}_i^n E')_{\nu_{|\Omega}}$. Indeed, this follows by using Eq. (74) and the strong subadditivity of smooth min-entropies. We conclude that whatever min-entropy lower-bound statement holds for $\nu_{Q_1^n E'}$ must also hold for $\rho_{Q_1^n E}$.

To prove Proposition 5, we then show that the new state $\nu_{Q_1^n E}$ satisfies the Markov chain conditions in Eq. (8). We can do this by showing that given the state $\nu_{S_1^{i-1} P_1^{i-1} E'}$, there exists a recovery map $\mathcal{R}_{P_i E \leftarrow E'}$ which acts on Eve's registers $E' = (E, \Lambda_1^n)$ and recovers the register P_i, i.e., $\mathcal{R}(\nu_{S_1^{i-1} P_1^{i-1} E'}) = \nu_{S_1^{i-1} P_1^i E}$. Since the POVM elements M_p are proportional to the identity in every subspace V^λ, the probability distribution of P_i only depends on the subspace V^λ, which is indicated in Eve's register Λ_i. This means the variable P_i can therefore be recovered from Λ_i by simply generating it with the distribution $\Pr_P(p|\lambda) = m_p^\lambda$. Moreover, as we have shown the Markov chain conditions for $\nu_{Q_1^n E}$ and without loss of generality, Eve can only do better using a state of the form ν, we can conclude we may use the EAT (Theorem 1) to prove security.

Having shown that the Markov chain conditions follow from condition (A), it remains to show that (A) and (B) are equivalent. To do so, we first note that the commutation relation $[M_{sp}, M_{p'}] = 0$ in condition (B) is a direct consequence of the block diagonal conditions in (A). Conversely, we note that by construction the POVM elements M_p's are linear combinations of the measurement operators M_{sp}'s. Therefore, the commutation relation in condition (B) implies the commutation relation $[M_p, M_{p'}] = 0$ for all $p, p' \in \mathcal{P}$. This consequently implies the existence of a joint basis that simultaneously diagonalizes the operators M_p's. We can thus find an orthogonal decomposition V^λ so that $M_p = \bigoplus_\lambda m_p^\lambda \mathbb{1}_{V^\lambda}$. Using the commutation relation in condition (B) a second time implies that the operators M_{sp} must be block diagonal along the same subspaces V^λ's. $\qquad \square$

Remark 14. We note this proof does not change for Rényi entropies as they also satisfy strong subadditivity.

B Security of QKD using EAT without Smoothing

In this appendix, we present the necessary technical lemmas and the resulting proof for Theorem 5. The primary tool is Dupuis' recent result on applying privacy amplification without smoothing [29]. However, we will also need to prove a max-tradeoff function upper bound on $H_\alpha^\uparrow(S_1^n|P_1^n E)_{\rho_{|\Omega}}$. We note that in the original work [16] a max-tradeoff function upper bound for $H_\alpha^\uparrow$ is implied to be straightforward given the max-tradeoff result presented in said work and simply not presented because upper bounding an alternative entropy will result in a tighter bound on $H_{\max}^\varepsilon$ [16, Footnote 13]. For completeness, we present our proof of such a bound. Throughout this appendix we present results using the Greek letters $(\alpha, \beta, ...)$ that will be ultimately used in our key length security result rather than always using α for the Rényi entropy, so that it is easier to see how the results combine. We refer to Section 2.1 for a summary of common notations. We do however use A_i and B_i rather than S_i and P_i respectively from the main text.

B.1 Background Rényi divergence results

Here we present the special cases of the Rényi entropy chain rules which we will need in this section. We refer to Section 2.1 for basic entropic notation used in this work.

Theorem 7 ([55, Theorem 1]). *Let* $\rho_{ABC} \in \mathrm{D}(ABC)$, $\tau_C \in \mathrm{D}(C)$, $\alpha, \beta, \gamma \in (1/2, 1) \cup (1, \infty)$ *such that* $\frac{\alpha}{\alpha-1} = \frac{\beta}{\beta-1} + \frac{\gamma}{\gamma-1}$.

1. *Case 1: If* $(\alpha - 1)(\beta - 1)(\gamma - 1) > 0$, $\quad H_\beta^\uparrow(A|BC)_\rho \leq H_\alpha(\rho_{ABC}||\tau_C) - H_\gamma(\rho_{BC}||\tau_C)$.

2. *Case 2: If* $(\alpha - 1)(\beta - 1)(\gamma - 1) < 0$, $\quad H_\alpha(\rho_{ABC}||\tau_C) \leq H_\beta^\uparrow(A|BC)_\rho + H_\gamma(\rho_{BC}||\tau_C)$.

Remark 15. In Ref. [55], the result is presented with the product $(\alpha - 1)(\beta - 1)(\gamma - 1)$ to be bounded by one rather than zero. If one checks the conditions used to derive the theorem ([55, Propositions 7 and 8]), it only depends on the sign of the product. This has been realized in previous works, e.g. [34].

Corollary 8 (Special Cases of Chain Rules). Let $\rho_{ABC} \in \mathrm{D}(ABC)$, $\tau_C \in \mathrm{D}(C)$. Let $\alpha, \beta, \delta, \eta, \gamma, \zeta \in (1/2, 1) \cup (1, \infty)$.

1. Let $(\eta - 1)(\delta - 1)(\zeta - 1) > 0$, $\frac{\eta}{\eta - 1} = \frac{\delta}{\delta - 1} + \frac{\zeta}{\zeta - 1}$ and B be a trivial (one-dimensional) register. Then $H_\delta^\uparrow(A|C)_\rho \leq H_\eta(\rho_{AC}||\tau_C) + D_\zeta(\rho_C||\tau_C)$.

2. Let $(\alpha - 1)(\beta - 1)(\delta - 1) < 0$ and $\frac{\beta}{\beta - 1} = \frac{\alpha}{\alpha - 1} + \frac{\delta}{\delta - 1}$. Then $H_\beta^\uparrow(AB|C)_\rho \leq H_\alpha^\uparrow(A|BC)_\rho + H_\delta^\uparrow(B|C)_\rho$.

Proof. Item 1 follows from Item 1 of Theorem 7 by noting if B is trivial, the B register may be dropped. Because $H_\gamma(\rho_{BC}||\tau_C) = -D_\gamma(\rho_C|| \mathbb{1}_\mathbb{C} \otimes \tau_C)$, the negative signs cancel. Dropping the register B and setting $\beta \to \delta$, $\alpha \to \eta$, and $\gamma \to \zeta$ completes the proof. Item 2 follows from Item 2 of Theorem 7 by letting τ_C be the optimizer for $H_\alpha^\uparrow(AB|C)_\rho$. Then by definition, $H_\gamma^\uparrow(B|C)_\rho \geq H_\gamma(\rho_{BC}||\tau_C)$. Relabeling by $\alpha \to \beta$, $\beta \to \alpha$, $\gamma \to \delta$ completes the proof. $\qquad \square$

B.2 Applying privacy amplification without smoothing

In Ref. [29], it was shown that privacy amplification could be performed without smoothing. While it was stated as holding for strongly 2-universal hashing functions, it is straightforward to show that the proof is the same for a general family of 2-universal hash functions. Recall that a family of 2-universal hash functions is the pair $(p_F, \mathcal{F})$ where $\mathcal{F}$ is a set of functions from discrete alphabet $\mathcal{X}$ to discrete alphabet $\mathcal{Z}$ and p_f is a probability distribution over $\mathcal{F}$ such that $\Pr_f[f(x) = f(x')] \leq |\mathcal{Z}|^{-1}$ for all $x \neq x' \in \mathcal{X}$. Altering notation to better fit for our purposes, Theorem 8 of Ref. [29] is in terms of $\mathbb{E}_{f \in \mathcal{F}} \left\| \rho_{ZE}^f - \frac{1}{|\{0,1\}^\ell|} \mathbb{1}_Z \otimes \rho_E \right\|_1$ where ρ_{ZE}^f is ρ_{XE} after the hash function f has been applied to register X and $\mathcal{Z} = \{0,1\}^\ell$. Using that announcing the choice of hash function $f \in \mathcal{F}$ will make the state block diagonal in the register F that stores this announcement, it is clear that

$$\|\rho_{ZEF} - \frac{1}{|\{0,1\}^\ell|} \mathbb{1}_Z \otimes \rho_{EF}\|_1 = \sum_f p(f) \|\rho_{ZE}^f - \frac{1}{|\{0,1\}^\ell|} \mathbb{1}_Z \otimes \rho_E\|_1$$

$$= \mathbb{E}_f \|\rho_{ZE}^f - \frac{1}{|\{0,1\}^\ell|} \mathbb{1}_Z \otimes \rho_E\|_1 ,$$

so we state the result in the fashion more commonly used in QKD.

Proposition 6 (Special Case of [29, Theorem 8]). *Let* $\rho_{XE} \in \mathrm{D}(XE)$ *be a classical-quantum state where* $X \cong \mathbb{C}^{|\mathcal{X}|}$ *where* $\mathcal{X}$ *is some finite set. Let* $(p_f, \mathcal{F})$ *be a family of two-universal hash functions from* $\mathcal{X} \to \mathcal{Z}$ *and* $\mathcal{Z} = \{0,1\}^\ell$. *Let* $\alpha \in (1, 2)$. *Then*

$$\left\| \rho_{ZEF} - \frac{1}{|\{0,1\}^\ell|} \mathbb{1}_Z \otimes \rho_{EF} \right\|_1 \leq 2^{\frac{2}{\alpha} - 1} \cdot 2^{\frac{1-\alpha}{\alpha} \left(H_\alpha^\uparrow(X|E)_\rho - \ell \right)} ,$$

where F *is the register storing the announcement of the hash function.*

51

From this we obtain the following corollary immediately.

Corollary 9. Let $\rho_{XE|\Omega} \in D(XE)$ be a classical-quantum state. Let $\varepsilon_{sec} := \frac{1}{2} \cdot 2^{\frac{2}{\alpha}-1} \cdot 2^{\frac{1-\alpha}{\alpha}\left(H_\alpha^\uparrow(X|E)_\rho - \ell\right)}$ where $\alpha \in (1,2)$. Then for an ε_{sec}-secret key, the length of the key, ℓ, must satisfy the following bound:

$$\ell \leq H_\alpha^\uparrow(X|E)_\rho - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\varepsilon_{sec}}\right) + 2 .$$

Proof. Starting from how we defined ε_{sec}:

$$\varepsilon_{sec} \leq 2^{\frac{2}{\alpha}-2} \cdot 2^{\frac{1-\alpha}{\alpha}\left(H_\alpha^\uparrow(X|E)_\rho - \ell\right)}$$

$$\Rightarrow \log(\varepsilon_{sec}) \leq \frac{2}{\alpha} - 2 + \frac{1-\alpha}{\alpha}\left(H_\alpha^\uparrow(X|E)_\rho - \ell\right)$$

$$\Rightarrow \frac{1-\alpha}{\alpha}\ell \leq \frac{2}{\alpha} - 2 + \frac{1-\alpha}{\alpha}H_\alpha^\uparrow(X|E)_\rho + \log\left(\frac{1}{\varepsilon_{sec}}\right)$$

$$\Rightarrow \ell \leq H_\alpha^\uparrow(X|E)_\rho + \frac{\alpha}{1-\alpha}\log\left(\frac{1}{\varepsilon_{sec}}\right) + 2 .$$

Pulling a negative sign out of the $\frac{\alpha}{1-\alpha}$ term completes the proof. $\square$

Remark 16. Note we added the $\frac{1}{2}$ term in defining ε_{sec} because trace distance should be divided by two for the operational interpretation.

B.3 Entropy Accumulation Theorem for upper bound on $H_\delta^\uparrow$

In this section we prove an upper bound on $H_\delta^\uparrow$ in terms of a max-tradeoff function. While almost all of the work is done by [16], we split it into two pieces as we will need to use a chain rule and also as it allows us to specify what results of [16] we use at each step. As explained earlier, this result is implied to be expected to exist in some form in [16, Footnote 13]. We present it in its entirety for rigour.

As we switched the secret and public register notation, we emphasize in the current notation the Markov conditions are:

$$A_1^{i-1} \leftrightarrow B_1^{i-1}E \leftrightarrow B_i \qquad \forall i \in \{1,\ldots,n\} . \tag{79}$$

We proceed by using the original entropy price function which we know is sub-optimal in the second-order terms, but that will not matter for our purposes. For every i, we use a CPTP map $\mathcal{D}_i : X_i \to X_i D_i \overline{D}_i$

$$\mathcal{D}_i(W_{X_i}) = \sum_{x \in \mathcal{X}} \langle x| W_{X_i} |x\rangle |x\rangle\langle x| \otimes \tau(x)_{D_i\overline{D}_i} ,$$

where $\tau(x)_{D_i\overline{D}_i}$ is such that $H(D_i|\overline{D}_i)_{\tau(x)} = \overline{g} - f(\delta_x)$, f is a min-tradeoff function, $[g_{\min}, g_{\max}]$ is the smallest real interval containing $f(\mathbb{P}(\mathcal{X}))$ and $\overline{g} := (g_{\min} + g_{\max})/2$. This is possible by letting $\tau(x)_{D_i\overline{D}_i}$ be a mixture of the maximally entangled state and the maximally mixed state. Following the argument from [16, Beginning of Proof of Proposition 4.5], this can be done if $|D_i| \leq \exp(\lceil \|\nabla f\|_\infty \rceil)$. We also note the general definition $\overline{\rho} := (\mathcal{D}_n \circ \ldots \circ \mathcal{D}_1)(\rho)$. With all of this specified, we begin with our equivalent of Claim 4.6 of [16].

Lemma 2. *Let $\delta \in [1/2, \infty)$. Assuming the Markov chain conditions are satisfied [Eq. (79)], then*

$$H_\delta^\uparrow(A_1^n|B_1^nE)_{\rho_{|\Omega}} \leq H_\delta^\uparrow(A_1^nD_1^n|B_1^nE\overline{D}_1^n)_{\overline{\rho}_{|\Omega}} + nh - n\overline{g} ,$$

where $h \in \mathbb{R}$ that satisfies the conditions assumed in Theorem 1 and $\overline{g}$ is as defined above.

Proof. First note that

$$\overline{\rho}_{A_1^n X_1^n B_1^n E \overline{D}_1^n | \Omega} = \frac{1}{\rho[\Omega]} \sum_{x_1^n \in \Omega} |x_1^n\rangle\langle x_1^n| \otimes \rho_{A_1^n B_1^n E, x_1^n} \otimes \mathrm{Tr}_{D_1^n}(\tau(x_1^n)_{D_1^n \overline{D}_1^n}) \ .$$

Note that $\mathrm{Tr}_{D_i}(\tau(x_i)_{D_i \overline{D}_i}) = \frac{1}{|D_i|} \mathbb{1}_{\overline{D}_i}$ for all i and x_i because $\tau(x_i)$ is a mixture of the maximally mixed and maximally entangled state. It follows we know that register is independent of the rest of the registers and that

$$\overline{\rho}_{A_1^n X_1^n B_1^n E \overline{D}_1^n | \Omega} = \frac{1}{\rho[\Omega]} \sum_{x_1^n \in \Omega} |x_1^n\rangle\langle x_1^n| \otimes \rho_{A_1^n B_1^n E, x_1^n} \otimes \overline{\rho}_{\overline{D}_1^n} \ . \tag{80}$$

It follows the state is invariant under tracing off $\overline{\rho}_{\overline{D}_1^n}$ and re-appending it. Denote this map $\mathcal{R}$. By data-processing,

$$-D_\delta(\rho_{A_1^n X_1^n B_1^n E \overline{D}_1^n} || \mathbb{1}_{A_1^n X_1^n} \otimes \sigma_{B_1^n E \overline{D}_1^n})_{\overline{\rho}_{|\Omega}} \leq -D_\delta(\mathcal{R}(\rho_{A_1^n X_1^n B_1^n E \overline{D}_1^n}) || \mathcal{R}(\mathbb{1}_{A_1^n X_1^n} \otimes \sigma_{B_1^n E \overline{D}_1^n}))_{\overline{\rho}_{|\Omega}}$$
$$= -D_\delta(\rho_{A_1^n X_1^n B_1^n E \overline{D}_1^n} || \mathbb{1}_{A_1^n X_1^n} \otimes \overline{\sigma}_{B_1^n E \overline{D}_1^n})_{\overline{\rho}_{|\Omega}} \ , \tag{81}$$

where $\overline{\sigma}_{B_1^n E \overline{D}_1^n} = \sigma_{B_1^n E} \otimes \overline{\rho}_{\overline{D}_1^n}$. This implies that $H_\delta^\uparrow(A_1^n X_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}}$ is obtained by a maximizer of the form $\overline{\sigma}_{B_1^n E \overline{D}_1^n}$.

