Asymptotic Security Proof for Discrete-Modulated CVQKD without Cutoff Assumption

Twesh Upadhyaya | Thomas van Himbeeck | Jie Lin | Norbert Lütkenhaus

UNIVERSITY OF WATERLOO

IQC Institute for Quantum Computing

Introduction

Goal is to compute tight key rates for DMCVQKD with a small number of modulated states.

Want to harness the existing numerics framework for finite-dimensional optimizations [1][2].

Previous work assumes the state is finite-dimensional; the cutoff assumption. This gives numerically stable results but is not a rigorous security proof [3].

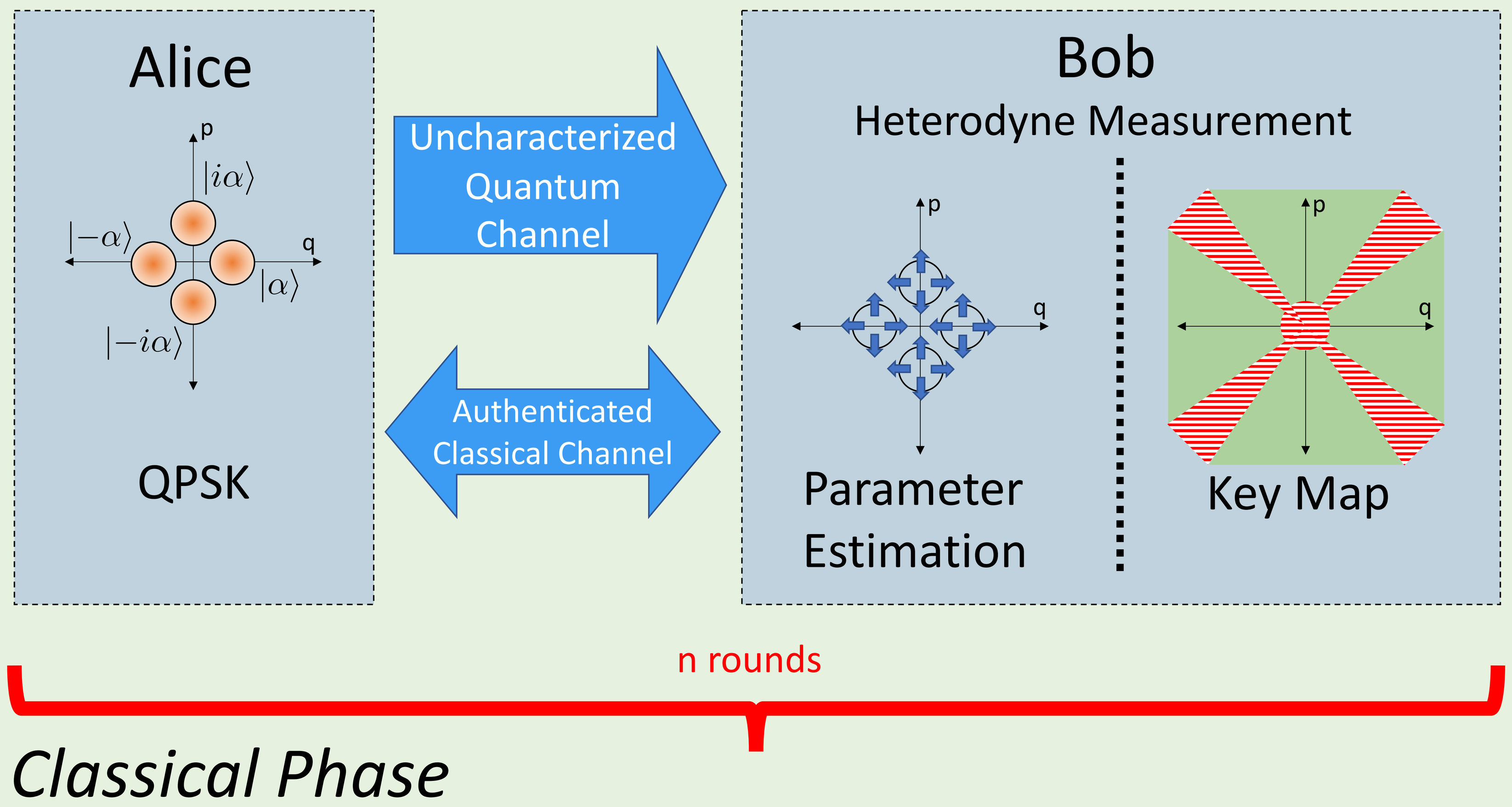
Our Contribution

We establish the asymptotic security of DMCVQKD with a small number of modulated states. In particular, we do not use a cutoff assumption.

We develop a framework to provide tight, reliable key rates for other protocols with infinite-dimensional Hilbert spaces.

Protocol

Quantum Phase



Classical Phase

