New Security Proof of a Restricted High-Dimensional QKD Protocol (arXiv:2307.09560)

Hasan Iqbal, Walter O. Krawec

Computer Science and Engineering, UConn

Introduction

- Modern cryptographic protocols have unproven computational assumptions while QKD offers unconditional security.
- High-dimensional QKD offers many practical advantages but analytical security proofs are not straight-forward in restricted scenarios.

The HD-3-State-BB84 protocol

In this work, we consider the following protocol which had a numerical security analysis before [1].

- Alice randomly chooses any of the $Z = \{|0\rangle, |1\rangle, ..., |D-1\rangle\}$ basis states to send to Bob in a key-round.
- In a test round, she sends only the first state of the Fourier basis, $|x_0\rangle$.
- Bob randomly chooses to measure in basis Z or POVM $|x_0\rangle\langle x_0|, \mathbb{I} - |x_0\rangle\langle x_0|$.
- The perform classical error correction and privacy amplification if the noise is acceptable.

Proof Sketch

- Calculate the density operators for a 'key-round' ρ_{AB^zE} and a 'test-round' σ_{AB^zE} after Bob's measurement .
- Use Berta's entropic uncertainty relation in σ_{B^zE} to find $H(B^Z|E)_\sigma \geq \log(D) - H(B^X)_\sigma$.
- Use Winter's continuity to find $|H(B^Z|E)_\sigma - H(B^Z|E)_\rho| \leq f(\epsilon)$, where $\epsilon \geq \frac{1}{2}||\rho_{B^zE} - \sigma_{B^zE}||$.

Proof Sketch (cont.)

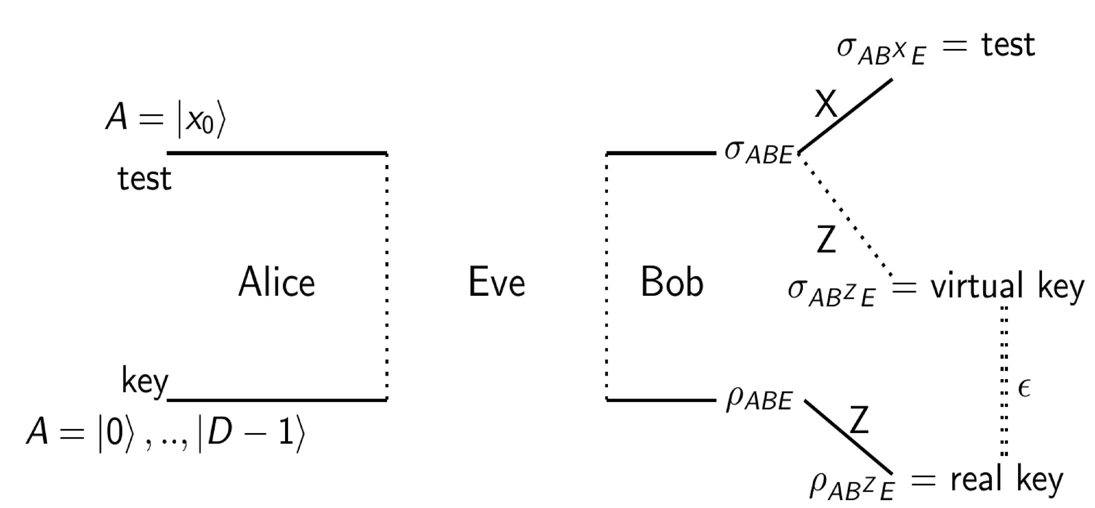

Figure: A schematic view of our proof method

Evaluation

We evaluate the following key rate:

$$K \geq \log(D) - \Delta - H(B^X)_\sigma - leak_{EC}$$

where $\Delta = |H(B^Z|E)_\rho - H(B^Z|E)_\sigma|$. We evaluate our analysis and compare it with [1].