Next we recall Lemma 3.1 of [16] (with terms moved around):

$$-D_\delta(\rho_{A_1 B} || \mathbb{1}_{A_1} \otimes \sigma_B) + H_\delta(A_2 | A_1 B)_\nu = -D_\delta(\rho_{A_1 A_2 B} || \mathbb{1}_{A_1 A_2} \otimes \sigma_B) \ ,$$

for any σ_B where

$$\nu_{A_1 A_2 B} = \nu_{A_1 B}^{\frac{1}{2}} \rho_{A_2 | A_1 B} \nu_{A_1 B}^{\frac{1}{2}} \quad \text{where} \quad \nu_{A_1 B} = \frac{\left(\rho_{A_1 B}^{\frac{1}{2}} \sigma_B^{\frac{1-\alpha}{\alpha}} \rho_{A_1 B}^{\frac{1}{2}}\right)^\alpha}{\mathrm{tr}\left(\rho_{A_1 B}^{\frac{1}{2}} \sigma_B^{\frac{1-\alpha}{\alpha}} \rho_{A_1 B}^{\frac{1}{2}}\right)^\alpha} \ .$$

Making the substitutions $A_1 = A_1^n X_1^n$, $A_2 = D_1^n$, $B = B_1^n E \overline{D}_1^n$ and letting $\sigma = \overline{\sigma}_{B_1^n E \overline{D}_1^n}$ be the optimizer of $H_\delta^\uparrow(A_1^n X_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}}$, we obtain

$$H_\delta^\uparrow(A_1^n X_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}} + H_\delta(D_1^n | A_1^n X_1^n B_1^n E \overline{D}_1^n)_\nu = -D_\delta(\overline{\rho}_{A_1^n X_1^n D_1^n B_1^n E \overline{D}_1^n | \Omega} || \mathbb{1}_{A_1^n X_1^n D_1^n} \otimes \overline{\sigma}_{B_1^n E \overline{D}_1^n})$$
$$\leq H_\delta^\uparrow(A_1^n X_1^n D_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}} \ ,$$

where the second inequality is by the definition of $H_\delta^\uparrow$. Now the goal is to simplify.

1. $H_\delta^\uparrow(A_1^n X_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}} = H_\delta^\uparrow(A_1^n | B_1^n E)_{\rho_{|\Omega}}$ as [16, Lemma B.7] allows us to remove the X_1^n register and $\overline{D}_1^n$ is independent of everything as shown in Eq. (80).

2. $H_\delta(D_1^n | A_1^n X_1^n B_1^n E \overline{D}_1^n)_\nu = H_\delta(D_1^n | \overline{D}_1^n X_1^n)_\nu$ as [16, Eq. (46)] still holds because our ν is of the same form.

3. $H_\delta^\uparrow(A_1^n X_1^n D_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}} = H_\delta^\uparrow(A_1^n D_1^n | B_1^n E \overline{D}_1^n)_{\overline{\rho}_{|\Omega}}$ by [16, Eq. (43)], as the proof for this equation still holds in our setting.

Therefore we have simplified to

$$H_\delta^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} + H_\delta(D_1^n|\overline{D}_1^n X_1^n)_\nu \leq H_\delta^\uparrow(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}_{|\Omega}} \ .$$

Using the fact that $H_\delta(D_1^n|\overline{D}_1^n X_1^n)_\nu \geq n\overline{g} - nh$ as before [16, Below Eq. (52)] and by pushing that term over to the other side,

$$H_\delta^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} \leq H_\delta^\uparrow(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}_{|\Omega}} - n\overline{g} + nh \ .$$

$\square$

Theorem 10. *Let $\delta \in (1/2,1)$, $\eta \in (1, 1+2/V)$, $\zeta \in (1/2,1) \cup (1,\infty)$, such that $\frac{\eta}{\eta-1} = \frac{\delta}{\delta-1} + \frac{\zeta}{\zeta-1}$ and $(\eta-1)(\delta-1)(\zeta-1) > 0$. Assuming the Markov chain conditions are satisfied [Eq. (79)], then*

$$H_\delta^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} \leq nh - \frac{\delta}{1-\delta}\log(\rho[\Omega]) + n\frac{\eta-1}{4}V^2 \ ,$$

where $V := 2\lceil\|\nabla f\|_\infty\rceil + 2\log(1+2d_A)$.

Proof. Combining Lemma 2 with [16, Lemma B.5] applied to $\overline{\rho}$, which we can do by requiring $\delta \in (1/2,1)$ and noting $\overline{\rho} = \rho[\Omega]\overline{\rho}_{|\Omega} + (\overline{\rho} - \rho[\Omega]\overline{\rho}_{|\Omega})$, one obtains

$$H_\delta^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} \leq H_\delta^\uparrow(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}} - \frac{\delta}{\delta-1}\log\left(\frac{1}{\rho[\Omega]}\right) + nh - n\overline{g} \ .$$

Next we use Theorem 8 Item 1 with the substitutions $A = A_1^n D_1^n$, $C = B_1^n E\overline{D}_1^n$, $\tau_C = \overline{\rho}_{B_1^n E\overline{D}_1^n}$, where we will require $\eta \in (1, 1+1/\log(1+d_A d_D))$.

$$H_\delta^\uparrow(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}} \leq H_\eta(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}} + D_\gamma(\overline{\rho}_{B_1^n E\overline{D}_1^n}||\overline{\rho}_{B_1^n E\overline{D}_1^n}) = H_\eta(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}} \ ,$$

where the equality is by positive definiteness of Rényi divergences. This gives us

$$H_\delta^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} \leq H_\eta(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}} - \frac{\delta}{\delta-1}\log\left(\frac{1}{\rho[\Omega]}\right) + nh - n\overline{g} \ .$$

We just need to bound the H_η term, which follows the same type of argument as leading to [16, Eq. (40)], as noted at the end of the proof of [16, Proposition 4.5]. We have

$$H_\eta(A_1^n D_1^n|B_1^n E\overline{D}_1^n)_{\overline{\rho}} \leq \sum_i \sup_{\omega_{R_{i-1}R}} H_\eta(A_i D_i|B_i\overline{D}_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)}$$

$$\leq \sum_i \sup_{\omega_{R_{i-1}R}} H(A_i D_i|B_i\overline{D}_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} + n(\eta-1)\log^2(1+2d_A d_D)$$

$$\leq \sum_i \sup_{\omega_{R_{i-1}R}} H(A_i D_i|B_i\overline{D}_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} + n\frac{\eta-1}{4}V^2 \ ,$$

where the first line is because the Markov conditions are satisfied even including the $D_i\overline{D}_i$ registers due to our assumption that the Markov conditions in Eq. (79) hold[14] so we can apply [16, Corollary 3.5], the second is by applying [16, Lemma B.9] which we can do by our restriction on η, and the third is by definition of V. Lastly one can show $H(A_i D_i|B_i\overline{D}_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \leq \overline{g}$ [16, End of proof of Proposition 4.5]. Combining these points gets us our theorem. $\square$

---

[14] We omit the proof of this implication; see the proof of [16, Proposition 4.5] which contains proof of this.

B.4 QKD security proof with Rényi entropies

We now can present the proof of Theorem 5. In the main text we present physical and virtual QKD protocols (Protocol 1 and Protocol 2 respectively). As explained in the main text, they are equivalent and so the following security proof holds for both. From a technical viewpoint, we use the EAT which holds for sequential processes, so the security is most directly proven for the virtual QKD protocol because it is sequential.

Proof of Theorem 5. By the equivalence of Protocol 1 and Protocol 2, which is by construction, proving the security of Protocol 1 is equivalent to proving the security of Protocol 2. We refer to Protocol 2 in the proof, but this is just for the ease of the reader to link to the main text and Protocol 2's sequential presentation. Let Ω' be the event that Protocol 3 does not abort (i.e. Ω is satisfied) and error correction verification accepts (i.e. $\mathrm{hash}(\mathbf{Z}) = \mathrm{hash}(\widehat{\mathbf{Z}})$). Let Ω'' be the event that Protocol 2 does not abort and error correction verification passes. Let $\tilde{\rho}_{|\Omega''}$ be the output of the Protocol 2 conditioned on not aborting and error correction verification passing and $\rho_{|\Omega'}$ be the output of Protocol 3 conditioned on not aborting *and* error correction verification passing.

Fundamentally, we are interested in the entropy of the raw key which excludes the registers discarded in the general sifting step or the registers used for parameter estimation. As defined in Protocol 2, $\mathbf{Z} \equiv \overline{A}_1^n \setminus (\overline{A}_{\mathcal{S}} \cup \overline{A}_{\mathcal{T}})$. However, we note that Alice announces $\overline{A}_{\mathcal{T}}$ in Protocol 2, making it part of what is conditioned on, and $\overline{A}_{\mathcal{S}}$ is determined entirely by the registers $\widetilde{A}_1^n$, $\widetilde{B}_1^n$, and T_1^n. In other words, it is clear by Protocol 2 that there exists a deterministic function f which can reconstruct $\overline{A}_{\mathcal{S}}, \overline{A}_{\mathcal{T}}$ using a map of the form $\sum_{(s,p)} |s\rangle\langle s| \otimes |p\rangle\langle p| \, (\cdot) \, |s\rangle\langle s| \otimes |p\rangle\langle p| \otimes |f(s,p)\rangle\langle f(s,p)|_{\overline{A}_{\mathcal{S}} \overline{A}_{\mathcal{T}}}$. Therefore, by [16, Lemma B.7],

$$H_\alpha^\uparrow(\mathbf{Z}|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} C E)_{\tilde{\rho}_{|\Omega''}} = H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} C E)_{\tilde{\rho}_{|\Omega''}} \ .$$

We can handle the classical communication cost of error correction by [34, Eq. (5.96)]:

$$H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} C E)_{\tilde{\rho}_{|\Omega''}} \geq H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\tilde{\rho}_{|\Omega''}} - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} \tag{82}$$

$$= H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}^n \widetilde{B}^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} \tag{83}$$

where C is the register storing the classical communication due to error correction, and the equality comes from noting that $\rho_{\overline{A}_1^n \widetilde{A}_1^n \widetilde{B}_1^n T_1^n X_1^n E|\Omega'} = \tilde{\rho}_{\overline{A}_1^n \widetilde{A}_1^n \widetilde{B}_1^n T_1^n X_1^n E|\Omega''}$. We stress that Bob's private register, $\overline{B}_i^n$, for both the EAT and the QKD protocol, is excluded in the equality as they differ. We note that $\overline{A}_{\mathcal{T}}$ is conditioned upon as Alice publicly announced it, but X_1^n is not conditioned upon as Bob computes it locally and does not need to announce it unless aborting.

With all of this addressed, the entropy term that we would like to calculate to perform privacy amplification is

$$H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} \ . \tag{84}$$

This imposes one major difficulty: We need to find a way to relate this term to the term $H_\beta^\uparrow(\overline{A}_1^n \overline{B}_1^n|\widetilde{A}^n \widetilde{B}^n T_1^n E)_{\rho_{|\Omega'}}$ on the left-hand side of Eq. (20), where the Entropy Accumulation Theorem can be applied.

Following derivations in the DI-QKD setting [18], but also handling the $\overline{A}_{\mathcal{T}}$ register, we use the following series of claims:

$$\begin{aligned} H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} &\geq H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} \overline{B}_1^n E)_{\rho_{|\Omega'}} \\ &\geq H_\beta^\uparrow(\overline{A}_1^n \overline{B}_1^n \overline{A}_{\mathcal{T}}|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} - H_\delta^\uparrow(\overline{B}_1^n \overline{A}_{\mathcal{T}}|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} \\ &\geq H_\beta^\uparrow(\overline{A}_1^n \overline{B}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} - H_\delta^\uparrow(\overline{B}_1^n \overline{A}_{\mathcal{T}}|T_1^n E)_{\rho_{|\Omega'}} \ . \end{aligned} \tag{85}$$

The first inequality is the data processing inequality for sandwiched Rényi entropies [34, Corollary 5.5] for the specific choice of tracing out the $\overline{B}_1^n$ register. The second inequality is Case 2 of Theorem 8 with the substitutions $A = \overline{A}_1^n$, $B = \overline{A}_{\mathcal{T}}\overline{B}_1^n$, $C = \widetilde{A}_1^n\widetilde{B}_1^nT_1^nE$, where we also demand $\alpha \in (1,2)$, $\delta \in (1/2,1)$. The last inequality is again using the data-processing inequality for the $H_\delta^\uparrow$ term and [16, Lemma B.7] for the $H_\beta^\uparrow$ term using that $\overline{A}_{\mathcal{T}}$ may be generated using a deterministic mapping from $\overline{A}_1^n$ and T_1^n.

As Eq. (85) includes the term in Eq. (84), we need to bound the $H_\delta^\uparrow$ term in Eq. (85). We will do this using Theorem 10. We use the replacements $A_i = \overline{A}_{\mathcal{T}_i}\overline{B}_i$, $B_i = T_i$, and $E = E$, from which it is clear how to define the EAT maps for this process. We note it is okay to use $\overline{A}_{\mathcal{T}}$ as we may treat it as if it were actually n registers where it is $\perp$ whenever $T_i \neq 0$. The Markov conditions trivially hold since T_i uses seeded randomness. Then using the fact that $\overline{A}_{\mathcal{T}_i}\overline{B}_i = \perp \times \perp$ except when $T_i = 1$ which happens with probability γ, we construct the max-tradeoff function analytically by the following observation:

$$
\begin{aligned}
H(\overline{A}_{\mathcal{T}_i}\overline{B}_i|T_iR')_{\mathcal{M}_i(\omega)} &\leq H(\overline{A}_{\mathcal{T}_i}\overline{B}_i|T_i)_{\mathcal{M}_i(\omega)} \\
&= (1-\gamma)H(\overline{A}_{\mathcal{T}_i}\overline{B}_i|T_i=0)_{\mathcal{M}_i(\omega)} + \gamma H(\overline{A}_{\mathcal{T}_i}\overline{B}_i|T_i=1)_{\mathcal{M}_i(\omega)} \\
&\leq \gamma \log|\mathcal{A} \times \mathcal{B}|
\end{aligned}
\tag{86}
$$

where $\mathcal{A}$ and $\mathcal{B}$ are the alphabets of private outcomes Bob utilizes during parameter estimation. This tells us we can let the max-tradeoff function $f_{\max}(\boldsymbol{q}) = \gamma\log|\mathcal{A}\times\mathcal{B}|$ for all $\boldsymbol{q} \in \mathbb{P}(\mathcal{X})$. This also implies $\|\nabla f_{\max}\|_\infty = 0$. Note that for Theorem 10 to hold, we require $\delta \in (1/2,1)$, which is why we demanded this in the first chain rule. Therefore, using Theorem 10 we get

$$
H_\delta^\uparrow(\overline{A}_{\mathcal{T}}\overline{B}_1^n|T_1^nE)_{\rho_{|\Omega'}} \leq n\gamma\log|\mathcal{A}\times\mathcal{B}| - \frac{\delta}{1-\delta}\log(\varepsilon_{\mathrm{acc}}) + n(\eta-1)\log(1+2d_S)
\tag{87}
$$

where we have replaced $\rho[\Omega]$ with $\rho[\Omega']$ and then assumed $\varepsilon_{\mathrm{acc}} \leq \rho[\Omega']$.[15] We have also defined $d_S = (|\mathcal{A}|+1)(|\mathcal{B}|+1)$.