- Error Correction: Reverse Reconciliation
- Privacy Amplification

Key Rate Formula

Under collective attacks in the asymptotic limit, given by Devetak-Winter formula [4]: $R = I(A:B) - \chi(X:E)$

Evaluated on worst-case state compatible with statistics from parameter estimation; after post-processing.

Reformulate: $R = \min_{\rho \in \mathbf{S}} [H(X|E)] - H(X) + I(A:B)$

If ϕ is the CPTNI map representing the post-processing performed by Alice and Bob, then: $f(\rho) = H(X|E)_{\phi(\rho)}$

Infinite and Finite Optimizations

$$
\begin{aligned}
f(\rho^\infty) = \min\ & f(\rho) \\
\text{subject to:}\ & \\
& \rho \in \mathrm{Pos}(\mathcal{H}_{AB}^\infty) \\
& \mathrm{Tr}(\rho) = 1 \\
& \rho \in \mathbf{S}_\infty
\end{aligned}
\qquad
\begin{aligned}
f(\rho^N) = \min\ & f(\rho) \\
\text{subject to:}\ & \\
& \rho \in \mathrm{Pos}(\mathcal{H}_{AB}^N) \\
& 1 - W \leq \mathrm{Tr}(\rho) \leq 1 \\
& \rho \in \mathbf{S}_N
\end{aligned}
$$

