CS269Q Project Proposal

Yousef Hindy and Pieter-Jan Stas

May 2019

1 Proposed Topic

We hope to explore applications of quantum information to cryptography and communication. In particular, we hope to explore how we can use the principles we learned in the class of quantum programming to potentially implement an already existing scheme. It would be very interesting too to synthesize some of the results from recent papers and come up with our own scheme that has advantages over the independent ones already created. We also hope to explore the relationship between quantum error correction and secure quantum communication as outlined in [1].

2 Implementation Structure

We will begin our project by reading several papers outlined in the references section. There is a quite a bit of research already done on the security of quantum information and cryptography, so this will occupy a good chunk of the first part of our project.

Since we are still in the exploratory phase of our project, we will hopefully be able to reach out to some of the authors and get their advice. To start, we will likely implement a simple version of Cleve, Gottesman, and Lo's quantum secret [1] in PyQuil. Once we have this running, we will likely go back to the theoretical drawing board and come up with our own scheme.

3 Key Results & Deliverables

Our project will be successful if we are able to develop a system that provides secure communication over a quantum channel. We likely will face challenges as the number of qubits are limited and most of the results out there right now are theoretical and assume fault-tolerant quantum computers, so it will be interesting to see how noisy channels affect the ability of our method to communicate effectively. From this, we could include a discusion about the efficacy and practicality of our schemes on today's quantum computers. In addition, once we have code that is up and running, it would be awesome to create a Jupyter Notebook tutorial on how to use the system and the principles behind it.

References

[1] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, pp. 648–651, Jul 1999.

[2] D. Boneh and M. Zhandry, "Quantum-secure message authentication codes," in *Advances in Cryptology – EUROCRYPT 2013* (T. Johansson and P. Q. Nguyen, eds.), (Berlin, Heidelberg), pp. 592–608, Springer Berlin Heidelberg, 2013.

[3] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, p. 076001, Jul 2013.

[4] A. M. Childs, W. van Dam, S.-H. Hung, and I. E. Shparlinski, "Optimal quantum algorithm for polynomial interpolation," *arXiv e-prints*, p. arXiv:1509.09271, Sep 2015.

[5] K. Senthoor and P. Kiran Sarvepalli, "Communication Efficient Quantum Secret Sharing," *arXiv e-prints*, p. arXiv:1801.09500, Jan 2018.