Combining Eq. (85) and Eq. (87),

$$
\begin{aligned}
H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n\widetilde{B}_1^nT_1^n\overline{A}_{\mathcal{T}}E)_{\rho_{|\Omega'}} \geq{}& H_\beta^\uparrow(\overline{A}_1^n\overline{B}_1^n|\widetilde{A}_1^n\widetilde{B}_1^nT_1^nE)_{\rho_{|\Omega'}} - n\gamma\log|\mathcal{A}\times\mathcal{B}| \\
&+ \frac{\delta}{1-\delta}\log(\varepsilon_{\mathrm{acc}}) - n(\eta-1)\log(1+2d_S) \,.
\end{aligned}
$$

We now apply the equivalent of Theorem 4 to the $H_\beta^\uparrow$ term. We can do this by our restriction on β earlier along with noting on the relevant marginal that any frequency distribution $\boldsymbol{q}$ accepted in the event Ω' is by definition also accepted in the event Ω so the value of h will hold. Therefore, the only formal change in Theorem 4 is using the replacement $\varepsilon_{\mathrm{EA}} \to \varepsilon_{\mathrm{acc}}$. Therefore, we have that either the input state aborts with probability greater than $1 - \varepsilon_{\mathrm{acc}}$ or

$$
\begin{aligned}
H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}_1^n\widetilde{B}_1^nT_1^n\overline{A}_{\mathcal{T}}E)_{\rho_{|\Omega'}} >{}& nh - n\frac{(\beta-1)\ln 2}{2}V^2 - \frac{\beta}{\beta-1}\log\frac{1}{\varepsilon_{\mathrm{acc}}} - n(\beta-1)^2K_\beta \\
&- n\gamma\log|\mathcal{A}\times\mathcal{B}| + \frac{\delta}{1-\delta}\log(\varepsilon_{\mathrm{acc}}) \\
&- n(\eta-1)\log(1+2d_S) \,.
\end{aligned}
$$

Grouping terms, the $\varepsilon_{\mathrm{acc}}$ correction term is of the form $\frac{\beta-\delta}{(\beta+1)(1-\delta)}\log(\varepsilon_{\mathrm{acc}})$. Then, plugging this back into Eq. (83) and applying the leftover hash lemma for non-smooth entropies [29], Theorem 9, resolves everything except that one has many conditions on $\alpha,\beta,\delta,\gamma,\eta,\zeta$.

---

[15] Note in principle this is a free parameter, but it does imply a lower bound on the probability that the input will pass parameter estimation and error correction verification, which is why we label it $\varepsilon_{\mathrm{acc}}$ for accept.

To get the simplified conditions on $\alpha, \beta, \delta, \gamma, \eta, \zeta$ in the theorem, note the conditions on α, β, δ are satisfied for $\beta \in (1, 2), \delta \in (1/2, 1), \alpha = \frac{-\beta+\delta}{-1+2\delta-\beta\delta}$. The conditions on $\delta \in (1/2, 1), \eta \in (1, 1 + \log^{-1}(1 + d_S)), \zeta \in (1/2, 1) \cup (1, \infty)$ are satisfied for the whole relevant range so long as $\zeta = \frac{-\delta+\eta}{-1+2\eta-\delta\eta}$, which does not enter into our key length. Finally, we note that $\eta > 1$, $\log(1 + 2d_S) > 1$, so $-n(\eta-1)\log(1 + 2d_S) < 0$, so this term is always a penalty on the key rate. In principle we would need to minimize η, but noting that $-n(\eta-1)\log(1 + 2d_S)$ goes to 0 as η goes to 1, and η is free to tend towards 1, we choose η such that $-n(\eta-1)\log(1 + 2d_S) = -1$.

Lastly, we need to explain the security claim in the statement of the theorem. There are two cases. Either $\rho[\Omega] < \varepsilon_{\text{acc}}$ or $\rho[\Omega] \geq \varepsilon_{\text{acc}}$. If $\rho[\Omega] < \varepsilon_{\text{acc}}$, then for that input, the security is trivially bounded by ε_{acc} by using Eq. (2) with the replacement $\Pr(\text{accept}) = \rho[\Omega] < \varepsilon_{\text{acc}}$. Therefore the focus is on the case $\rho[\Omega] \geq \varepsilon_{\text{acc}}$. First we consider the secrecy. Starting from the subnormalized state[16] $\rho_{S_A E F}$ where $S_A := h(\mathbf{Z})$ is the hashed key, h is the hash function, and F is the announcement of the hash function,

$$\frac{1}{2}\|\rho_{S_A EF} - |S_A|^{-1}\mathbb{1}_{S_A} \otimes \rho_{EF}\|_1 = \frac{1}{2}\rho[\Omega']\|\rho_{S_A F_{|\Omega'}} - |S_A|^{-1}\mathbb{1}_{S_A} \otimes \rho_{EF_{|\Omega'}}\|_1 \leq \rho[\Omega']\varepsilon_{\text{sec}} \leq \varepsilon_{\text{sec}} ,$$

where we started from the subnormalized state, normalized it by the condition of passing, and in the last line used that Theorem 9 tells us the trace norm divided by two is at most ε_{sec}. Therefore any input such that $\rho[\Omega'] \geq \varepsilon_{\text{acc}}$, the key is ε_{sec}-secret. Finally, we need to address correctness which is an upper bound on $\Pr[S_A \neq S_B \& \Omega']$. By the analysis of error correction verification using 2-universal hash functions [13], ε_{EC} is exactly what bounds this term, so we have the key is ε_{EC}-correct. Therefore, when $\rho[\Omega'] \geq \varepsilon_{\text{acc}}$, the key is $\varepsilon_{\text{sec}} + \varepsilon_{\text{EC}}$-secure. Combining these points, we have the protocol is $\max\{\varepsilon_{\text{acc}}, \varepsilon_{\text{sec}} + \varepsilon_{\text{EC}}\}$-secure. Finally, noting that if $\varepsilon_{\text{acc}} < \varepsilon_{\text{EC}} + \varepsilon_{\text{sec}}$ you could increase to $\varepsilon_{\text{acc}} = \varepsilon_{\text{EC}} + \varepsilon_{\text{sec}}$ to increase the key length without changing the security claim, so without loss of generality $\varepsilon_{\text{acc}} \geq \varepsilon_{\text{EC}} + \varepsilon_{\text{sec}}$. As such, we can just say the protocol is ε_{acc}-secure. □

We remark on an alternative key length that may be obtained largely following the same proof that allows us to express things in terms of ε_{EA} directly. This does not seem to provide a clear advantage over the previous proof. As such, we note that the use of [16, Lemma B.5] could presumably be replaced by [56, Lemma 10] for the smoothed version, but we omit such a proof in this work.

Proposition 7. *Consider any QKD protocol which follows Protocol 1 and satisfies Assumption 1. $\varepsilon_{\text{EA}}, \varepsilon_{\text{sec}}, \varepsilon_{\text{EC}} \in (0, 1]$, $\varepsilon_{\text{EC,rob}} \in [0, 1]$, such that $\varepsilon_{\text{EA}} \geq \varepsilon_{\text{sec}} + \varepsilon_{\text{EC}}$. Let h such that $f(\mathbf{q}) \geq h$ for all $\mathbf{q} \in \mathcal{Q}$ where f is the min-tradeoff function generated by Algorithm 1 or Algorithm 2.*

Let $\beta \in (1, 2)$, $\delta \in (1/2, 1)$ and $\alpha = \frac{-\beta+\delta}{-1+2\delta-\beta\delta}$. The QKD protocol is ε_{EA}-secure for key length

$$\begin{aligned}
\ell \leq &nh - \text{leak}_{\varepsilon_{\text{EC}}} - n\frac{(\beta - 1)\ln 2}{2}V^2 - n(\beta - 1)^2 K_\beta - n\gamma \log|\mathcal{A} \times \mathcal{B}| \\
&+ \frac{\beta - \delta}{(\beta - 1)(1 - \delta)}\log(\varepsilon_{\text{EA}}) + \frac{\alpha}{\alpha - 1}\log(\varepsilon_{\text{sec}} \cdot (1 - \varepsilon_{\text{EC,rob}})) + 1
\end{aligned} \tag{88}$$

where

$$V = \sqrt{\text{Var}(f) + 2} + \log\left(2d_S^2 + 1\right)$$

$$K_\beta = \frac{1}{6(2 - \beta)^3 \ln 2}2^{(\beta-1)(\log d_S + \text{Max}(f) - \text{Min}_\Sigma(f))}\ln^3\left(2^{\log d_S + \text{Max}(f) - \text{Min}_\Sigma(f)} + e^2\right) ,$$

---

[16]Subnormalization is due to aborting the protocol on the input.

where $\mathcal{A}$ and $\mathcal{B}$ are the alphabets of private outcomes for Alice's and Bob's announcements excluding the symbol $\perp$, respectively, $d_S = (|\mathcal{A}|+1)(|\mathcal{B}|+1)$, $\mathrm{leak}_{\varepsilon_{\mathrm{EC}}}$ is the amount of information leakage during the error correction step.

Proof. We largely follow the previous proof with some modifications which we explain. We start at Eq. (83). First we note that $\rho_{|\Omega} = \rho[\Omega'|\Omega]\rho_{|\Omega'} + (\rho_{|\Omega} - \rho[\Omega'|\Omega]\rho_{|\Omega'})$, where $[\Omega'|\Omega]$ denotes the event Ω' occurring conditioned on Ω occurring, i.e. the probability that error correction succeeds given we pass parameter estimation.[17] Moreover, since ultimately $\alpha > 1$ will always hold on the conditions that complete the proof, we can apply [16, Lemma B.5, Eq. (80)] to determine

$$
\begin{aligned}
H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}^n\widetilde{B}^nT_1^n\overline{A}_\mathcal{T}E)_{\rho_{|\Omega'}} &\geq H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}^n\widetilde{B}^nT_1^n\overline{A}_\mathcal{T}E)_{\rho_{|\Omega}} - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{\rho[\Omega'|\Omega]}\right) \\
&\geq H_\alpha^\uparrow(\overline{A}_1^n|\widetilde{A}^n\widetilde{B}^nT_1^n\overline{A}_\mathcal{T}E)_{\rho_{|\Omega}} + \frac{\alpha}{\alpha-1}\log(1 - \varepsilon_{\mathrm{EC,rob}}),
\end{aligned}
$$

where the second inequality follows from the assumption $\rho[\Omega'|\Omega] \geq 1 - \varepsilon_{\mathrm{EC,rob}}$.[18] Everything through Eq. (87) is the same argument but with $\rho_{|\Omega}$. The only change this results in is that any term with $\varepsilon_{\mathrm{acc}} \to \varepsilon_{\mathrm{EA}}$. Since we consider $\rho_{|\Omega}$, we can apply Theorem 4 directly, so we replace $\varepsilon_{\mathrm{acc}}$ in previous proof with $\varepsilon_{\mathrm{EA}}$ again. Combining things and simplifying the greek alphabet parameters is the largely the same as before. This completes the proof.

As for the security claim. We split into two cases in the same fashion. In the case $\rho[\Omega] < \varepsilon_{\mathrm{EA}}$, the state is trivially $\varepsilon_{\mathrm{EA}}$ secure. In the case $\rho[\Omega] \geq \varepsilon_{\mathrm{EA}}$, we have identical analysis to the previous case. The correctness argument is the same as before, so the security claim is $\varepsilon = \max\{\varepsilon_{\mathrm{EA}}, \varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{EC}}\}$. $\qquad\square$

C Relation between Fixed-Length and Probabilistic Round-by-Round Parameter Estimation Protocols

In this appendix we provide the proof of Theorem 6. Effectively, we need to describe the QKD protocol in enough detail that we can view the output as a (somewhat complicated) CQ state whose probability of certain sequences can be determined using the structure of the protocol. To do this, we first describe the general description of a device-dependent QKD protocol through the parameter estimation step in the most explicit formal fashion, i.e. in terms of conditional states. We then show how this relates to the output of the EAT subprotocol, and finally we relate conditional states of these two cases. This allows us to determine exactly how the security parameter relates in the two cases. We stress that the notation in this appendix slightly differs from that of the rest of the paper so as to keep things concise. In this appendix, we use registers Q_AQ_B instead of register Q to separate Alice's and Bob's registers. We try to keep the notation as close to the main text for consistency.

---

[17]As the notation is a slight abuse of notation from conditional probability which would have $\rho[\text{EC accepts}|\Omega]$, we clarify. Recall one starts with the output after error correction ρ. We can partition the total state according to the events error correction and parameter estimation pass, Ω', just parameter estimation passes, $\Omega \setminus \Omega'$, and everything else, so that $\rho = \rho[\Omega']\rho_{|\Omega'} + \rho[\Omega \setminus \Omega']\rho_{\Omega\setminus\Omega'} + (\rho - \rho[\Omega']\rho_{|\Omega'} + \rho[\Omega \setminus \Omega']\rho_{\Omega\setminus\Omega'})$. Then by definition, $\rho_{|\Omega} = \rho[\Omega]^{-1}(\rho[\Omega']\rho_{|\Omega'} + \rho[\Omega' \setminus \Omega]\rho_{|\Omega'\setminus\Omega})$. Recalling Ω' is Ω and error correction passes, we can think of $\rho[\Omega'|\Omega] := \rho[\Omega']/\rho[\Omega]$ as the probability of error correction passing given parameter estimation.

[18]The choice of notation is as follows. The ε-robustness of a protocol on an input ρ is the probability of it aborting on that input [13]. Ideally, we want our error correction scheme to be 0-robust whenever parameter estimation has passed, i.e. $\rho[\Omega'|\Omega] = 1$ is the ideal case. As such, the assumption we have made is roughly that if parameter estimation passes, then the error correction will be $\varepsilon_{\mathrm{EC,rob}}$-robust.

As explained in Section 3.2, since we are considering device-dependent QKD protocols, we may make the assumption that the measurements by Alice and Bob are performed in an n-fold manner, i.e. $\mathcal{E}^M = \Phi_{\mathcal{P}}^{\otimes n}$ where $\Phi_{\mathcal{P}} : Q_A Q_B \to \mathbb{C}^{|\mathcal{A} \times \mathcal{B}|}$ where, following the notation of Theorem 5, $\mathcal{A} \times \mathcal{B}$ is a joint finite alphabet of Alice and Bob's outcomes for parameter estimation, and we dropped the subscript i from the Hilbert spaces as traditionally device-dependent QKD assumes the dimension to be fixed in each round. Given this assumption, we may write the output state of the measurement as

$$(\mathcal{E}^M \otimes \mathcal{I}_E)(\rho_{Q_{A,1}^n Q_{B,1}^n E}) = \sum_{(a_1^n, b_1^n, p_1^n)} |a_1^n\rangle\langle a_1^n| \otimes |b_1^n\rangle\langle b_1^n| \otimes |p_1^n\rangle\langle p_1^n| \otimes \rho_E^{(a_1^n, b_1^n, p_1^n)} \ ,$$

where a_i, b_i are outcomes of Alice's and Bob's private registers and outcomes of all public registers of the ith round are grouped as p_i, and $\rho_E^{(a_1^n, b_1^n, p_1^n)}$ is the (subnormalized) conditional state of Eve.

