High-Dimensional Semi-Quantum Cryptography

Hasan Iqbal, Walter O. Krawec

Computer Science and Engineering, UConn

Objectives

Can we have unconditional security with limited Quantum resource?

- Restrict one parties capability.
- Bridge the gap between Classical and Quantum Realm
- Use less expensive Quantum hardwares
- Fallback option for fully fledged QKD

Motivation

- Perfect security is impossible with all-classical capabilities but possible with quantum resources.
- High-dimensional QKD offers better protection.
- Using HD-resources in SQKD provides advantages.

What is Quantum Key Distribution?

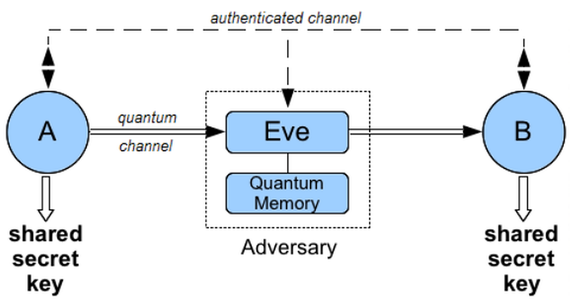

Figure: Quantum Key Distribution

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

What is High-Dimensional SQKD

- High-Dimensional qudits instead of traditional qubits.
- More information transmitted in each iteration.
- Robust against quantum cloning.
- Better noise resistance.

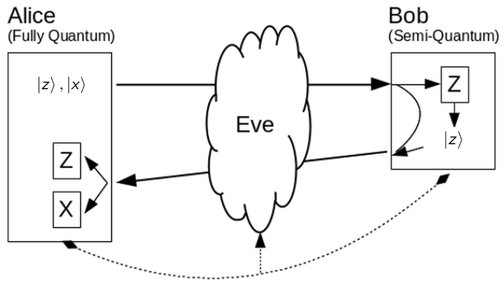

Figure: HD-SQKD

Important Result

High-dimensional SQKD offers the best key-rate so far. Proof technique developed here is applicable to other protocols.

Simplified Protocol

HD-SQKD	OW-SQKD
1. A prepares $\|z\rangle$ or $\|x\rangle$, sends to Bob	1. Bob prepares and sends two states depending on his choice of whether MR or Meas
2. Eve attacks the forward channel	2. Eve attacks only once
3. Bob measures/resends or reflects	3. Alice measures in two basis
4. Eve attacks the reverse channel	
5. Alice measures returning qubits.	

Reduction

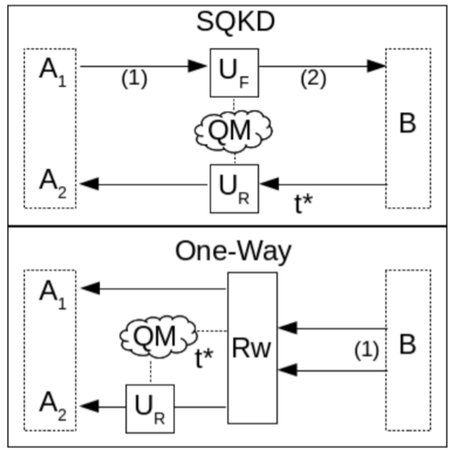

Figure: Figure caption

Evaluation

- Noise tolerance: How much disturbance in the channel can the protocol withstand.
- How does it compare to a famous fully quantum HD-QKD protocol.

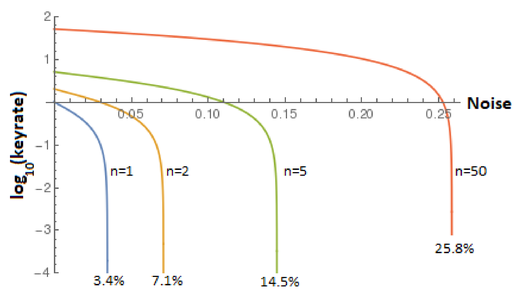

Figure: Noise Tolerance in different dimensions

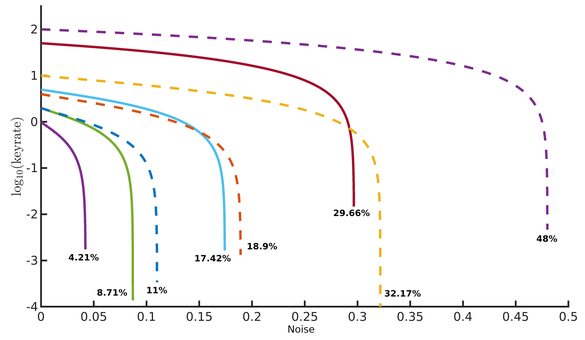

Figure: Noise vs Key rate: HD-SQKD vs HD-BB84

Conclusion

- We have proposed a new HD-SQKD protocol.
- Performed an information theoratic-security analysis.
- Showed how to reduce a two-way protocol to one way.
- Proved that Qudits can indeed benefit SQKD model.
- Applying this proof technique to other protocols would be quite interesting.

References

[1] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical bob. In *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, pages 10–10. IEEE, 2007.

[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 semi-quantum cryptography. *arXiv preprint arXiv:1907.11340*, 2019.

Contact Information

- Email: hasan.iqbal@uconn.edu
- Phone: +1 (312) 975 7006