Finite-Key Analysis of Quantum Key Distribution using Entropy Accumulation

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

1 Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, ON, Canada N2L 3G1
2 Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada
3 Department of Electrical & Computer Engineering, University of Illinois, Urbana, Illinois 61801, USA
4 Institute for Quantum Computing, Baidu Research, Beijing 100193, China
* These authors contributed equally

Introduction

Our aim: Computing finite size key rates for QKD against coherent attacks.
Two challenges that need to be addressed:

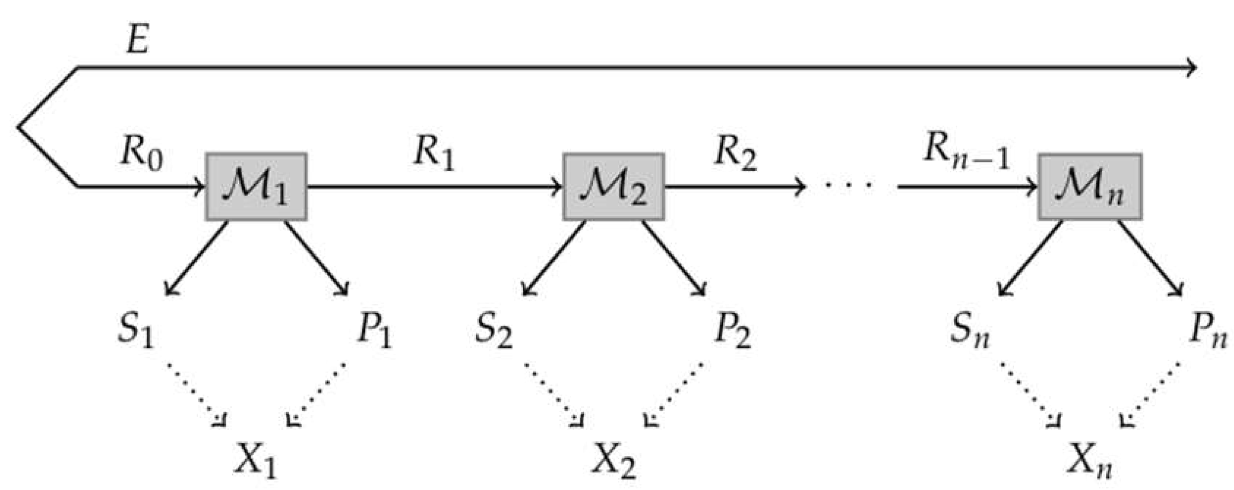
- Cover largest possible class of protocols
- Obtain good key rates (w. r. t. scaling with dimension and block size)

Our method: combine two existing tools

- **Entropy accumulation theorem (EAT) [1,2,3]**
- **Numerical framework [4]** for asymptotic QKD key rates using convex optimization

Our result: Algorithm to compute finite-size key rates for *entanglement-based* QKD protocols which satisfy an *additional restriction* (see sufficient conditions for Markov chain conditions below)

Background: Entropy Accumulation Theorem



Diagrammatic depiction of EAT process. $\mathcal{M}_i$'s are EAT channels, E, R_i's, S_i's and P_i are quantum registers, X_i's are classical registers that are a function of (S_i, P_i).

Definitions (simplified)

EAT Theorem [1,2]: For EAT channels satisfying the Markov chain condition, given a min-tradeoff function f, set of accepted statistics Ω, and $h \in \mathbb{R}$ s.t. $f(\vec{p}) \geq h \; \forall \, \vec{p} \in \Omega$, it is the case that

$$H_{\min}^{\varepsilon}(S_1^n | P_1^n E) \geq nh - O(\sqrt{n}).$$

An **EAT channel** $\mathcal{M}_i$ describes the operation of the device in round i and is a CPTP map $R_{i-1} \to S_i P_i R_i$ composed with a CPTP map $\mathcal{T}_i : S_i P_i \to X_i$

A **min-tradeoff function** f lower bounds the entropy generated per round i for any state admitting statistics $\vec{q}$ under testing $\mathcal{T}_i$ for each possible $\vec{q}$

New sufficient Conditions for Markov Condition

Markov chain conditions:

- The Markov conditions require that $S_1^{i-1} \leftrightarrow P_1^{i-1} E \leftrightarrow P_i \;\; i \in [n]$ hold on the output of the process, i.e., there is a Markov chain structure for all rounds.
- Markov conditions are difficult to verify except in the simple case where the public announcements are privately seeded.
- We identify a more general condition ensuring the Markov chain conditions.