Next Alice and Bob perform parameter estimation.[19] Canonically the assumption is they are going to pick a random subset of the n signals of size m and announce their respective outcomes on those m rounds.[20] Finally they decide if they continue the protocol or not based on those outcomes. That is, they have some set of observed sequences $\mathcal{Q} \subset \mathcal{X}'^{\times m}$ which they accept on, where $\mathcal{X}'$ is as defined in Section 6.4. It follows that one could split $\mathcal{E}^{PE}$ as a channel which generates which rounds to test, a map where they make their announcements, and a map where they abort if the observations are not in a set of pre-agreed upon acceptable observations $\mathcal{Q}$:

$$\mathcal{E}^{PE} = \mathcal{E}^{\mathcal{Q}} \circ \mathcal{E}^{PE,ann} \circ \mathcal{E}^{PE,testgen} \ .$$

Note that while fundamentally $\mathcal{Q}$ is a set of sequences of length m, $x_1^m \in \mathcal{X}'^{\times m}$, it can trivially be extended to a set of sequences of length n, $x_1^n \in (\mathcal{X}' \cup \{\bot\})^{\times n}$, which better matches the EAT and is denoted Ω. In the case that it is a set of sequences of length n, it only makes sense for all sequences in Ω to have $n - m$ of the entries be the $\bot$ symbol. To match with EAT we mean this event Ω than aligns properly with extending $\mathcal{Q}$.

Having completed the explanation of the protocol, we can see the natural definitions for these maps are:

$$\mathcal{E}^{PE,testgen}(\alpha) = \frac{1}{|T_m|} \sum_{t_1^n \in T_m} |t_1^n\rangle\langle t_1^n|$$

where $T_m = \{x \in \{0,1\}^n : \text{Hamming Weight}(x) = m\}$.

$$\mathcal{E}^{PE,ann}(\rho_{A_1^n B_1^n T_1^n}) = \sum_{(a_1^n, b_1^n, t_1^n)} |\text{x}^{\times n}(a_1^n, b_1^n, t_1^n, p_1^n)\rangle\langle \text{x}^{\times n}(a_1^n, b_1^n, t_1^n, p_1^n)|_{X_1^n} \otimes |a_1^n\rangle\langle a_1^n|$$

$$\otimes |b_1^n\rangle\langle b_1^n| \otimes |p_1^n\rangle\langle p_1^n| \otimes \rho_E^{(a_1^n, b_1^n, p_1^n)}$$

where $\text{x}(a_i, b_i, t_i, p_i) = (a_i \times b_i) \in \mathcal{A} \times \mathcal{B}$ when $t_i = 1$ and otherwise equals $\bot$, i.e. x is the *deterministic* announcement function due to testing that constructs $x_i \in \mathcal{X}$.

---

[19]In Protocol 2, sifting and the key map happen each round along with parameter estimation. In Renner's original framework [13], it is not the case as the sifting and key map happen afterwards in the blockwise processing, which is the reason for this discrepancy from the main text.

[20]This is equivalent to applying a random permutation and then performing parameter estimation on the first m indices, but to match the EAT, we do not reformat in this manner. We note an alternative model one might propose that seems to be intuitive is to perform probabilistic round-by-round testing, count the total number of tests at the end, and then a posteriori treat the protocol as having picked that many tests. This does not fit into a pre-existing universally composable security proof for fixed-length testing. In particular, it does not fit into the security proof method of [13].

$$\mathcal{E}^{\mathcal{Q}}(\rho_{X_1^n}) = \sum_{x_1^n \in \Omega} |x_1^n\rangle\langle x_1^n| \, \rho_{X_1^n} \, |x_1^n\rangle\langle x_1^n| \ ,$$

where we the event Ω as the set of sequences of length n that satisfy $\mathcal{Q}$ as stated earlier.

Since p_i is a function of (a_i, b_i, t_i) by construction of Protocol 1 and x_i is a function of (a_i, b_i, t_i, p_i), we are interested in the set $\{(a_1^n, b_1^n, t_1^n)$ such that $x_1^n \in \Omega$ with non-zero probability$\}$. Throughout, when we write a summation over something of the form "$(a_1^n, b_1^n, t_1^n) : x_1^n \in \Omega$," we are indicating the set of sequences that result in $x_1^n \in \Omega$. Therefore, combining all of this, we find the output state after parameter estimation is

$$\widetilde{\rho}^{out} = \frac{1}{|T_m|} \sum_{(a_1^n, b_1^n, t_1^n) : x_1^n \in \Omega} \left|\mathrm{x}^{\times n}(a_1^n, b_1^n, t_1^n, p_1^n)\right\rangle\!\!\left\langle\mathrm{x}^{\times n}(a_1^n, b_1^n, t_1^n, p_1^n)\right|_{X_1^n} \otimes |a_1^n\rangle\langle a_1^n|$$
$$\otimes |b_1^n\rangle\langle b_1^n| \otimes |p_1^n\rangle\langle p_1^n| \otimes |t_1^n\rangle\langle t_1^n| \otimes \rho_E^{(a_1^n, b_1^n, p_1^n)} \ ,$$

where $\widetilde{\rho}^{out} = (\mathcal{E}^{PE,ann} \circ \mathcal{E}^{PE,testgen} \circ \mathcal{E}^M \otimes \mathcal{I}_E)(\rho_{Q_1^{A,n} Q_1^{B,n} E})$. We stress by construction of Ω, that any element of $(a_1^n, b_1^n, t_1^n) : x_1^n \in \Omega$ has $t_1^n \in T_m$, which is why we don't restrict the space T^n. We will define the final output after sifting and the key map (but prior to error correction) as

$$\rho^{out} = \frac{1}{|T_m|} \sum_{(\hat{a}_1^n, \hat{b}_1^n, t_1^n) : x_1^n \in \Omega} \left|\mathrm{x}^{\times n}(\hat{a}_1^n, \hat{b}_1^n, t_1^n, p_1^n)\right\rangle\!\!\left\langle\mathrm{x}^{\times n}(\hat{a}_1^n, \hat{b}_1^n, t_1^n, p_1^n)\right|_{X_1^n} \otimes |\hat{a}_1^n\rangle\langle \hat{a}_1^n|$$
$$\otimes \left|\hat{b}_1^n\right\rangle\!\!\left\langle\hat{b}_1^n\right| \otimes |p_1^n\rangle\langle p_1^n| \otimes |t_1^n\rangle\langle t_1^n| \otimes \rho_E^{(\hat{a}_1^n, \hat{b}_1^n, p_1^n)} \ ,$$

where hats denoted updated registers, and the reason that we can define x on the updated sequence is that by assumption testing commutes with sifting and the key map, given the registers T_1^n.

This completes our account of the output state of parameter estimation in the fixed-length device-dependent QKD protocol. However, we will need these extra definitions when comparing to the output of the EAT protocol:

$$\rho_{|\Omega_{sub}}^{out} = (\mathcal{E}^{\mathcal{Q}} \otimes \mathcal{I}_E)(\rho^{out}) \qquad \rho_{|\Omega}^{out} = \frac{1}{\mathrm{Tr}\left(\rho_{\Omega_{sub}}^{out}\right)} \rho_{\Omega_{sub}}^{out} \ . \tag{89}$$

Using the same notation as we did for the fixed-length device-dependent QKD protocol, it is straightforward from the effective tensor product structure of device-dependent QKD (Section 3.2) that the output of the EAT protocol can be written as:

$$\rho_{EAT}^{out} = \sum_{(\hat{a}_1^n, \hat{b}_1^n, t_1^n) : x_1^n \in \Omega} \left|\mathrm{x}^{\times n}(\hat{a}_1^n, \hat{b}_1^n, t_1^n, p_1^n)\right\rangle\!\!\left\langle\mathrm{x}^{\times n}(\hat{a}_1^n, \hat{b}_1^n, t_1^n, p_1^n)\right|_{X_1^n} \otimes |\hat{a}_1^n\rangle\langle \hat{a}_1^n|$$
$$\otimes \left|\hat{b}_1^n\right\rangle\!\!\left\langle\hat{b}_1^n\right| \otimes |p_1^n\rangle\langle p_1^n| \otimes |t_1^n\rangle\langle t_1^n| \otimes \rho_E^{(\hat{a}_1^n, \hat{b}_1^n, p_1^n)} \ .$$

Our interest is then proving the relation of ρ_{EAT}^{out} to ρ^{out} to prove Theorem 6.

Proof of Theorem 6. Ultimately we need to argue about the probabilities of given sequences conditioned on passing, so we start by simplifying the joint probability of the sequences. For notational simplicity in this proof, we let

$$\hat{r}_i := (\hat{a}_i, \hat{b}_i, p_i) \quad i \in [n] \quad \text{and} \quad \widehat{\mathcal{S}}_{|\Omega} := \{(x_1^n, r_1^n, t_1^n) : x_1^n \in \Omega\} \ ,$$

and r_i, $\mathcal{S}_{|\Omega}$ are defined the same way but with the un-updated a_i, b_i. First consider $\rho^{in} \equiv \rho_{Q^n_{A,1} Q^n_{B,1} E}$ to the fixed-length protocol that satisfies data partitioning as in Protocol 1 (so that we consider the same announcement structure between the two settings for fair comparison). Then, for any *non-zero* probability sequence, we have:

$$\Pr(x^n_1, r^n_1, t^n_1) = \Pr(r^n_1, t^n_1) = \Pr(t^n_1)\Pr(r^n_1) = \frac{1}{|T_m|}\Pr(r^n_1) \ ,$$

where the first equality is because x^n_1 is produced by a deterministic function of the other sequences, the second equality is because t^n_1 is determined independent of the other sequences, and the third equality is because t^n_1 was uniformly chosen from the set T_m. Note that sifting and the key map, while deterministic, are not bijective in general. However, since accepting or not accepting a sequence is a deterministic function given x^n_1 which is a deterministic function of (r^n_1, t^n_1) and doesn't change under updating, we have

$$\sum_{(x^n_1, \hat{r}^n_1, t^n_1) \in \mathcal{S}_{|\Omega}} \Pr(x^n_1, \hat{r}^n_1, t^n_1) = \sum_{(x^n_1, r^n_1, t^n_1) \in \mathcal{S}_{|\Omega}} \Pr(x^n_1, r^n_1, t^n_1) = \frac{1}{|T_m|} \sum_{(x^n_1, r^n_1, t^n_1) \in \mathcal{S}_{|\Omega}} \Pr(x^n_1|r^n_1, t^n_1)\Pr(r^n_1) \ .$$

Now we consider the EAT protocol. Note that the sequence t^n_1 is an i.i.d. sequence generated from sampling the distribution $Q = (1-\gamma, \gamma)^T$, whose probability is determined by the method of types. Following the notation used in [40], we have $\Pr(t^n) = Q^n(t^n_1)$ for any binary sequence t^n_1 sampled from Q n times. It follows,

$$\Pr(r^n_1, t^n_1) = \Pr(t^n_1)\Pr(r^n_1) = Q^n(t^n_1)\Pr(r^n_1) \ ,$$

which, again using that acceptance is a deterministic function of (r^n_1, t^n_1),

$$\sum_{(x^n_1, \hat{r}^n_1, t^n_1): x^n_1 \in \Omega} \Pr(x^n_1, \hat{r}^n_1, t^n_1) = \sum_{(x^n_1, \hat{r}^n_1, t^n_1): x^n_1 \in \Omega} \Pr(x^n_1|r^n_1, t^n_1)\Pr(r^n_1, t^n_1)$$
$$= \sum_{(x^n_1, r^n_1, t^n_1): x^n_1 \in \Omega} Q^n(t^n_1)\Pr(x^n_1|r^n_1, t^n_1)\Pr(r^n_1) \ ,$$

where in the first line we stress we have kept the sum indexing over the non-updated registers, so the sum is independent of how they get updated conditioned on $x^n_1 \in \Omega$. By [40, Theorem 11.1.2], we know $Q^n(t^n_1) = 2^{-n(H(f_t) - D(f_t \| Q))}$ where f_t is the frequency distribution over T induced by t^n_1 (i.e. the type). Therefore, if t^n_1 has Hamming weight m, since m is defined as $m = \gamma n$, we have $Q^n(t^n_1) = 2^{-nh(\gamma)}$ as the relative entropy term is zero, where $h(\cdot)$ is the binary entropy function. As a sequence will only be accepted if t^n_1 has Hamming weight m and x^n_1 is acceptable, we have that

$$\rho^{out}_{EAT}[\Omega] = \mathrm{Tr}\left(\sum_{(x^n_1, \hat{r}^n_1, t^n_1) \in \widehat{\mathcal{S}}_{|\Omega}} \Pr(x^n_1, \hat{r}^n_1, t^n_1) |x^n_1, \hat{r}^n_1, t^n_1\rangle\langle x^n_1, \hat{r}^n_1, t^n_1| \otimes \hat{\rho}^{(\hat{r}^n_1)}_E\right)$$
$$= \sum_{(x^n_1, \hat{r}^n_1, t^n_1) \in \widehat{\mathcal{S}}_{|\Omega}} \Pr(x^n_1, \hat{r}^n_1, t^n_1)$$
$$= 2^{-nh(\gamma)} \sum_{(x^n_1, \hat{r}^n_1, t^n_1) \in \mathcal{S}_{|\Omega}} \Pr(x^n_1|r^n_1, t^n_1)\Pr(r^n_1)$$
$$= 2^{-nh(\gamma)}|T_m| \sum_{(x^n_1, \hat{r}^n_1, t^n_1) \in \mathcal{S}_{|\Omega}} \frac{1}{|T_m|}\Pr(x^n_1|r^n_1, t^n_1)\Pr(r^n_1)$$

$$= 2^{-nh(\gamma)} |T_m| \operatorname{Tr}\left(\sum_{(x_1^n, \hat{r}_1^n, t_1^n) \in \widehat{\mathcal{S}}_{|\Omega}} \Pr(x_1^n, \hat{r}_1^n, t_1^n) \, |x_1^n \hat{r}_1^n, t_1^n\rangle\langle x_1^n \hat{r}_1^n, t_1^n| \otimes \hat{\rho}_E^{(\hat{r}_1^n)} \right)$$

$$= 2^{-nh(\gamma)} \binom{n}{m} \rho^{out}[\Omega] \; ,$$

where the last line is because there are $\binom{n}{m}$ n-length bit strings with Hamming weight m.

To see that $\rho_{EAT|\Omega}^{out} = \rho_{|\Omega}^{out}$, we make the following observations:

1. The set of sequences $(a_1^n, b_1^n, p_1^n, t_1^n)$ allowed by Ω is exactly the same in both cases.

2. For any tuple of sequences (a_1^n, b_1^n, p_1^n), $p(a_1^n, b_1^n, p_1^n)$ is the same for both protocols given that ρ^{in} is the same and the measurement and announcement procedures are the same— it is just the distribution over $\Pr(t_1^n)$ that differs.

3. For every *allowed* tuple of sequences, the probability $\Pr(t_1^n)$ is a fixed (uniform) value. Specifically, for allowed tuples of sequences, $\Pr(t_1^n) = 2^{-nh(\gamma)}$ for EAT, but $\Pr(t_1^n) = \frac{1}{|T_m|}$ for fixed test length. While the fixed value differs in the two cases, it cancels under the renormalization of conditioning the state on the allowed tuples of sequences.[21]

It therefore follows under the renormalization that the distribution over the sequences in both cases is identical (and $\rho_E^{(a_1^n, b_1^n, p_1^n)}$ for each sequence is the same too since both are based on (a_1^n, b_1^n, p_1^n) followed by the introduction of an independent sequence and then deterministic functions). $\qquad\square$

Note this equivalence was able to be derived in effect because the testing in both cases is independent and the probability is uniform over sequences contained in the event Ω in question beyond the conditional probabilities that arise from the measurement, and since the measurements and announcements are the same process in both cases, this is not altered.

Finally, we explain the derivation of the bound presented below Theorem 6:

$$\log\left(\bar{\varepsilon} \rho_{EAT}^{out}[\Omega]\right) = \log(\bar{\varepsilon}) + \log\left(2^{-nh(\gamma)} \binom{n}{m} \rho^{out}[\Omega] \right)$$

$$= \log\left(\bar{\varepsilon} \rho^{out}[\Omega]\right) - nh(\gamma) + \log\binom{n}{m}$$

$$\geq \log\left(\bar{\varepsilon} \rho^{out}[\Omega]\right) + \log\left(\frac{e^2}{\sqrt{2\pi}} \sqrt{\gamma(1-\gamma)n} \right)$$

$$= \log(\bar{\varepsilon} \varepsilon_{\mathrm{PE}}) + \log\left(\frac{e^2}{\sqrt{2\pi}} \sqrt{\gamma(1-\gamma)n} \right) \; ,$$

where the inequality follows from using $\sqrt{2\pi} n^{n+1/2} e^{-n} \leq n! \leq e n^{n+1/2} e^{-n}$ [57] to bound $\binom{n}{m}$.

