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

Introduction

- Perfect security is impossible with all-classical capabilities.
- Surprisingly, it is possible with quantum resources.
- Develop high-dimensional semi-quantum protocol with better security.

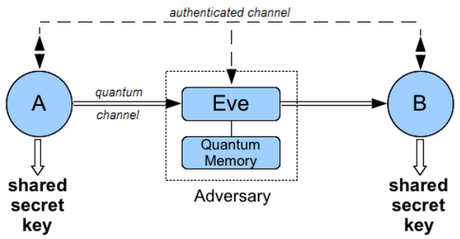


Figure: Quantum Key Distribution

Using qudits instead of qubits, modify The following figure shows a general depiction of high-dimensional semi-quantum QKD.

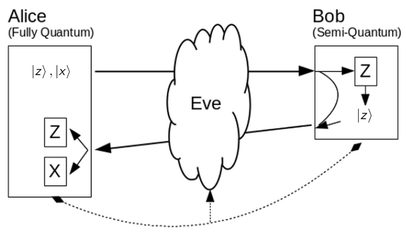
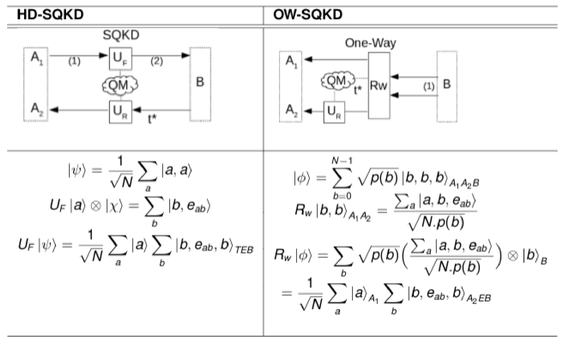


Figure: HD-SQKD

Materials

HD-QKD offers:

- More information transmitted in each iteration.
- Robust against quantum cloning.
- Better noise resistance.



Important Result

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

Mathematical Section

$$|z\rangle \in \{|0\rangle, |1\rangle, ..., |N-1\rangle\}, |x\rangle = \mathcal{F}|z\rangle$$

$$|\phi_R\rangle = \sum_{b=0}^{2^n-1}\sqrt{p(b)}\,|b,b\rangle_{A_1A_2}\otimes|0\rangle_B$$

$$|\phi_{MR}\rangle = \sum_{b=0}^{2^n-1}\sqrt{p(b)}\,|b,b,b\rangle_{A_1A_2B}$$

HD-SQKD	OW-SQKD
1. A prepares $\|z\rangle$ or $\|x\rangle$, sends to Bob	1. Bob prepares and sends $\|\phi_R\rangle$ or $\|\phi_{MR}\rangle$ if he wants to reflect or measure respectively
2. Eve attacks with U_F	2. Eve attacks with U
3. Bob measures or resends in $\mathcal{Z}$ basis	3. Alice measures A_1 and A_2 registers in $\mathcal{Z}$ or $\mathcal{X}$ basis
4. Eve attacks with U_R	
5. Alice measures the returning n qubits in the preparation basis	

Figure: Figure caption

Reduction

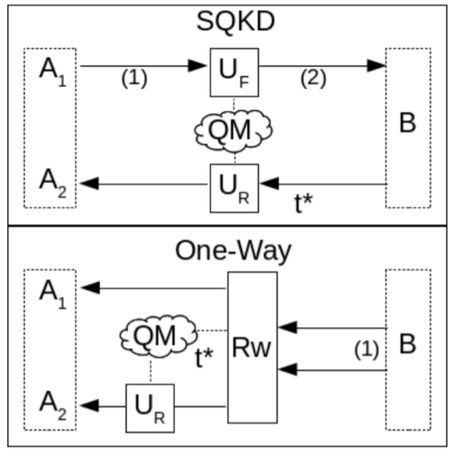


Figure: Figure caption

Evaluation

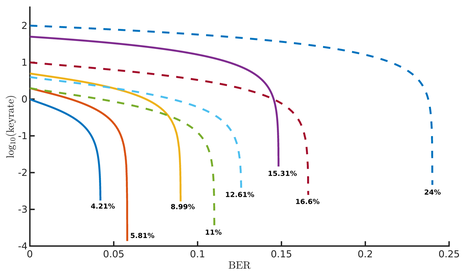
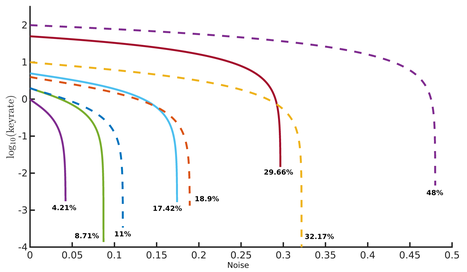


Figure: Figure caption



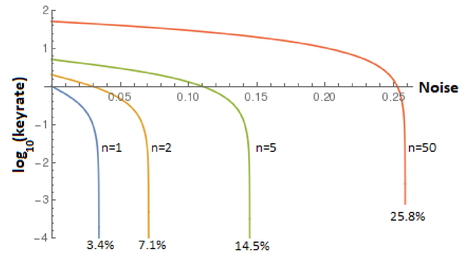


Figure: Figure caption

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.

Additional Information

Maecenas ultricies feugiat velit non mattis. Fusce tempus arcu id ligula varius dictum.

- Curabitur pellentesque dignissim
- Eu facilisis est tempus quis
- Duis porta consequat lorem

References

[1] J. M. Smith and A. B. Jones.
Book Title.
Publisher, 7th edition, 2012.

[2] A. B. Jones and J. M. Smith.
Article Title.
Journal title, 13(52):123–456, March 2013.

Contact Information

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