New sufficient conditions:

- The measurements operators are block diagonal.
- In each block, the probability of a given announcement is the same.

Proof Sketch: Eve's optimal attack will also have the block diagonal form. The form guarantees the Markov chain structure on the optimal attack.

Possible Future Work

- Investigate more complicated protocols such as optical implementations
- Generalize results to hold for prepare-and-measure protocols

References

[1] F. Dupuis, O. Fawzi, and R. Renner, Commun. Math.Phys. 379, 867 (2020), arXiv:1607.01796.
[2] F. Dupuis and O. Fawzi, IEEE Trans. Inf. Theory 65,7596 (2019), arXiv:1805.11652.
[3] F. Dupuis, arXiv:2105.05342 (2021).
[4] A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum 2, 77 (2018), arXiv: 1710.05511
[5] R. Tannous, Z. Ye, J. Jin, K. B. Kuntz, N. Lütkenhaus, and T. Jennewein, Appl. Phys. Lett. 115, 211103 (2019).

New algorithms for Min-Tradeoff Functions

We provide two algorithms for construction min-tradeoff functions.

Algorithm 1

Finds optimal min-tradeoff function (asymptotic terms only)

1. Find suboptimal solution $\bar{\rho}$ for the nonlinear SDP for given statistics $\vec{q}$.
2. Solve dual SDP of the linearization at the suboptimal solution.
3. The dual variable gives the coefficients of a valid min-tradeoff function.

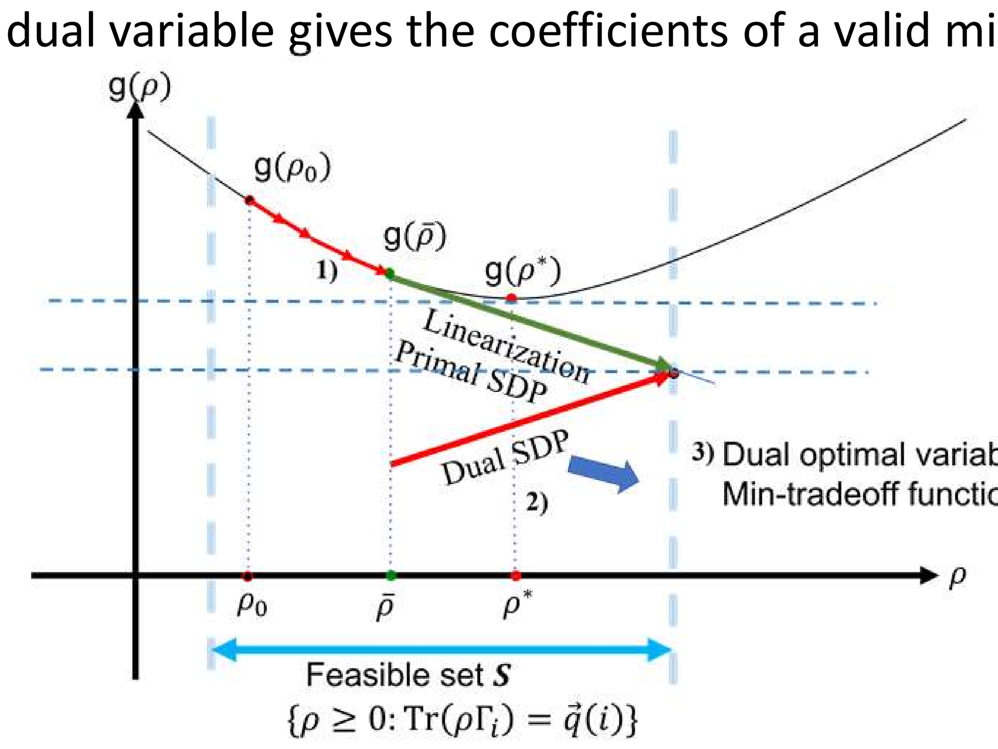
NB: - similar to the asymptotic numerical algorithm [4]
- Optimal min-tradeoff function obtained by optimizing over $\vec{q}$

Algorithm 2

Finds best min-tradeoff function (asymptotic and leading $O\left(\frac{1}{\sqrt{n}}\right)$ corrections)

NB: - Modified objective function compared to of Algorithm 1 to include leading corrections to the key rate from EAT.
- Derive the new primal problem using Fenchel duality