---

[21] For a simple example, imagine we have the two states: $\rho_1 = y p_{00} |00\rangle\langle00| + x p_{01} |01\rangle\langle01| + x p_{10} |10\rangle\langle10| + z p_{11} |11\rangle\langle11|$ and $\rho_2 = y' p_{00} |00\rangle\langle00| + x' p_{01} |01\rangle\langle01| + x' p_{10} |10\rangle\langle10| + z' p_{11} |11\rangle\langle11|$. Say we condition only on the strings of Hamming weight one. Then, we have $\rho_{1|\Omega} = \frac{1}{x p_{01} + x p_{10}} (x p_{01} |01\rangle\langle01| + x p_{10} |10\rangle\langle10|)$ and $\rho_{2|\Omega} = \frac{1}{x' p_{01} + x' p_{10}} (x' p_{01} |01\rangle\langle01| + x' p_{10} |10\rangle\langle10|)$. These conditional states are the same because the renormalization cancels the fixed (but different) pre-factor x (resp. x') for all the strings we are interested in.

D Security of QKD using EAT with Smoothing

In this section we present the security proof for smooth min-entropy rather than sandwiched Rényi entropies.

D.1 Background smooth entropy results

For completeness, in this section we present the max-tradeoff function and original version of the EAT [16] for max-tradeoff functions which we make use of in the security proof in this Section. Likewise, we give an account of the Leftover Hashing Lemma [13] and how it is applied in Theorem 15.

We first state the min-tradeoff function in terms of smooth min-entropy.

Proposition 8 (Theorem V.2 of [17] (Special Case)). *Consider EAT channels $\mathcal{M}_1, ..., \mathcal{M}_n$ and $\rho_{S_1^n P_1^n X_1^n E}$ as defined in Eq. (7) such that it satisfies the Markov conditions [Eq. (8)]. Let $h \in \mathbb{R}$, $\alpha \in (1,2)$, f be a min-tradeoff function for $\mathcal{M}_1, \ldots, \mathcal{M}_n$, and let $\bar{\varepsilon} \in (0,1)$. Let S_i always be classical. Then, for any event $\Omega \subseteq \mathcal{X}^n$ that implies $f(\mathsf{freq}(X_1^n)) \geqslant h$,*

$$H_{\min}^{\bar{\varepsilon}}(S_1^n | P_1^n E)_{\rho_{|\Omega}} \geq nh - n\frac{(\alpha-1)\ln 2}{2}V^2 - \frac{1}{\alpha-1}\log\frac{2}{\bar{\varepsilon}^2\rho[\Omega]^2} - n(\alpha-1)^2 K_\alpha \tag{90}$$

holds for

$$V = \sqrt{\mathsf{Var}(f) + 2} + \log\left(2d_S^2 + 1\right) \tag{91}$$

$$K_\alpha = \frac{1}{6(2-\alpha)^3\ln 2}2^{(\alpha-1)(\log d_S + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))}\ln^3\left(2^{\log d_S + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2\right) \tag{92}$$

where $\mathsf{Max}(f))$, $\mathsf{Min}(f)$, $\mathsf{Min}_\Sigma(f)$ and $\mathsf{Var}(f)$ are defined in Eq. (14) and $d_S = \max_{i\in[n]}|S_i|$ is the maximum dimension of the systems S_i.

Moreover, for a specific choice of $\alpha \in (1,2)$ [17],

$$H_{\min}^{\bar{\varepsilon}}(S_1^n | P_1^n E)_{\rho_{|\Omega}} > nh - c\sqrt{n} - c'$$

where c and c' are functions of $\bar{\varepsilon}$, d_S, $\rho[\Omega]$, and properties of the tradeoff function as follows:

$$c = \sqrt{2\ln 2}\left(\log\left(2d_S^2 + 1\right) + \sqrt{2 + \mathsf{Var}(f)}\right)\sqrt{1 - 2\log(\bar{\varepsilon}\rho[\Omega])} \tag{93}$$

$$c' = \frac{35(1 - 2\log(\bar{\varepsilon}\rho[\Omega]))}{\left(\log(2d_S^2 + 1) + \sqrt{2 + \mathsf{Var}(f)}\right)^2}2^{\log d_S + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)}\ln^3\left(2^{\log d_S + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2\right) . \tag{94}$$

Next we recall the notion of max-tradeoff function.

Definition 7. *Following the notation of Section 3. An affine function f on $\mathbb{P}(\mathcal{X})$ is called max-tradeoff function f for an EAT Channel $\mathcal{M}_i$ if it satisfies*

$$f(\boldsymbol{q}) \geq \sup_{\nu\in\Sigma_i(\boldsymbol{q})} H(S_i|P_i R)_\nu, \quad \forall \boldsymbol{q} \in \mathbb{P}(\mathcal{X}) .$$

We now state the EAT for max-tradeoff functions from [16].

Theorem 11 (Part of Theorem 4.4 of [16]). *Let $\mathcal{M}_1, \ldots, \mathcal{M}_n$ be EAT channels and $\rho_{S_1^n P_1^n X_1^n E}$ be of the form in Eq. (7) which satisfies the Markov conditions from Eq. (8). Let $h \in \mathbb{R}$, let f be an affine max-tradeoff function for $\mathcal{M}_1, \ldots, \mathcal{M}_n$, and let $\bar{\varepsilon} \in (0,1)$. Then, for any event $\Omega \subseteq \mathcal{X}^n$ that implies $f(\mathrm{freq}(X_1^n)) \leqslant h$,*

$$H_{\max}^{\bar{\varepsilon}}(S_1^n | P_1^n E)_{\rho_{|\Omega}} < nh + c\sqrt{n} \tag{95}$$

holds for $c = 2\left(\log(1 + 2d_S) + \lceil \|\nabla f\|_\infty \rceil\right)\sqrt{1 - 2\log(\bar{\varepsilon}\rho[\Omega])}$, where $d_S := \max_{i \in [n]}\{|S_i|\}$.

This completes the statement of the EAT for max-tradeoff functions. We now turn our attention to the Leftover Hashing Lemma (LHL). The LHL tells us that applying a two-universal hash function to a somewhat secret string constructs a shorter ε-secret key. The notion of secrecy is measured by distance from uniformity given Eve's side-information.

Theorem 12 (Corollary 5.6.1 of [13]). *Let $\rho_{XE} \in \mathrm{D}(XE)$ be a classical-quantum state where $X \cong \mathbb{C}^{|\Sigma|}$ where Σ is some finite set. Let $\mathcal{F}$ be a family of two-universal hash functions from $\Sigma \to \{0,1\}^\ell$ and $\varepsilon > 0$. Then*

$$\frac{1}{2}\left\| \rho_{F(X)EF} - \frac{1}{|\{0,1\}^\ell|}\mathbb{1}_{F(X)} \otimes \rho_{EF} \right\|_1 \leq \varepsilon + 2^{-\frac{1}{2}(H_{\min}^{\varepsilon'}(X|E) - \ell - 2)} .$$

From this we obtain the following corollary immediately.

Corollary 13. *Let $\rho_{XE} \in \mathrm{D}(XE)$ be a classical-quantum state. Let $\varepsilon_{sec} := \varepsilon' + 2^{-\frac{1}{2}(H_{\min}^{\varepsilon'}(X|E) - \ell - 2)}$ and $\varepsilon' > 0$. Let $\varepsilon_{\mathrm{PA}} := \varepsilon_{sec} - \varepsilon' > 0$. Then for an ε_{sec}-secret key, the length of the key, ℓ, must satisfy the following bound:*

$$\ell \leq H_{\min}^{\varepsilon'}(X|E) - 2\log\left(\frac{2}{\varepsilon_{\mathrm{PA}}}\right) .$$

D.2 Technical lemmas for smooth entropy key rate

The following lemma shows that generating a classical register from the classical side information does not change the value of the smooth min-entropy.

Lemma 3. *For any CQ state $\rho_{AB} = \sum_i p_i \rho_A^i \otimes |i\rangle\langle i|_B$ and $\rho_{ABC} = \sum_i p_i \rho_A^i \otimes |i\rangle\langle i|_B \otimes |f(i)\rangle\langle f(i)|_C$ with a given function f, it holds that*

$$H_{\min}^\varepsilon(A|B) = H_{\min}^\varepsilon(A|BC). \tag{96}$$

Proof. This can be seen by defining isometry $V : |i\rangle_B \to |i\rangle_B |f(i)\rangle_C$. Then $\rho_{ABC} = V\rho_{AB}V^\dagger$. The result then holds by the fact that the smooth min-entropy is invariant under local isometries [34, Corollary 6.11]. Note that this holds for any function f which may not necessarily be deterministic one (c.f. [34, Eqs. 6.77]). $\qquad\square$

Lemma 4. *Consider a CCQ state $\rho_{XPE} = \sum_{(x,p)} |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes \rho_E^{(x,p)}$. Consider another classical register Y which be constructed using a deterministic function on the registers X and P, i.e. $f : X \times P \to Y$. That is, there exists an isometry, $V \equiv \sum_{(x,p)} |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes |f(x,p)\rangle_Y$ reconstructing Y from X and P. Then*

$$H_{\min}^\varepsilon(YX|PE)_{V\rho V^\dagger} = H_{\min}^\varepsilon(X|PE)_\rho . \tag{97}$$

Proof. To prove this proposition, we simply prove

$$H^\varepsilon_{\min}(YX|PE)_{V\rho V^\dagger} \geq H^\varepsilon_{\min}(X|PE)_\rho \ , \tag{98}$$

$$H^\varepsilon_{\min}(YX|PE)_{V\rho V^\dagger} \leq H^\varepsilon_{\min}(X|PE)_\rho \ . \tag{99}$$

We start with Eq. (98) as it is straightforward using previous results. Namely, we see:

$$H^\varepsilon_{\min}(YX|PE)_{V\rho V^\dagger} \geq H^\varepsilon_{\min}(X|PE)_{V\rho V^\dagger} = H^\varepsilon_{\min}(X|PE)_\rho \ . \tag{100}$$

The first inequality comes from the fact that the entropy of a classical register is non-negative [34, Lemma 6.17]. The equality follows from noting that $\mathrm{Tr}_Y(V\rho V^\dagger) = \rho$. Therefore we can focus on the other direction of the inequality.

By combining [34, Definitions 6.2 and 6.9] we note the definition of the smooth min-entropy terms we are concerned with:

$$H^\varepsilon_{\min}(YX|PE)_{V\rho V^\dagger} := \max_{\overline{\rho} \in \mathcal{B}^\varepsilon(V\rho V^\dagger)} \max_{\overline{M}_{PE} \in \mathrm{D}_\leq(PE)} \max\left\{\overline{\lambda} \in \mathbb{R} : \mathbb{1}_Y \otimes \mathbb{1}_X \otimes 2^{-\overline{\lambda}} \overline{M}_{PE} \geq \overline{\rho}_{YXPE}\right\} \tag{101}$$

$$H^\varepsilon_{\min}(X|PE)_\rho := \max_{\widetilde{\rho} \in \mathcal{B}^\varepsilon(\rho)} \max_{\widetilde{M}_{PE} \in \mathrm{D}_\leq(PE)} \max\left\{\widetilde{\lambda} \in \mathbb{R} : \mathbb{1}_X \otimes 2^{-\widetilde{\lambda}} \widetilde{M}_{PE} \geq \widetilde{\rho}_{XPE}\right\} \ , \tag{102}$$

where $\mathrm{D}_\leq$ is the set of sub-normalized states. One can see from these definitions it would be sufficient to show the optimal solution for $H^\varepsilon_{\min}(YX|PE)_{V\rho V^\dagger}$ is a feasible solution for $H^\varepsilon_{\min}(X|PE)_\rho$ to prove Eq. (99). Suppose the optimal solution of $H^\varepsilon_{\min}(YX|PE)_{V\rho V^\dagger}$ is taken at $(\overline{\lambda}, \overline{M}_{PE}, \overline{\rho}_{YXPE})$ where $\overline{\rho}_{YXPE}$ is chosen as a CCCQ state by [34, Lemma 6.13]. This gives

$$\mathbb{1}_Y \otimes \mathbb{1}_X \otimes 2^{-\overline{\lambda}} \overline{M}_{PE} \geq \overline{\rho}_{YXPE} := \sum_{(y,x,p)} |y\rangle\langle y| \otimes |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes \overline{\rho}_E^{(y,x,p)} \ . \tag{103}$$

Applying the pinching map $\Delta_P(\cdot) := \sum_p |p\rangle\langle p| \cdot |p\rangle\langle p|$ on both sides, we get

$$\sum_{(y,x,p)} |y\rangle\langle y| \otimes |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes 2^{-\overline{\lambda}} \overline{M}_E^{(p)} \geq \sum_{(y,x,p)} |y\rangle\langle y| \otimes |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes \overline{\rho}_E^{(y,x,p)}, \tag{104}$$

with $\overline{M}_E^{(p)} := \langle p|\overline{M}_{PE}|p\rangle$. We can further 'un-compute' Y by applying $V^\dagger \cdot V$ on both sides,

$$\sum_{(x,p)} |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes 2^{-\overline{\lambda}} \overline{M}_E^{(p)} \geq \sum_{(x,p)} |x\rangle\langle x| \otimes |p\rangle\langle p| \otimes \overline{\rho}_E^{(f(x,p),x,p)}, \tag{105}$$

which is equivalent to

$$\mathbb{1}_X \otimes 2^{-\overline{\lambda}} \sum_p |p\rangle\langle p| \otimes \overline{M}_E^{(p)} \geq V^\dagger \overline{\rho}_{YXPE} V \ . \tag{106}$$

Since $V^\dagger \cdot V$ is a CPTNI map, we know that the purified distance cannot increase under this map. Therefore,

$$P(V^\dagger \overline{\rho}_{YXPE} V, \rho_{XPE}) \leq P(\overline{\rho}_{YXPE}, V\rho_{XPE} V^\dagger) \leq \varepsilon, \tag{107}$$

where the second inequality follows by the assumption of $\overline{\rho}_{YXPE}$. Thus, it is the case that $(\overline{\lambda}, \sum_p |p\rangle\langle p| \otimes \overline{M}_E^{(p)}, V^\dagger \overline{\rho}_{YXPE} V)$ is a feasible solution for $H^\varepsilon_{\min}(X|PE)_\rho$, which implies Eq. (99). $\square$

D.3 Entropy Accumulation subprotocol with smoothing

Here we present the equivalent of Theorem 4. The proof is the same as in the main text except that we need to use the smooth min-entropy EAT (Proposition 8).

Theorem 14. *Consider the entropy accumulation protocol defined in Protocol 3 where the announcements $\widetilde{A}_i$'s and $\widetilde{B}_i$'s satisfy Assumption 1. Let $\Omega = \{x_1^n \in \mathcal{X}^n : \mathsf{freq}(x_1^n) \in \mathcal{Q}\}$ and ρ be the output of the protocol. Let h such that $f(\boldsymbol{q}) \geq h$ for all $\boldsymbol{q} \in \mathcal{Q}$ where f is the min-tradeoff function generated by Algorithm 1 or Algorithm 2. Then for any $\alpha \in (1, 2)$, $\varepsilon_{\mathrm{EA}}, \bar{\varepsilon} \in (0, 1)$, either the protocol aborts with probability greater than $1 - \varepsilon_{\mathrm{EA}}$, or*

$$H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n \overline{B}_1^n | \widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega}} > nh - n\frac{(\alpha-1)\ln 2}{2}V^2 - \frac{1}{\alpha-1}\log\frac{2}{\bar{\varepsilon}^2 \varepsilon_{\mathrm{EA}}^2} - n(\alpha-1)^2 K_\alpha \quad (108)$$

where V and K_α are given by Eqs. (91) and (92) and we replace $\rho[\Omega]$ by $\varepsilon_{\mathrm{EA}}$.