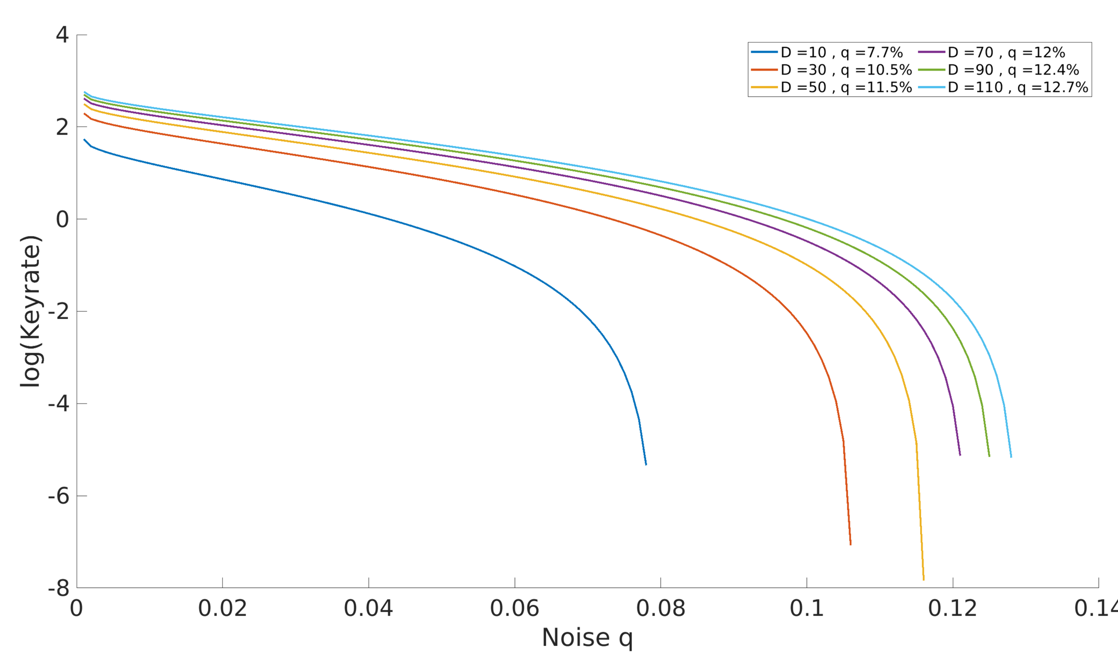

Figure: Noise Tolerance in high-dimensions

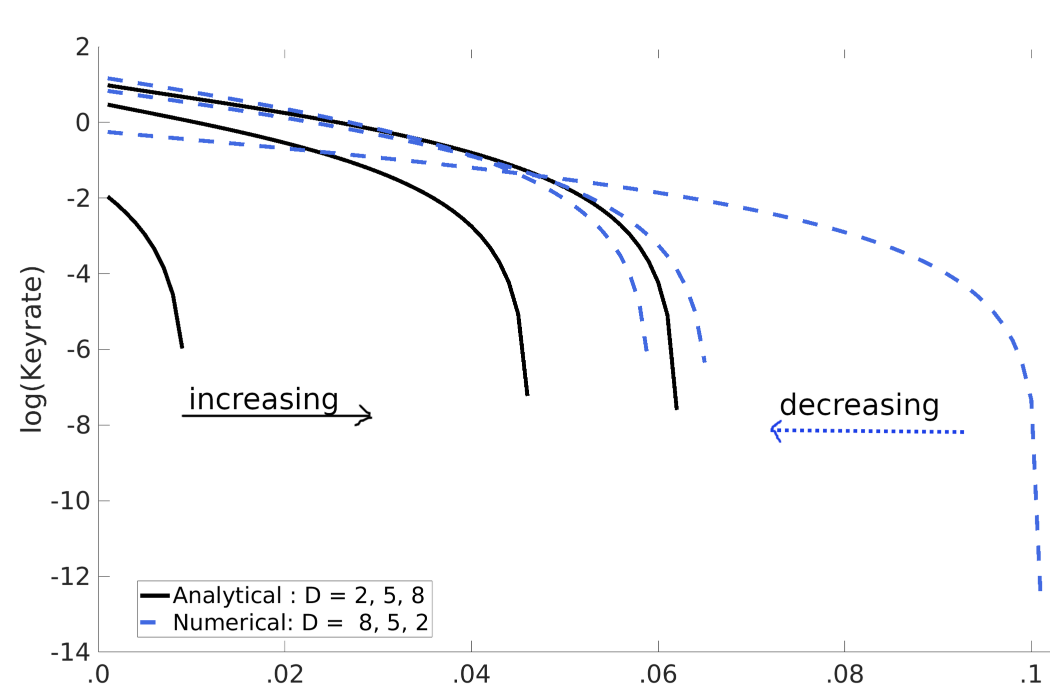

Figure: Noise vs Key rate for HD-3-State-BB84 Ours vs [1]

A New Lemma

For two cq-states ρ_{B^zE} and σ_{B^zE} where $\sigma_E = \rho_E + \Lambda_E$ where Λ_E is some small 'noise', the following holds for $D = 2$ in the depolarizing channel with parameter $0 \leq q \leq .1416$:

$$\begin{aligned}&\left|H(B^Z|E)_\rho - H(B^Z|E)_\sigma\right| \\ &\leq h(1 - q - \sqrt{q(1-q)}).\end{aligned}$$

Proof Sketch of This Lemma

- In a depolarizing channel, we know the eigenvalues of ρ_{B^zE}.
- Tracing out B^Z, we use Horn's theorem to generate a set of possible eigenvalues of ρ_E.
- Because $\sigma_E = \rho_E + \Lambda_E$ in our protocol, the eigenvalues of σ_E can not vary too much from the eigenvalues of ρ_E due to Weyl's eigenvalue stability inequality.

Comparison of Our Bound With Others

We compare our new bound for the cq-states in the protocol with Winter's bound and Wilde's conjecture and plot the conditional entropy difference.

