Project Proposal

Matthew Langlois - 7731813

Jan 30

Quantum Cryptography

As a 4th year computer science student with a keen interest in security I hope to base my project around quantum cryptography. This past semester I took Cryptography (CSI4108) and really enjoyed learning about the math behind modern day cryptography algorithms. However as we slowly navigate our way into the world of quantum computing all of our security algorithms are going to need to be adjusted to reflect the new possibilities of quantum.

In this research paper I plan to explore the basics of quantum computing to provide a basis for quantum cryptography. I will analyze current cryptographic implementations and their weaknesses in a quantum world. After understanding why modern algorithms fail to secure information in a quantum world I will explore options for securing data in a quantum world. This paper will hopefully demonstrate the need for preparing cryptographically secure algorithms when entering a quantum world.