Moreover, the bound can be further optimized by using Eq. (90) and optimizing over α.

D.4 QKD security proof with smooth entropies

Here we present the equivalent of Theorem 5. The proof is similar, but we include it for completeness.

Theorem 15. *Consider any QKD protocol which follows Protocol 1 and satisfies Assumption 1. Let $\bar{\varepsilon}, \varepsilon_{\mathrm{PA}}, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{acc}} \in (0, 1)$ such that $\varepsilon_{\mathrm{acc}} \geq \bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}$. Let h such that $f(\boldsymbol{q}) \geq h$ for all $\boldsymbol{q} \in \mathcal{Q}$ where f is the min-tradeoff function generated by Algorithm 1 or Algorithm 2. For $\alpha \in (1, 2)$, the QKD protocol is $\varepsilon_{\mathrm{acc}}$-secure for key length*

$$\begin{aligned}
\ell \leq{}& nh - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} - n\frac{(\alpha-1)\ln 2}{2}V^2 - n(\alpha-1)^2 K_\alpha - n\gamma\log(|\mathcal{A}||\mathcal{B}|) \\
& - 2\sqrt{n}\log(1 + 2d_S)\sqrt{1 - 2\log(\bar{\varepsilon}/4 \cdot \varepsilon_{\mathrm{acc}})} - \frac{1}{\alpha-1}\log\frac{32}{(\bar{\varepsilon} \cdot \varepsilon_{\mathrm{acc}})^2} \\
& - 2\log\left(1 - \sqrt{1 - (\bar{\varepsilon}/4)^2}\right) - 2\log(2/\varepsilon_{\mathrm{PA}})
\end{aligned} \quad (109)$$

where V and K_α are given by Eqs. (91) and (92), $\mathcal{A}$ and $\mathcal{B}$ are the alphabets of private outcomes Alice and Bob will announce excluding the symbol $\perp$, $d_S = (|\mathcal{A}| + 1)(|\mathcal{B}| + 1)$, $\mathrm{leak}_{\varepsilon_{\mathrm{EC}}}$ is the amount of information leaked during error correction.

Proof. By the equivalence of Protocol 1 and Protocol 2, which is by construction, proving the security of Protocol 1 is equivalent to proving the security of Protocol 2. We refer to Protocol 2 in the proof, but this is just for the ease of the reader to link to the main text and Protocol 2's sequential presentation. Let Ω' be the event that Protocol 3 does not abort (i.e. Ω is satisfied) and error correction succeeds (i.e. $\mathrm{hash}(\mathbf{Z}) = \mathrm{hash}(\widehat{\mathbf{Z}})$). Let Ω'' be the event that Protocol 2 does not abort and error correction verification succeeds. Let $\tilde{\rho}_{|\Omega''}$ be the output of the Protocol 2 conditioned on not aborting and error correction succeeding and $\rho_{|\Omega'}$ be the output of Protocol 3 conditioned on not aborting *and* error correction being applied and succeeding.

Fundamentally, we are interested in the entropy of the raw key which excludes the sifted registers or the registers used for parameter estimation. As defined in Protocol 2, $\mathbf{Z} \equiv \overline{A}_1^n \setminus (\overline{A}_{\mathcal{S}} \cup \overline{A}_{\mathcal{T}})$. However, we note that Alice announces $\overline{A}_{\mathcal{T}}$, making it part of what is conditioned on, and $\overline{A}_{\mathcal{S}}$ is determined entirely by the registers $\widetilde{A}_1^n$, $\widetilde{B}_1^n$, and T_1^n. Therefore, by Lemma 4, we can conclude:

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{Z}|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} CE)_{\tilde{\rho}_{|\Omega''}} = H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} CE)_{\tilde{\rho}_{|\Omega''}} \ .$$

We can handle the classical communication cost of error correction by [34, Lemma 6.17]:

$$H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} CE)_{\tilde{\rho}_{|\Omega''}} \geq H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\tilde{\rho}_{|\Omega''}} - \text{leak}_{\varepsilon_{\text{EC}}} \tag{110}$$

$$= H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}^n \widetilde{B}^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} - \text{leak}_{\varepsilon_{\text{EC}}} \tag{111}$$

where C is the register storing the classical communication due to error correction, and the equality comes from noting that $\rho_{\overline{A}_1^n \widetilde{A}_1^n \widetilde{B}_1^n T_1^n X_1^n E_{|\Omega'}} = \tilde{\rho}_{\overline{A}_1^n \widetilde{A}_1^n \widetilde{B}_1^n T_1^n X_1^n E_{|\Omega''}}$. We stress that Bob's private register, $\overline{B}_i^n$, for both the EAT and the QKD protocol, is excluded in the equality as they differ. We note that $\overline{A}_{\mathcal{T}}$ is conditioned upon as Alice publicly announced it, but X_1^n is not conditioned upon as Bob computes it locally and does not need to announce it unless aborting.

With all of this addressed, we can conclude that we would like to do privacy amplification using the smooth min-entropy term:

$$H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} \ . \tag{112}$$

This imposes one major difficulty: we need to find a way to relate this to the term $H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n \overline{B}_1^n|\widetilde{A}^n \widetilde{B}^n T_1^n E)_{\rho_{|\Omega'}}$ on the left-hand side of Eq. (108).

Following derivations in the DI-QKD setting [18], but also handling the $\overline{A}_{\mathcal{T}}$ register, we use the following series of claims:

$$H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}}$$

$$\geq H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n \overline{A}_{\mathcal{T}} \overline{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}}$$

$$\geq H_{\min}^{\bar{\varepsilon}/4}(\overline{A}_1^n \overline{B}_1^n \overline{A}_{\mathcal{T}}|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} - H_{\max}^{\bar{\varepsilon}/4}(\overline{B}_1^n \overline{A}_{\mathcal{T}}|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} - 2\log\left(1 - \sqrt{1 - (\bar{\varepsilon}/4)^2}\right)$$

$$\geq H_{\min}^{\bar{\varepsilon}/4}(\overline{A}_1^n \overline{B}_1^n|\widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} - H_{\max}^{\bar{\varepsilon}/4}(\overline{B}_1^n \overline{A}_{\mathcal{T}}|T_1^n E)_{\rho_{|\Omega'}} - 2\log\left(1 - \sqrt{1 - (\bar{\varepsilon}/4)^2}\right) \ . \tag{113}$$

The first inequality holds by data-processing. The second inequality follows from [34, Eq. (6.60)]. The third inequality comes from data-processing for the smooth max-entropy term and applying Lemma 4 to remove $\overline{A}_{\mathcal{T}}$ in the smooth min-entropy term. More specifically, the strong subadditivity follows from the data-processing inequality of smooth max-entropy of [34, Theorem 6.19] where we have applied the partial trace map on the side information.

Now all that is left is to bound the max-entropy term using the original version of EAT (Theorem 11) [16]. To do this we use the EAT in the form of Theorem 11 with the replacements $S_i \to \overline{A}_{\mathcal{T}_i} \overline{B}_i$, $P_i \to T_i$, and $E \to E$. We note it is okay to use $\overline{A}_{\mathcal{T}}$ as we may treat it as if it were actually n registers where it is $\perp$ whenever $T_i \neq 0$. The Markov conditions trivially hold since T_i uses seeded randomness. Then using the fact that $\overline{A}_{\mathcal{T}_i} \overline{B}_i = \perp \times \perp$ except when $T_i = 1$ which happens with probability γ, we construct the max-tradeoff function analytically by the following observation:

$$H(\overline{A}_{\mathcal{T}_i} \overline{B}_i|T_i R')_{\mathcal{M}_i(\omega)} \leq H(\overline{A}_{\mathcal{T}_i} \overline{B}_i|T_i)_{\mathcal{M}_i(\omega)}$$

$$= (1 - \gamma)H(\overline{A}_{\mathcal{T}_i} \overline{B}_i|T_i = 0)_{\mathcal{M}_i(\omega)} + \gamma H(\overline{A}_{\mathcal{T}_i} \overline{B}_i|T_i = 1)_{\mathcal{M}_i(\omega)}$$

$$\leq \gamma \log|\mathcal{A} \times \mathcal{B}| \tag{114}$$

where $\mathcal{A}$ and $\mathcal{B}$ are the alphabets of private outcomes Bob utilizes during parameter estimation. This tells us we can let the max-tradeoff function $f_{\max}(\boldsymbol{q}) = \gamma \log |\mathcal{A} \times \mathcal{B}|$ for all $\boldsymbol{q} \in \mathbb{P}(\mathcal{X})$. This also implies $\|\nabla f_{\max}\|_\infty = 0$. Therefore, using this with Theorem 11 we get

$$H_{\max}^{\bar{\varepsilon}/4}(\overline{B}_1^n \overline{A}_{\mathcal{T}} | T_1^n E)_{\rho_{|\Omega'}} \leq n\gamma \log |\mathcal{A} \times \mathcal{B}| + \sqrt{n}\, 2 \log(1 + 2d_S)\sqrt{1 - 2\log(\bar{\varepsilon}/4 \cdot \varepsilon_{\mathrm{acc}})} \qquad (115)$$

where we have assumed $\rho[\Omega'] \geq \varepsilon_{\mathrm{acc}}$, and $d_S := (|\mathcal{A}|+1)(|\mathcal{B}|+1)$ using that $|\overline{B}_i| = |\mathcal{B}|+1, |\overline{A}_{\mathcal{T},i}| = |\mathcal{A}| + 1$.

We now put all of these together to get the following:

$$\begin{aligned}
H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n | \widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} \geq\ & H_{\min}^{\bar{\varepsilon}/4}(\overline{A}_1^n \overline{B}_1^n | \widetilde{A}_1^n \widetilde{B}_1^n T_1^n E)_{\rho_{|\Omega'}} - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} - n\gamma \log(|\mathcal{A} \times \mathcal{B}|) \\
& - 2\sqrt{n} \log(1 + 2d_S)\sqrt{1 - 2\log(\bar{\varepsilon}/4 \cdot \varepsilon_{\mathrm{acc}})} \\
& - 2\log\left(1 - \sqrt{1 - (\bar{\varepsilon}/4)^2}\right)\ .
\end{aligned} \qquad (116)$$

We now apply Theorem 14 to the right-hand-side min-entropy term (with appropriate choice of $\bar{\varepsilon}/4$ and $\varepsilon_{\mathrm{EA}} \to \varepsilon_{\mathrm{acc}}$) so that we have that either the input state aborts with probability greater than $1 - \varepsilon_{\mathrm{acc}}$ or

$$\begin{aligned}
& H_{\min}^{\bar{\varepsilon}}(\overline{A}_1^n | \widetilde{A}_1^n \widetilde{B}_1^n T_1^n \overline{A}_{\mathcal{T}} E)_{\rho_{|\Omega'}} \\
& \geq nh - \mathrm{leak}_{\varepsilon_{\mathrm{EC}}} - n\frac{(\alpha - 1)\ln 2}{2} V^2 - n(\alpha - 1)^2 K_\alpha - n\gamma \log(|\mathcal{A} \times \mathcal{B}|) \\
& \quad - 2\sqrt{n} \log(1 + 2d_S)\sqrt{1 - 2\log(\bar{\varepsilon}/4 \cdot \varepsilon_{\mathrm{acc}})} - 2\log\left(1 - \sqrt{1 - (\bar{\varepsilon}/4)^2}\right) \\
& \quad - \frac{1}{\alpha - 1}\log\frac{32}{(\bar{\varepsilon} \cdot \varepsilon_{\mathrm{acc}})^2}\ .
\end{aligned} \qquad (117)$$

Applying the leftover hash lemma [13] (Theorem 13) completes the proof.

The proof of the security claim is nearly identical to the non-smooth case. We consider two mutually exclusive and exhaustive cases. When $\rho[\Omega] < \varepsilon_{\mathrm{acc}}$, then the output is trivially $\varepsilon_{\mathrm{acc}}$-secure. Now consider $\rho[\Omega]$. Starting from the subnormalized state[22] $\rho_{S_A EF}$ where $S_A := h(\mathbf{Z})$ is the hashed key, h is the hash function, and F is the announcement of the hash function,

$$\begin{aligned}
\frac{1}{2}\|\rho_{S_A EF} - |S_A|^{-1}\mathbb{1}_{S_A} \otimes \rho_{EF}\|_1 =\ & \frac{1}{2}\rho[\Omega']\|\rho_{S_A F_{|\Omega'}} - |S_A|^{-1}\mathbb{1}_{S_A} \otimes \rho_{EF_{|\Omega'}}\|_1 \\
\leq\ & \frac{1}{2}\|\rho_{S_A F_{|\Omega'}} - |S_A|^{-1}\mathbb{1}_{S_A} \otimes \rho_{EF_{|\Omega'}}\|_1\ , \\
\leq\ & \varepsilon_{\mathrm{sec}} = \bar{\varepsilon} + \varepsilon_{\mathrm{PA}}
\end{aligned}$$

where the second inequality is by theorem 12 along with the definition of $\varepsilon_{\mathrm{sec}}$ in Theorem 13 by choosing $\varepsilon' \to \bar{\varepsilon}$. The final inequality is by the definition $\varepsilon_{\mathrm{PA}} := \varepsilon_{\mathrm{sec}} - \varepsilon'$ in Theorem 13. The correctness argument is the same as in the unsmoothed proof. Therefore we the key is $\max\{\varepsilon_{\mathrm{acc}}, \bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}\}$-secure. As in the previous proofs, note that if $\varepsilon_{\mathrm{acc}} < \bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}$, you could improve the key rate without changing the security claim by setting $\varepsilon_{\mathrm{acc}} = \bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}$. This completes the proof. $\qquad \square$

---

[22]Subnormalization is due to aborting the protocol on the input

E   Key Rate Optimization Based on Quantum Conditional Entropy

We find a way to represent Eve's conditional states in terms of Alice's and Bob's joint state and express the quantum conditional entropy $H(S_i|P_iR)$ with those conditional states. (We use register R to refer to Eve's register in a single round as depicted in Figure 1.) We then show this function is convex. We write the objective function based on the quantum conditional entropy as

$$W(\rho) := H(S_i|P_iR)_\rho, \tag{118}$$

for $\rho \in D(Q_i)$. Proposition 1 gives us a more explicit expression of $W(\rho)$ in terms of $\rho \in D(Q_i)$ and Alice's and Bob's joint POVM. The convexity of $W(\rho)$ is given in Proposition 9. We now prove Proposition 1.