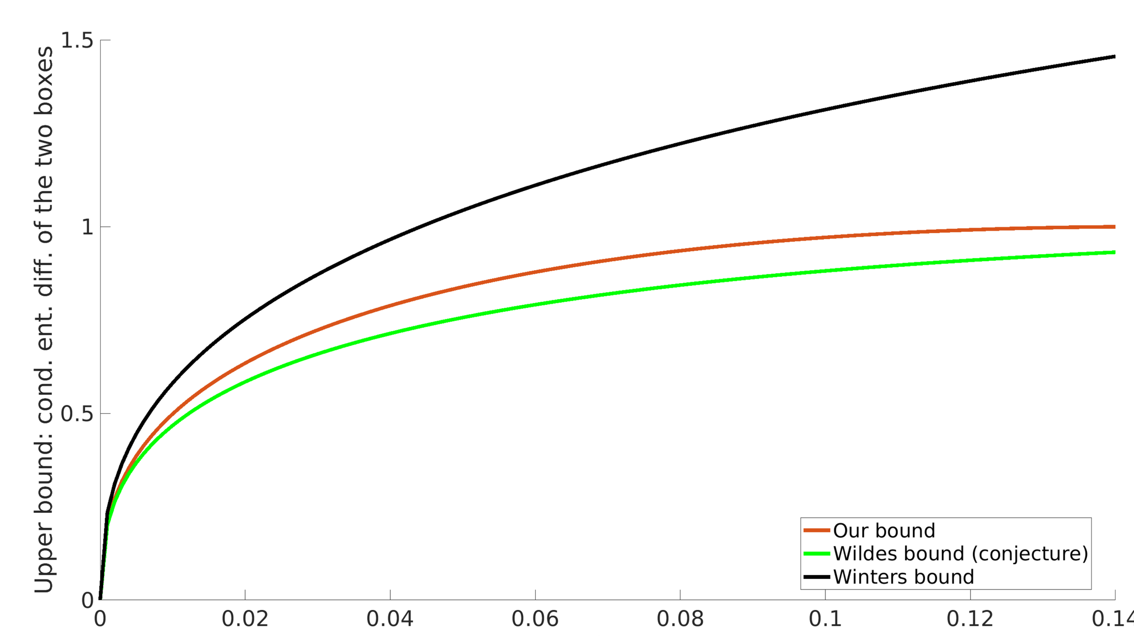

Figure: Continuity bound comparison in a limited scenario

Improved Key Rate With New Bound

We see that our bound slightly improves the key rate for $D = 2$ and $0 \leq q \leq .1464$ compared to Winter's bound.

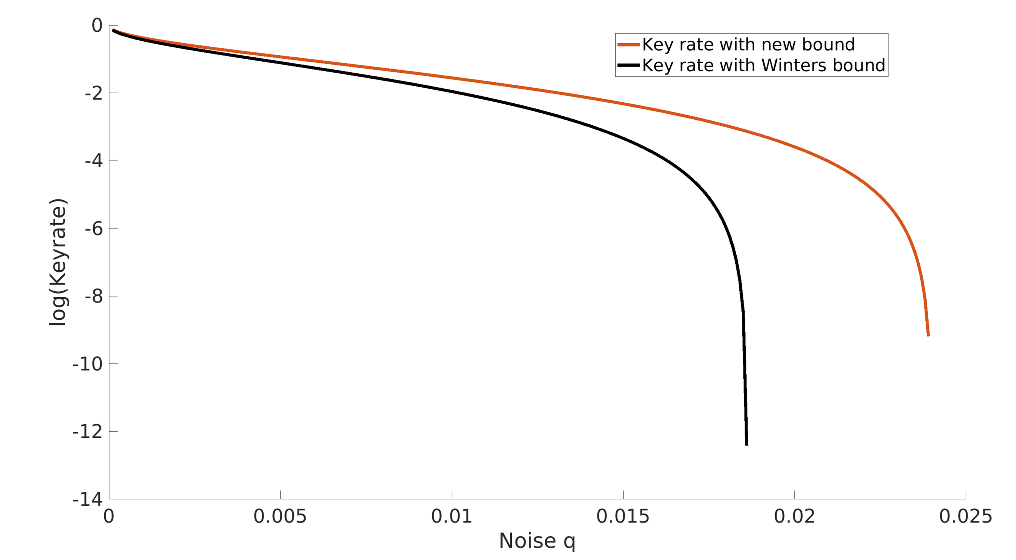

Figure: Comparison of key rates with our bound and Winter's bound

Conclusion

- We have proved the analytical security of the HD-3-State-BB84.
- Established the advantage of using HD-resources.
- Derive a new continuity bound for quantum entropies applicable in a limited scenario.

References

[1] Nurul T Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim, and Daniel J Gauthier. Securing quantum key distribution systems using fewer states. *Physical Review A*, 97(4):042347, 2018.

[2] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11, 2014.

[3] Hasan Iqbal and Walter O Krawec. High-dimensional semiquantum cryptography. *IEEE Transactions on Quantum Engineering*, 1:1–17, 2020.