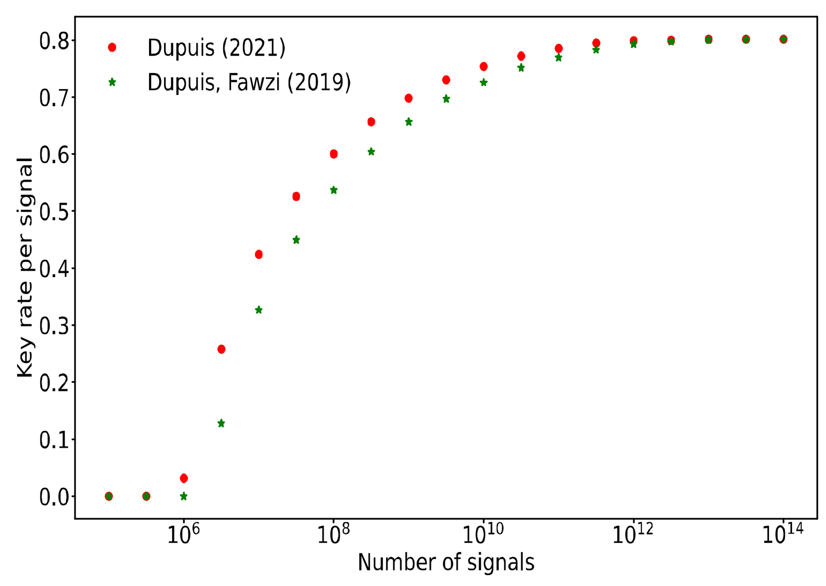
1. Use convex optimization solver to find a suboptimal solution for the primal problem.
2. Solve the dual problem of the linearization.
3. The dual variable gives the coefficients of a valid min-tradeoff function.



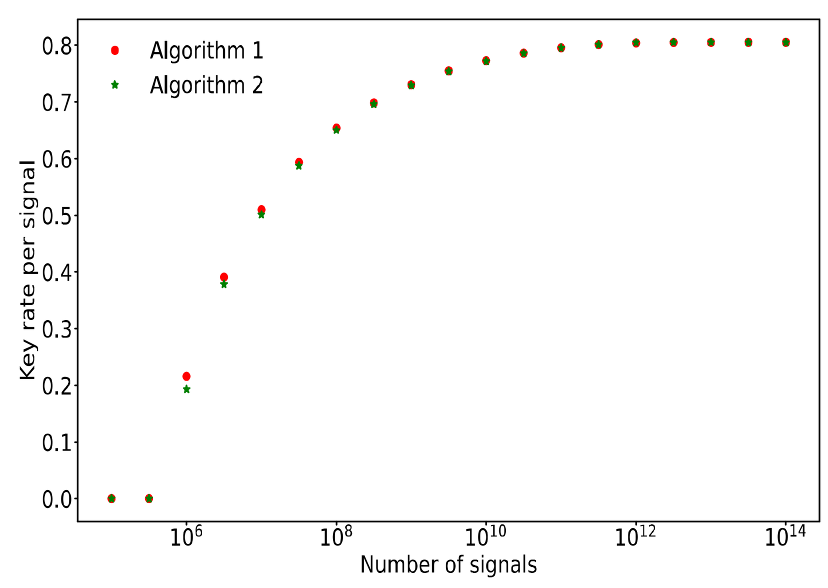
Diagrammatic depiction of algorithms abstractly: g is the objective function.

Applications

Qubit BB84

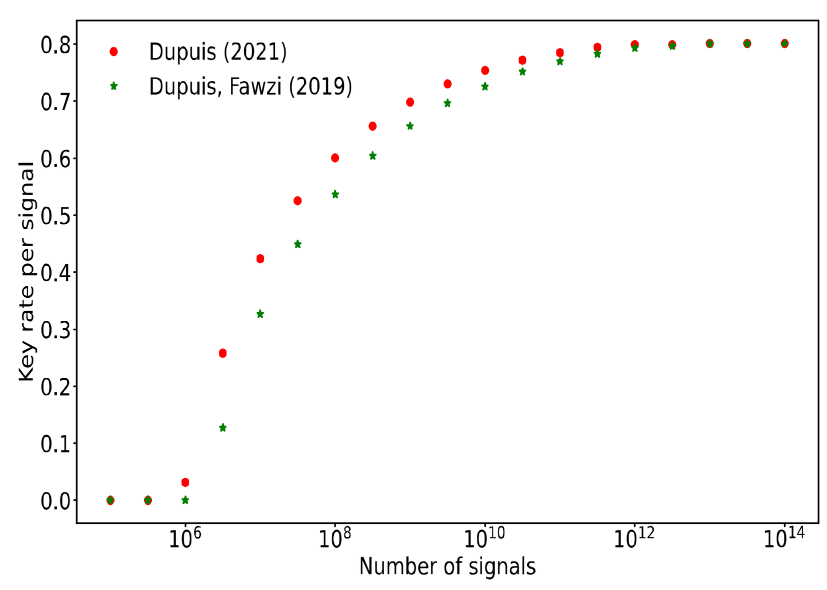


Key rate versus the number of signals by using two versions of EAT for the second-order correction terms: Dupuis, Fawzi (2019) [2] and Dupuis (2021) [3].