Proof of Proposition 1. Recall from the definition of conditional entropy that for a classical-quantum state $\rho_{S_iP_iR} = \sum_{s,p} |s\rangle\langle s|_{S_i} \otimes |p\rangle\langle p|_{P_i} \otimes \rho_R^{(s,p)}$, we have $H(S_i|P_iR) = \sum_{s,p} H(\rho_R^{(s,p)}) - \sum_p H(\rho_R^{(p)})$, where $\rho_R^{(p)} = \sum_s \rho_R^{(s,p)}$. We need to find the marginal states $\rho_R^{(s,p)} = \mathrm{Tr}_{AB}[(M_{sp} \otimes \mathbb{1}_R)\rho_{Q_iR}]$. Without loss of generality, we can write the purifying state as $\rho_{Q_iR} = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \sqrt{\rho} \otimes \mathbb{1}_R |\Phi^+\rangle$ and $|\Phi^+\rangle = \sum_j |j\rangle_{Q_i} |j\rangle_R$, from which we find

$$\begin{aligned}
\rho_R^{(s,p)} &= \mathrm{Tr}_{Q_i}[(M_{sp} \otimes \mathbb{1}_R)\rho_{Q_iR}] \\
&= \mathrm{Tr}_{Q_i}[(\sqrt{\rho}M_{sp}\sqrt{\rho} \otimes \mathbb{1}_R)|\Phi^+\rangle\langle\Phi^+|] \\
&= \sum_{s,p} (\sqrt{\rho}M_{sp}\sqrt{\rho})^T .
\end{aligned} \tag{119}$$

By the fact that for any operator A, $(A^\dagger A)$ and $(A^\dagger A)^T$ have the same spectrum, it is the case that $H(\rho_R^{(s,p)}) = H\big([(\sqrt{\rho}K_{sp})(K_{sp}\sqrt{\rho})]^T\big) = H(K_{sp}\rho K_{sp}) = H(K_{sp}\rho K_{sp}^\dagger)$ and a similar expression holds for $H(\rho_R^{(p)})$. $\qquad\square$

Proposition 9. *The function $W(\rho)$ is convex.*

Proof. Let $\bar\rho_Q = \sum_\lambda p_\lambda \rho_Q^\lambda$ be a convex decomposition of $\bar\rho_Q$. We want to show that

$$\sum_\lambda p_\lambda W(\rho_Q^\lambda) \geq W(\bar\rho_Q). \tag{120}$$

Let ρ_{QR}^λ be the purification of ρ_Q^λ. From these, we define the state $\rho_{QR\Lambda} = \sum_\lambda p_\lambda \rho_{QR}^\lambda \otimes |\lambda\rangle\langle\lambda|_\Lambda$, which satisfies $\mathrm{Tr}_{R\Lambda}[\rho_{QR\Lambda}] = \bar\rho_Q$. Then

$$\sum_\lambda p_\lambda W(\rho_Q^\lambda) := \sum_\lambda p(\lambda) H(S|PR)_{\widetilde{\mathcal{M}} \otimes \mathcal{I}_R(\rho_{QR}^\lambda)} \tag{121}$$

$$= H(S|PR\Lambda)_{\widetilde{\mathcal{M}} \otimes \mathcal{I}_{R\Lambda}(\rho_{QR\Lambda})} \tag{122}$$

$$\geq H(S|PR)_{\widetilde{\mathcal{M}} \otimes \mathcal{I}_R(\bar\rho_{QR})} \tag{123}$$

$$:= W(\bar\rho_Q) \tag{124}$$

where $\bar\rho_{QR}$ is the purification of $\bar\rho_Q$ and where the inequality comes from subadditivity because the entropy will be minimized when Eve holds a purification of $\bar\rho_Q$. $\qquad\square$

The physical intuition of the proof is the fact that if Eve has a family of states ρ_Q^λ that she sends out with probability $p(\lambda)$, while keeping their purification, then that attack will be suboptimal. This is because it is better to send out the average state $\bar\rho_Q = \sum_\lambda p(\lambda)\rho_Q^\lambda$ and keep

the corresponding purification, as this produces the same measurement statistics and Eve holds more information about the state.

As mentioned in the main text, we need to introduce a small perturbation to guarantee that the gradient $\nabla W(\rho)$ is well-defined for any $\rho \geq 0$. To do so, we introduced the perturbed objective function $W_\epsilon(\rho)$, which is

$$W_\epsilon(\rho) = \sum_{s,p} H\left(\mathcal{K}_{sp}^\epsilon(\rho)\right) - \sum_p H\left(\mathcal{K}_p^\epsilon(\rho)\right). \tag{125}$$

Then the gradient $\nabla W_\epsilon(\rho)$ always exists for all $\rho \geq 0$:

$$\nabla W_\epsilon(\rho) = -\sum_{s,p}(\mathcal{K}_{sp}^\epsilon)^\dagger \left[\log \mathcal{K}_{sp}^\epsilon(\rho)\right] + \sum_p (\mathcal{K}_p^\epsilon)^\dagger \left[\log \mathcal{K}_p^\epsilon(\rho)\right]. \tag{126}$$

By [28, Lemma 7], we know that

$$\left\|\mathcal{K}_{sp}(\rho) - \mathcal{K}_{sp}^\epsilon(\rho)\right\|_1 \leq \epsilon(d-1) \quad \text{and} \quad \left\|\mathcal{K}_p(\rho) - \mathcal{K}_p^\epsilon(\rho)\right\|_1 \leq \epsilon(d-1). \tag{127}$$

By the continuity of von Neumann entropy (known as Fannes' inequality), it holds for any $\epsilon \in (0, 1/(e(d-1))]$ [23] and any density operator ρ,

$$\left|H\left(\mathcal{K}_{sp}(\rho)\right) - H\left(\mathcal{K}_{sp}^\epsilon(\rho)\right)\right| \leq \zeta_\epsilon \quad \text{and} \quad \left|H\left(\mathcal{K}_p(\rho)\right) - H\left(\mathcal{K}_p^\epsilon(\rho)\right)\right| \leq \zeta_\epsilon. \tag{128}$$

with $\zeta_\epsilon = \epsilon(d-1)\log\frac{d}{\epsilon(d-1)}$. Thus we have Eq. (28) after taking the worst-case scenario among all contributing terms.

F   Proof for the Second Algorithm Construction

F.1   Basic definitions

For completeness, we review some basic definitions. In this appendix, f, g, h denote some general functions. Readers are cautioned not to confuse them with min-tradeoff functions used in the main text.

Definition 8 (Affine hull). *For a set $C \subseteq \mathbb{R}^n$, the* affine hull *of C, denoted by $\mathrm{aff}(C)$, is defined as*

$$\mathrm{aff}(C) = \left\{\sum_{i=1}^k \theta_i x_i : x_1, \ldots, x_k \in C, \sum_{i=1}^k \theta_i = 1 \text{ for some } k \in \mathbb{N}\right\}. \tag{129}$$

We note that the affine hull is the smallest affine set that contains C.

Definition 9 (Relative interior). *The* relative interior *of a set $C \subseteq \mathbb{R}^n$, denoted by $\mathrm{relint}(C)$ is defined as*

$$\mathrm{relint}(C) = \{x \in C : B_r(x) \cap \mathrm{aff}(C) \subseteq C \text{ for some } r > 0\}, \tag{130}$$

where $B_r(x)$ is a ball centered at x with a radius r.

It is often convenient to let a function f be defined over the entire $\mathbb{R}^n$ and let it take the value $+\infty$ outside its domain which is denoted by $\mathrm{dom}(f)$. It is thus interesting to talk about the extended-value extension.

---

[23]Here e is the base of the natural logarithm.

Definition 10 (Extended-value extension)**.** *If $f : \text{dom}(f) \subseteq \mathbb{R}^n \to \mathbb{R}$ is convex, we define its extended-value extension $\tilde{f} : \mathbb{R}^n \to \mathbb{R} \cup \{+\infty\}$ by*

$$\tilde{f}(x) = \begin{cases} f(x) & x \in \text{dom}(f) \\ +\infty & x \notin \text{dom}(f). \end{cases} \tag{131}$$

It is sometimes useful to define the domain of an extension as

$$\text{dom}(\tilde{f}) = \{x \in \mathbb{R}^n : \tilde{f}(x) < \infty\}. \tag{132}$$

F.2   Fenchel duality

We review one form of duality called *Fenchel duality* that is relevant for our algorithm. See [58] for details about Fenchel duality.

Definition 11 (Fenchel conjugate)**.** *The Fenchel conjugate of a function $h : \mathbb{R}^n \to [-\infty, +\infty]$ is the function $h^* : \mathbb{R}^n \to [-\infty, +\infty]$ defined by*

$$h^*(v) = \sup_{x \in \mathbb{R}^n} \{\langle v, x \rangle - h(x)\}. \tag{133}$$

We now state Fenchel's duality theorem [58, Theorem 3.3.5] with the condition for strong duality replaced by Eq. (136) according to [58, page 74, Exercise 20(e)].

Theorem 16 (Fenchel duality, [58, Theorem 3.3.5])**.** *For given functions $f : \mathbb{R}^n \to (-\infty, +\infty]$ and $g : \mathbb{R}^m \to (-\infty, +\infty]$ and a (bounded) linear map $A : \mathbb{R}^n \to \mathbb{R}^m$, let $p, d \in [-\infty, +\infty]$ be primal and dual values in the following Fenchel problems:*

$$p = \inf_{x \in \mathbb{R}^n} \{f(x) + g(Ax)\}, \tag{134}$$

$$d = \sup_{v \in \mathbb{R}^m} \{-f^*(A^\dagger v) - g^*(-v)\}. \tag{135}$$

These values satisfy the weak duality $p \geq d$.
  If f and g are convex and satisfy the condition

$$\text{relint}(\text{dom}(g)) \cap A \, \text{relint}(\text{dom}(f)) \neq \emptyset, \tag{136}$$

where $A \, \text{relint}(\text{dom}(f)) = \{Ax : x \in \text{relint}(\text{dom}(f))\}$, then the strong duality holds; i.e., $p = d$, and the supremum in the dual problem [Eq. (135)] is attained if $d < +\infty$.

We note that although the formulation of this theorem is for unconstrained optimization, one can easily handle constrained optimization by the extended-value extension. Similarly, one can define an indicator function for a set C by

$$\delta_C(x) = \begin{cases} 0 & \text{if } x \in C \\ \infty & \text{if } x \notin C, \end{cases} \tag{137}$$

and use this indicator function to convert a constraint set C into a part of the objective function.

F.3 Deriving dual problem of Eq. (44)

In this section, let $\mathcal{H}$ be a Hilbert space and define a map that stores the measurement outcomes of the POVM $\{M_\lambda\}$ with associated alphabet $\mathcal{X}$ for outcomes as

$$\Phi_{\mathcal{M}}(\sigma) = \sum_{\lambda \in \mathcal{X}} \mathrm{Tr}(\sigma M_\lambda) \, |\lambda\rangle . \tag{138}$$

Let W be the quantum conditional entropy function in Eq. (24). Let $m = |\mathcal{X}|$ be the number of outcomes. We define the set

$$\mathcal{F}_{\mathrm{dual}} := \{\boldsymbol{f} \in \mathbb{R}^m : \boldsymbol{f} \cdot \Phi_{\mathcal{M}}(\rho) \leq W(\rho) \; \forall \rho \in \mathrm{D}(\mathcal{H})\} . \tag{139}$$

It is also easy to see that $\mathcal{F}_{\mathrm{dual}}$ is a convex set. Moreover, we can write the indicator function [see Eq. (137)] for the set $\mathcal{F}_{\mathrm{dual}}$ in a useful way by the following lemma.

Lemma 5. *Let $\delta_{\mathcal{F}_{dual}}$ be the indicator function for the set $\mathcal{F}_{dual}$. Then,*

$$\sup_\rho \{\langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho)\rangle - W(\rho) : \rho \in \mathrm{Pos}(\mathcal{H})\} = \delta_{\mathcal{F}_{dual}}(\boldsymbol{f}) \; \forall \boldsymbol{f} \in \mathbb{R}^m . \tag{140}$$

Proof. Let $\alpha(\boldsymbol{f}) := \sup_\rho\{\langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho)\rangle - W(\rho) : \rho \in \mathrm{Pos}(\mathcal{H})\}$.

If $\boldsymbol{f} \in \mathcal{F}_{\mathrm{dual}}$, then $\langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho)\rangle - W(\rho) \leq 0$ for any $\rho \in \mathrm{D}(\mathcal{H})$. As any positive operator can be scaled from $\rho \in \mathrm{D}(\mathcal{H})$ by a non-negative coefficient, it is the case that $\alpha \leq 0$. Thus, $\alpha(\boldsymbol{f}) = 0$ with $\rho = 0$.

If $\boldsymbol{f} \notin \mathcal{F}_{\mathrm{dual}}$, then there exists $\rho_0 \in \mathrm{D}(\mathcal{H})$ such that $\langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho_0)\rangle - W(\rho_0) > 0$. Let $\gamma = \langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho_0)\rangle - W(\rho_0)$ and $\rho_\beta = \beta\rho_0$ with $\beta \geq 0$. We notice that $W(\beta\rho) = \beta W(\rho)$ for any $\beta \geq 0$. Because $\Phi_{\mathcal{M}}$ is linear, with ρ_β, it is the case that $\alpha(\boldsymbol{f}) > \beta\gamma$. With $\beta \to \infty$, $\alpha(\boldsymbol{f}) \to \infty$. Thus, Eq. (140) holds. $\qquad\square$

To derive the dual problem of Eq. (44), we first compute the Fenchel conjugate of two functions that will become useful.

Lemma 6. *For $c_0 \geq 0$ and $c_1 > 0$, let $s : \mathbb{R} \to \mathbb{R} \cup \{+\infty\}$ be defined as*

$$s(x) = \begin{cases} -\sqrt{c_0^2 - |x|^2/c_1^2} & \text{if } |x| \leq c_0 c_1, \\ \infty & \text{otherwise.} \end{cases} \tag{141}$$

The Fenchel conjugate function of s is

$$s^*(y) = c_0\sqrt{1 + c_1^2 y^2} . \tag{142}$$

Proof. By Definition 11, the conjugate function of s is

$$\begin{aligned} s^*(y) &= \sup_{x \in \mathbb{R}}\{xy - s(x)\} \\ &= \sup_{x \in \mathbb{R}}\{xy + \sqrt{c_0^2 - |x|^2/c_1^2} : |x| \leq c_0 c_1\} \end{aligned} \tag{143}$$

By a simple calculation to optimize over x, it is easy to verify that Eq. (142) is indeed the conjugate function of s.[24] $\qquad\square$

---

[24] To find the supremum, one can solve case by case for two cases: $x \geq 0$ and $x < 0$. For each case, one looks for a solution of x where the derivative is zero by simple computation. Then, one verifies that both solutions in these two cases lead to the same optimal value which is indeed the supremum.

