High-dimensional Low-state Quantum Key Distribution

Hasan Iqbal, Walter O. Krawec

Computer Science and Engineering, UConn

Question

How can we keep our security infrastructure safe when quantum computing arrives?

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

What is Quantum Key Distribution

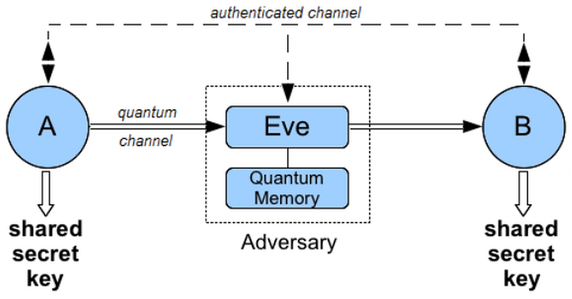

Figure: Quantum Key Distribution [1]

- Alice sends her friend Bob information via qubit through quantum channel.
- Adversary Eve can attack the channel in various ways.
- Alice and Bob communicates classically to produce a shared key.
- The key is secure as long as Eve does not know 'too much' about it compared to Bob.

The HD-Low-state Protocol

- 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 HD X basis.
- 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.

Important Result

HD-low-state protocol can be proven to be analytically secure. A new continuity bound derived here to improve the noise-tolerance of this protocol can be applied in other places also in a limited scenario.

Proof Method

- Calculate the density operator for a 'key-round' and a 'test-round' of the protocol.
- Use entropic uncertainty relation in the test round operator to find a lower bound on Eve's information based on Alice and Bob's entropy.
- Use a continuity bound for conditional quantum entropy to bound Eve's information in the key round from Eve's information in the test round.

Evaluation

We evaluate our analysis and compare with [2]. We also demonstrate the utility of our new continuity bound.

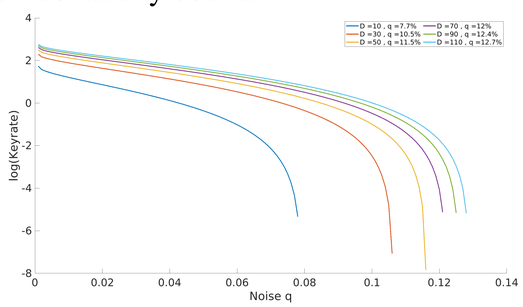

Figure: Noise Tolerance in high-dimensions

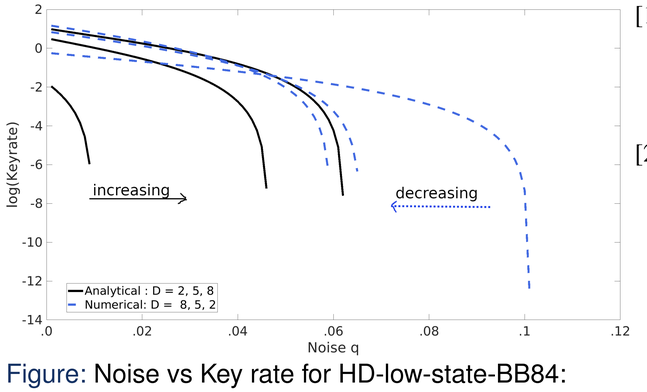

Figure: Noise vs Key rate for HD-low-state-BB84: Ours vs [2]

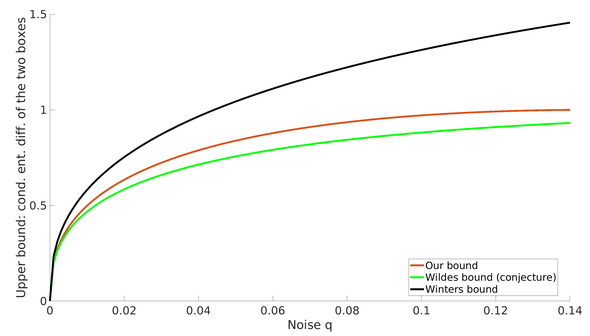

Figure: Continuity bound comparison in a limited scenario

Conclusion

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

References

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

[2] 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.