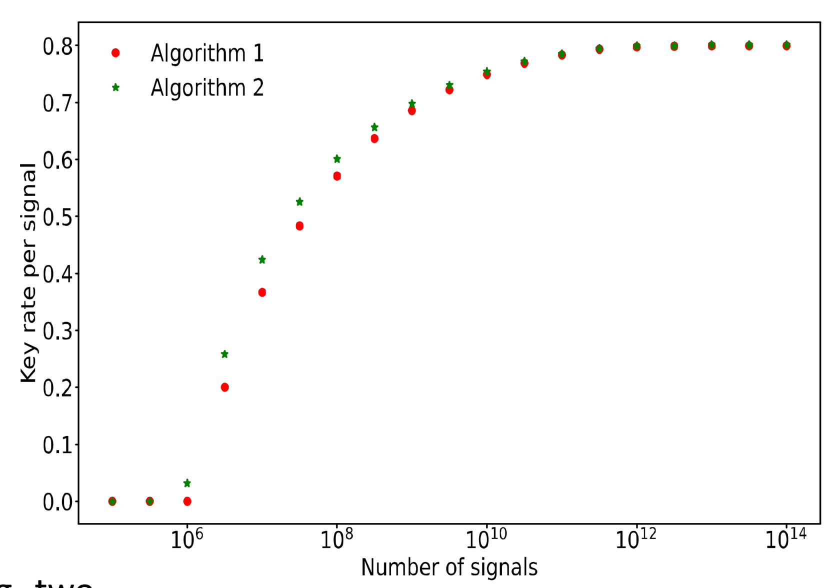


Key rate versus the number of signals for comparison of two algorithms

Six-state four-state protocol [5]

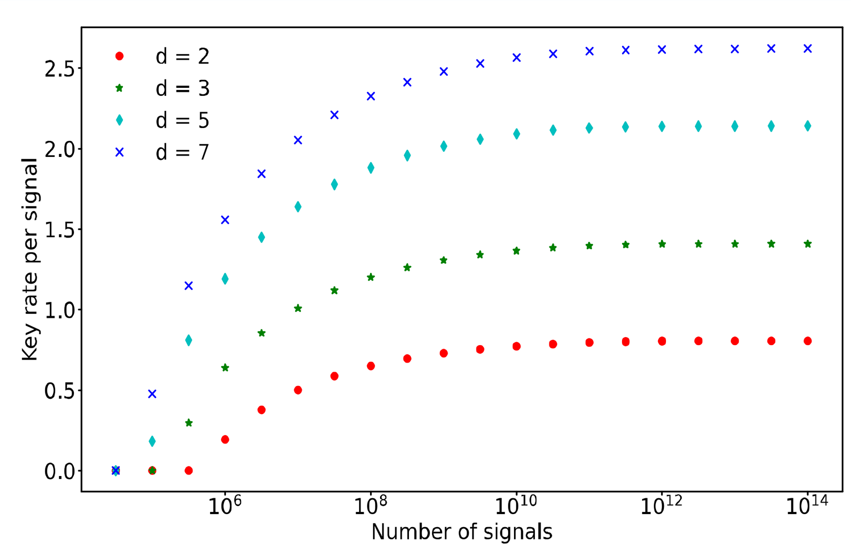


Key rate versus the number of signals by using two versions of EAT for the second-order correction terms: Dupuis, Fawzi (2019) [2] and Dupuis (2021) [3].



Key rate versus the number of signals for comparison of two algorithms

High-dimensional 2-mutually unbiased bases



Key rate versus the number of signals different prime dimension d = 2,3, 5, 7 of the d-dimensional 2-MUB protocol. It uses Algorithm 2 and the second-order correction term from Dupuis (2021) [3].

Canada

NSERC CRSNG

Discovery Grants Program: Grant No. 341495
Collaborative Research and Development Program, Grant No. CRDP J 522308-17

Financial support for this work has been partially provided by Huawei Technologies Canada Co., LTD.