Lemma 7. *For $c_0 \geq 0$ and $c_1 > 0$, let $\mathcal{E}(\boldsymbol{\lambda}) : \mathbb{R}^m \to \mathbb{R} \cup \{+\infty\}$ be defined as*

$$\mathcal{E}(\boldsymbol{\lambda}) = \begin{cases} s(\|\boldsymbol{\lambda}\|_1/2) & \text{if } \sum_x \boldsymbol{\lambda}(x) = 0 \\ \infty & \text{otherwise,} \end{cases} \tag{144}$$

where s is defined in Lemma 6. Then $\mathcal{E}$ is a convex function and its conjugate function $\mathcal{E}^*(\boldsymbol{f})$ is $\mathcal{E}^*(\boldsymbol{f}) = s^*(\max(\boldsymbol{f}) - \min(\boldsymbol{f}))$, that is,

$$\mathcal{E}^*(\boldsymbol{f}) = c_0\sqrt{1 + c_1^2[\max(\boldsymbol{f}) - \min(\boldsymbol{f})]^2} \,. \tag{145}$$

Proof. The convexity of $\mathcal{E}$ follows from the convexity of s and the convexity of the set $\{\boldsymbol{\lambda} \in \mathbb{R}^m : \sum_x \boldsymbol{\lambda}(x) = 0\}$. From Definition 11,

$$\begin{aligned} \mathcal{E}^*(\boldsymbol{f}) &= \sup_{\boldsymbol{\lambda} \in \mathbb{R}^m} \{\langle \boldsymbol{\lambda}, \boldsymbol{f} \rangle - \mathcal{E}(\boldsymbol{\lambda})\} \\ &= \sup_{\boldsymbol{\lambda} \in \mathbb{R}^m} \{\langle \boldsymbol{\lambda}, \boldsymbol{f} \rangle - s(\|\boldsymbol{\lambda}\|_1/2) : \sum_x \boldsymbol{\lambda}(x) = 0\} \\ &= \sup_{\boldsymbol{\lambda} \in \mathbb{R}^m} \{\langle \boldsymbol{\lambda}, \boldsymbol{f} \rangle + \sqrt{c_0^2 - \|\boldsymbol{\lambda}\|_1^2/(4c_1^2)} : \|\boldsymbol{\lambda}\|_1 \leq 2c_0c_1, \sum_x \boldsymbol{\lambda}(x) = 0\} \end{aligned} \tag{146}$$

Let $\boldsymbol{\lambda}_+$ be defined as $\boldsymbol{\lambda}_+(x) = \max(\boldsymbol{\lambda}(x), 0)$ and $\boldsymbol{\lambda}_-$ be defined as $\boldsymbol{\lambda}_-(x) = \max(-\boldsymbol{\lambda}(x), 0)$. Then, it is clear that $\boldsymbol{\lambda} = \boldsymbol{\lambda}_+ - \boldsymbol{\lambda}_1$ and $\|\boldsymbol{\lambda}\|_1 = \|\boldsymbol{\lambda}_+\|_1 + \|\boldsymbol{\lambda}_-\|_1$. The condition $\sum_x \boldsymbol{\lambda}(x) = 0$ implies $\|\boldsymbol{\lambda}_+\|_1 = \|\boldsymbol{\lambda}_-\|_1 = \frac{1}{2}\|\boldsymbol{\lambda}\|_1$. Thus,

$$\begin{aligned} \mathcal{E}^*(\boldsymbol{f}) &= \sup_{\substack{\boldsymbol{\lambda}_+ \in \mathbb{R}^m \\ \boldsymbol{\lambda}_- \in \mathbb{R}^m}} \{\langle \boldsymbol{f}, \boldsymbol{\lambda}_+ \rangle - \langle \boldsymbol{f}, \boldsymbol{\lambda}_- \rangle + \sqrt{c_0^2 - \|\boldsymbol{\lambda}_+\|_1^2/c_1^2} : \|\boldsymbol{\lambda}_+\|_1 = \|\boldsymbol{\lambda}_-\|_1 \leq c_0c_1, \boldsymbol{\lambda}_+ \geq 0, \boldsymbol{\lambda}_- \geq 0\} \\ &= \sup_{\boldsymbol{\lambda}_+ \in \mathbb{R}^m, v \in \mathbb{R}} \{\langle \boldsymbol{f}, \boldsymbol{\lambda}_+ \rangle - v\min(\boldsymbol{f}) + \sqrt{c_0^2 - v^2/c_1^2} : 0 \leq v = \|\boldsymbol{\lambda}_+\|_1 \leq c_0c_1, \boldsymbol{\lambda}_+ \geq 0\} \\ &= \sup_{v \in \mathbb{R}} \{v[\max(\boldsymbol{f}) - \min(\boldsymbol{f})] + \sqrt{c_0^2 - v^2/c_1^2} : 0 \leq v \leq c_0c_1\} \\ &= \sup_{v \in \mathbb{R}} \{v[\max(\boldsymbol{f}) - \min(\boldsymbol{f})] + \sqrt{c_0^2 - v^2/c_1^2} : |v| \leq c_0c_1\} \\ &= \sup_{v \in \mathbb{R}} \{v[\max(\boldsymbol{f}) - \min(\boldsymbol{f})] - s(v)\} \\ &= s^*(\max(\boldsymbol{f}) - \min(\boldsymbol{f})). \end{aligned} \tag{147}$$

In the second line above, we optimize $\boldsymbol{\lambda}_-$ and the optimal value is achieved when $\boldsymbol{\lambda}_-$ contains a single nonzero entry in the position corresponding to $\min(\boldsymbol{f})$. In the third line, we optimize $\boldsymbol{\lambda}_+$ and the optimal value is achieved when $\boldsymbol{\lambda}_+$ contains a single nonzero entry in the position corresponding to $\max(\boldsymbol{f})$. In the fourth line, we drop the constraint $v \geq 0$ since the optimal value is always achieved when $v \geq 0$ due to the fact $\max(\boldsymbol{f}) - \min(\boldsymbol{f}) \geq 0$. In the fifth line, we use the definition of s. The last line follows from the definition of s^*. $\qquad\square$

Proposition 10. *Let $c_0 \geq 0$ and $c_1 > 0$ be constants. For the problem*

$$\begin{aligned} h_{primal}(\boldsymbol{q}_0) := \underset{\rho}{\text{minimize}} \quad & W(\rho) + \sqrt{c_0^2 - \|\boldsymbol{q}_0 - \Phi_{\mathcal{M}}(\rho)\|_1^2/(4c_1^2)} \\ \text{subject to} \quad & \text{Tr}(\rho) = 1 \\ & \|\boldsymbol{q}_0 - \Phi_{\mathcal{M}}(\rho)\|_1 \leq 2c_0c_1 \\ & \rho \geq 0, \end{aligned} \tag{148}$$

its Fenchel dual problem is

$$h_{dual}(\boldsymbol{q}_0) := \underset{\boldsymbol{f}}{\text{maximize}} \quad \boldsymbol{q}_0 \cdot \boldsymbol{f} - c_0 \sqrt{1 + c_1^2 [\max(\boldsymbol{f}) - \min(\boldsymbol{f})]^2} \tag{149}$$

$$\text{subject to} \quad \boldsymbol{f} \cdot \Phi_{\mathcal{M}}(\rho) \leq W(\rho) \ \forall \rho \in \mathrm{D}(\mathcal{H}).$$

Moreover, if there exists $\sigma \in \mathrm{D}(\mathcal{H})$ such that $\Phi_{\mathcal{M}}(\sigma) = \boldsymbol{q}_0$, then $h_{primal}(\boldsymbol{q}_0) = h_{dual}(\boldsymbol{q}_0)$.

Proof. We introduce the indicator function $\delta_{\mathrm{Pos}(\mathcal{H})}$ for the set $\mathrm{Pos}(\mathcal{H})$ (see Eq. (137)). We identify any $\rho \in \mathrm{Pos}(\mathcal{H})$ as an element in $\mathbb{R}^n$ for $n = 4\dim(\mathcal{H})^2$ by representing ρ with its real and imaginary parts, and then applying an appropriate vectorization of ρ. Similarly, we abuse the notation $\Phi_{\mathcal{M}}$ and let it denote the corresponding linear map from $\mathbb{R}^n$ to $\mathbb{R}^m$ where m is the number of POVM elements for this measurement map. To apply Theorem 16, we define $f(\rho) = W(\rho) + \delta_{\mathrm{Pos}(\mathcal{H})}(\rho)$, $g(\boldsymbol{\lambda}) = \mathcal{E}(\boldsymbol{\lambda} - \boldsymbol{q}_0)$ and let $\Phi_{\mathcal{M}}$ play the role of A in the theorem. We first calculate f^* and g^*:

$$f^*(Z) = \sup_{\rho}\{\langle Z, \rho \rangle - f(\rho)\}$$

$$= \sup_{\rho}\{\langle Z, \rho \rangle - W(\rho) : \rho \in \mathrm{Pos}(\mathcal{H})\} \tag{150}$$

$$g^*(\boldsymbol{f}) = \sup_{\boldsymbol{\lambda}}\{\langle \boldsymbol{f}, \boldsymbol{\lambda} \rangle - \mathcal{E}(\boldsymbol{\lambda} - \boldsymbol{q}_0)\}$$

$$= \sup_{\boldsymbol{\lambda}'}\{\langle \boldsymbol{f}, \boldsymbol{\lambda}' \rangle + \langle \boldsymbol{f}, \boldsymbol{q}_0 \rangle - \mathcal{E}(\boldsymbol{\lambda}')\}$$

$$= \mathcal{E}^*(\boldsymbol{f}) + \langle \boldsymbol{f}, \boldsymbol{q}_0 \rangle. \tag{151}$$

Because $\sum_x \boldsymbol{q}_0(x) = 1$ and $\sum_x \Phi_{\mathcal{M}}(\rho)(x) = 1$ for $\mathrm{Tr}(\rho) = 1$, one can use the definition of f and $\mathcal{E}$ to rewrite the problem in Eq. (148) as

$$h_{\mathrm{primal}}(\boldsymbol{q}_0) = \inf_{\rho \in \mathbb{R}^n}\{f(\rho) + \mathcal{E}(\Phi_{\mathcal{M}}(\rho) - \boldsymbol{q}_0)\}$$

$$= \inf_{\rho \in \mathbb{R}^n}\{f(\rho) + g(\Phi_{\mathcal{M}}(\rho))\}. \tag{152}$$

We then use the indicator function for the set $\mathcal{F}_{\mathrm{dual}}$ and the conjugate function $\mathcal{E}^*$ of $\mathcal{E}$ to rewrite Eq. (149) as

$$h_{\mathrm{dual}}(\boldsymbol{q}_0) = \sup_{\boldsymbol{f}}\{-\langle \boldsymbol{q}_0, -\boldsymbol{f} \rangle - \mathcal{E}^*(\boldsymbol{f}) - \delta_{\mathcal{F}_{\mathrm{dual}}}(\boldsymbol{f})\}$$

$$= \sup_{\boldsymbol{f}}\{-g^*(-\boldsymbol{f}) - \delta_{\mathcal{F}_{\mathrm{dual}}}(\boldsymbol{f})\}. \tag{153}$$

By Lemma 5, $\delta_{\mathcal{F}_{\mathrm{dual}}}(\boldsymbol{f}) = \sup_{\rho}\{\langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho) \rangle - W(\rho) : \rho \in \mathrm{Pos}(\mathcal{H})\}$. Using this substitution, we find

$$h_{\mathrm{dual}}(\boldsymbol{q}_0) = \sup_{\boldsymbol{f} \in \mathbb{R}^m} \{-\sup_{\rho}\{\langle \boldsymbol{f}, \Phi_{\mathcal{M}}(\rho) \rangle - W(\rho) : \rho \in \mathrm{Pos}(\mathcal{H})\} - g^*(-\boldsymbol{f})\}$$

$$= \sup_{\boldsymbol{f} \in \mathbb{R}^m} \{-\sup_{\rho}\{\langle \Phi_{\mathcal{M}}^{\dagger}(\boldsymbol{f}), \rho \rangle - W(\rho) : \rho \in \mathrm{Pos}(\mathcal{H})\} - g^*(-\boldsymbol{f})\} \tag{154}$$

$$= \sup_{\boldsymbol{f} \in \mathbb{R}^m} \{-f^*(\Phi_{\mathcal{M}}^{\dagger}(\boldsymbol{f})) - g^*(-\boldsymbol{f})\}.$$

Therefore, the optimization problem in Eq. (149) is the dual problem of the optimization problem in Eq. (148).

To show $h_{\mathrm{primal}}(\boldsymbol{q}_0) = h_{\mathrm{dual}}(\boldsymbol{q}_0)$, we just need to verify the condition

$$\mathrm{relint}(\mathrm{dom}(g)) \cap \Phi_{\mathcal{M}} \, \mathrm{relint}(\mathrm{dom}(f)) \neq \emptyset. \tag{155}$$

From the definition of domain [see Eq. (132)],

$$\text{dom}(g) = \{\boldsymbol{\lambda} \in \mathbb{R}^m : \sum_x \boldsymbol{\lambda}(x) = 1, \|\boldsymbol{\lambda} - \boldsymbol{q_0}\|_1 \leq 2c_0 c_1\}$$

$$\text{dom}(f) = \{\rho \in \mathbb{R}^n : \rho \geq 0\} \tag{156}$$

It is clear that $\boldsymbol{q}_0 \in \text{relint}(\text{dom}(g))$. Moreover, there exists some $\epsilon > 0$ such that $(1 - \epsilon)\boldsymbol{q}_0 + \epsilon \mathbf{1}/m \in \text{relint}(\text{dom}(g))$. We now show that $(1 - \epsilon)\boldsymbol{q}_0 + \epsilon \mathbf{1}/m \in \Phi_{\mathcal{M}}\,\text{relint}(\text{dom}(f))$. By the assumption, there exists $\sigma \in \text{D}(\mathcal{H})$ such that $\Phi_{\mathcal{M}}(\sigma) = \boldsymbol{q}_0$. Then for any $\delta > 0$, it is the case that $\mathcal{D}_\delta(\sigma) \in \text{relint}(\text{dom}(f))$. In particular, $\mathcal{D}_\epsilon(\sigma) \in \text{relint}(\text{dom}(f))$. Since $\Phi_{\mathcal{M}}(\mathcal{D}_\epsilon(\sigma)) = (1-\epsilon)\boldsymbol{q}_0 + \epsilon \mathbf{1}/m$, it is the case that $(1-\epsilon)\boldsymbol{q}_0 + \epsilon \mathbf{1}/m \in \Phi_{\mathcal{M}}\,\text{relint}(\text{dom}(f))$. Therefore, Eq. (155) holds. We conclude that $h_{\text{primal}}(\boldsymbol{q}_0) = h_{\text{dual}}(\boldsymbol{q}_0)$. $\qquad\square$

Since we establish that $h_{\text{primal}}(\boldsymbol{q}_0) = h_{\text{dual}}(\boldsymbol{q}_0)$, we can now solve the primal problem in Eq. (148). The difficulty is that the objective function is not differentiable at points where $\Phi_{\mathcal{M}}(\rho) = \boldsymbol{q}_0$. Since many standard solvers handle differentiable functions more effectively, we introduce a slack variable and rewrite the problem to an equivalent one according to the following lemma.

Lemma 8. *The following optimization problem*

$$
\begin{aligned}
\tilde{h}_{primal}(\boldsymbol{q}_0) := \underset{\rho, \boldsymbol{\xi}}{\text{minimize}} \quad & W(\rho) - \sqrt{c_0^2 - \Big(\sum_x \boldsymbol{\xi}(x)\Big)^2 / (4c_1^2)} \\
\text{subject to} \quad & -\boldsymbol{\xi} \leq \Phi_{\mathcal{M}}(\rho) - \boldsymbol{q}_0 \leq \boldsymbol{\xi} \\
& \sum_x \boldsymbol{\xi}(x) \leq 2c_0 c_1 \\
& \text{Tr}(\rho) = 1 \\
& \rho \geq 0, \ \boldsymbol{\xi} \in \mathbb{R}^{|\mathcal{X}|}
\end{aligned}
\tag{157}
$$

has the same optimal value as the problem in Eq. (148), that is, $\tilde{h}_{primal}(\boldsymbol{q}_0) = h_{primal}(\boldsymbol{q}_0)$.

Proof. We first notice that the function $-\sqrt{c_0^2 - t^2/(4c_1^2)}$ is a monotonically non-decreasing function of $0 \leq t \leq 2c_0 c_1$. For $\boldsymbol{\xi} \geq 0, \|\boldsymbol{\xi}\|_1 = \sum_j \boldsymbol{\xi}(j)$. The condition $-\boldsymbol{\xi} \leq \Phi_{\mathcal{M}}(\rho) - \boldsymbol{q}_0 \leq \boldsymbol{\xi}$ implies that $\boldsymbol{\xi} \geq 0$ and $\|\boldsymbol{\xi}\|_1 \geq \|\boldsymbol{q}_0 - \Phi_{\mathcal{M}}(\rho)\|_1$. Thus, it is clear that $\tilde{h}_{\text{primal}}(\boldsymbol{q}_0) \geq h_{\text{primal}}(\boldsymbol{q}_0)$. Let $\rho^\star$ be an optimal solution for $h_{\text{primal}}(\boldsymbol{q}_0)$ and let $\boldsymbol{\xi}^\star(j) := |\boldsymbol{q}_0(j) - \Phi_{\mathcal{M}}(\rho^\star)(j)|$. Then $\|\boldsymbol{\xi}^\star\|_1 = \|\boldsymbol{q}_0 - \Phi_{\mathcal{M}}(\rho^\star)\|_1 \leq 2c_0 c_1$. This implies, $(\rho^\star, \boldsymbol{\xi}^\star)$ is a feasible solution for $\tilde{h}_{\text{primal}}(\boldsymbol{q}_0)$ that achieves the same objective function value as $h_{\text{primal}}(\boldsymbol{q}_0)$. Therefore, $\tilde{h}_{\text{primal}}(\boldsymbol{q}_0) \leq h_{\text{primal}}(\boldsymbol{q}_0)$. We conclude that $\tilde{h}_{\text{primal}}(\boldsymbol{q}_0) = h_{\text{primal}}(\boldsymbol{q}_0)$. $\qquad\square$