Require: $\Pi_N \mathbf{S}_\infty \Pi_N \subseteq \mathbf{S}_N$

$$W \geq 1 - \mathrm{Tr}(\rho \Pi_N) \quad \forall \rho \in \mathbf{S}_\infty$$

Uniform Continuity of Conditional Entropy

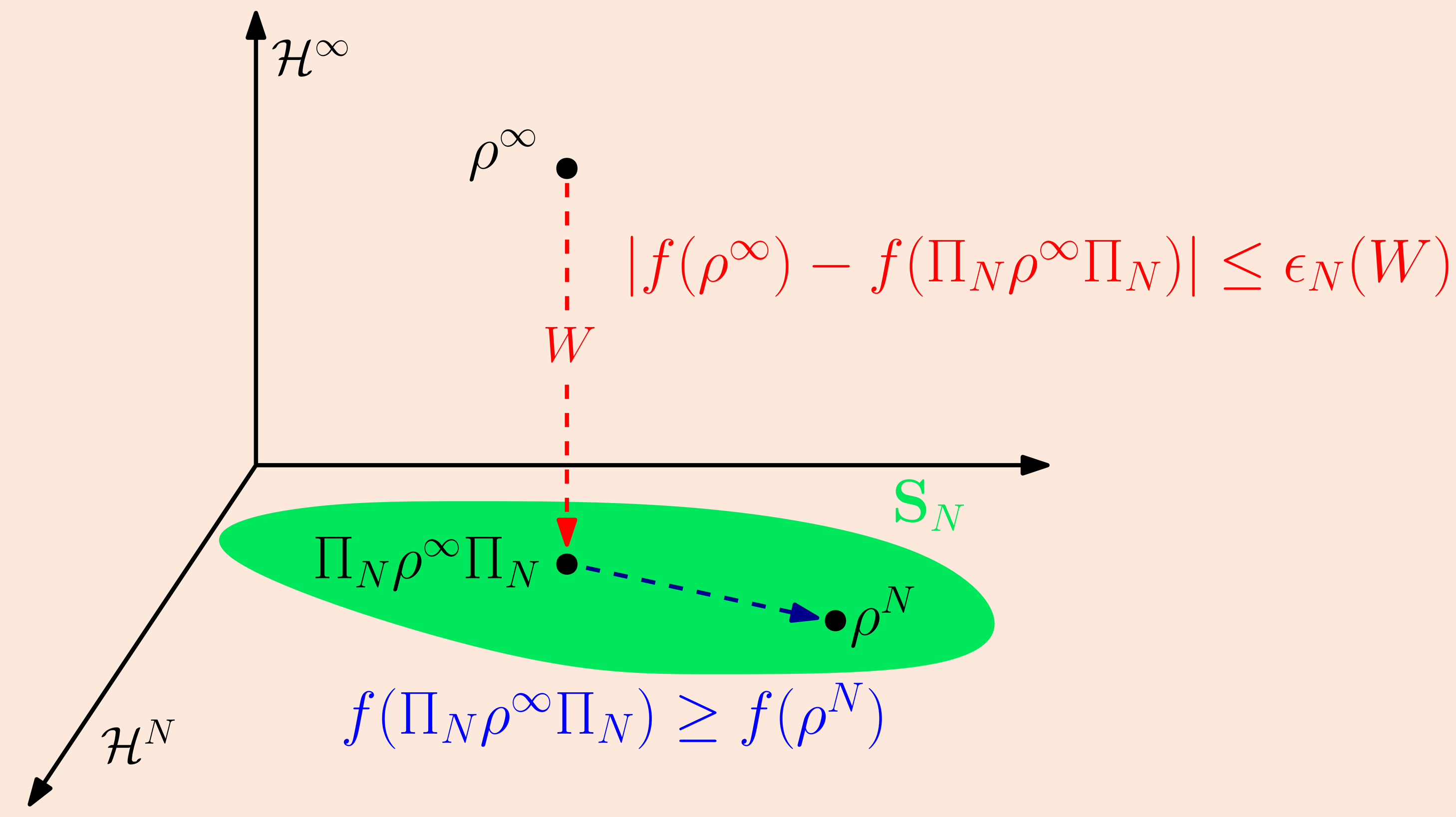
W can be determined from parameter estimation, and characterizes the weight outside the finite subspace.

Using a generalization of the result in [5], we have:

$$1 - W \leq F(P,Q) \implies |f(P) - f(Q)| \leq \epsilon_N(W)$$

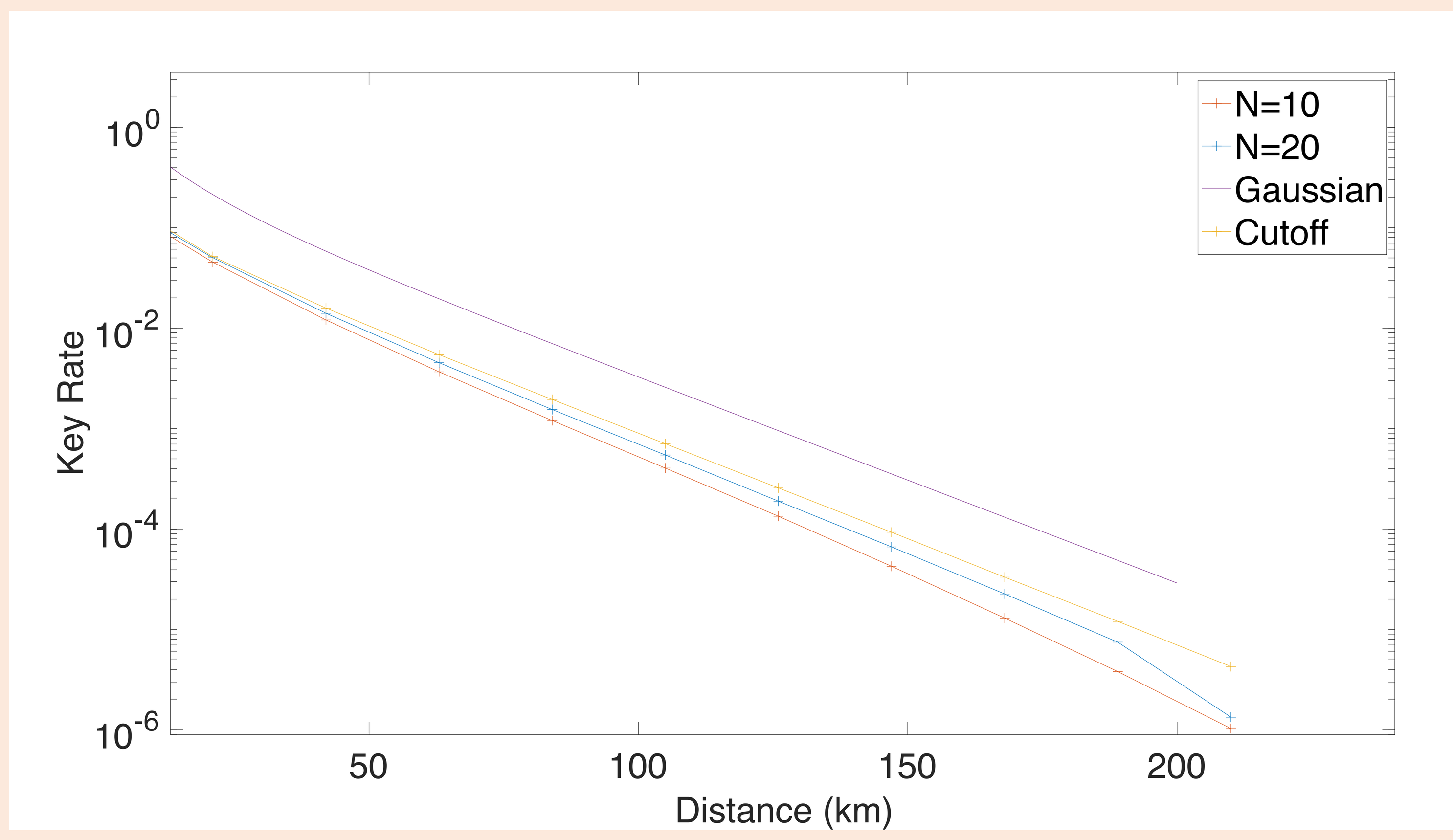
Main Theorem

$$f(\rho^N) - \epsilon_N(W) \leq f(\rho^\infty)$$



Results for Typical Simulation

Lossy and noisy channel, with ξ=0.01



Future Work

Extend to finite-size numerical framework for CVQKD.

Encapsulate different models of imperfect detectors, e.g. trusted noise.

References

[1] A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum **2**, 77 (2018).
[2] P. J. Coles, Phys. Rev. A **85**, 042103 (2012).
[3] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **9**, 041064 (2019).
[4] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[5] A. Winter. (2016) , Communications in Mathematical Physics, **347**(1):291–313.

The Institute for Quantum Computing is supported in part by Innovation, Science and Economic Development Canada. T.U. acknowledges the support of NSERC through the Alexander Graham Bell Canada Graduate Scholarship. This research has been supported by NSERC under the Discovery Grants Program, Grant No. 341495, and under the 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.

NSERC CRSNG