Project Specification

Team Member

Stacie Reynolds

Project Title

Quantum Computing and the Future of Public Key Cryptography

Introduction and Motivation

Public key cryptography is one of the most widely used methods for key distribution and digital signature generation/verification. Many industries across the world use this method to securely transmit sensitive data (e.g., financial information classified government documents, etc.) across the internet. Public key cryptography has been considered to be unbreakable because its security depends on the difficulty of factoring large integers and solving so called discrete logarithm problem. Currently, even the most powerful computers would take hundreds of years to break existing public key schemes, such as RSA or Diffie-Hellman. Quantum computing makes large integer factorization and the discrete logarithm problem computationally easy, allowing access to private keys without authorization. This poses a powerful threat to the ever popular public key cryptography systems being used to securely transmit sensitive data across the internet.

Alternative solutions to explore

- Shor's Algorithm
    - Factorization
    - The discrete logarithm problem
    - Elliptic curve discrete logarithm problem
- Grover's algorithm
- Post Quantum Cryptography
    - Coding based cryptography
    - Lattice based cryptography
    - Multivariate cryptography

Problems to be investigated

- The threat of quantum cryptography being used against current public key cryptography
- Breakthroughs in quantum computing to determine how soon an attack against the current public key cryptography system may become effective.
- Using post quantum cryptography to protect against quantum computing attacks

Hypothesis

A viable solution to protect sensitive data from attacks against the current public key cryptosystem will be one that operates successfully in both quantum and classical computers. In theory, a quantum computer can compute anything that can be computed by a classical computer. Therefore, it is necessary to find a solution that can operate on a classical computer environment. Post quantum cryptography will provide a solution to protect classical computers from attacks against the current

public key cryptosystem. Even though it may be decades before quantum computers are available to the average consumer, post quantum cryptography mechanisms will be compatible with both classical and quantum computers making cross communication between the two systems seamless to the user.

Tentative questions to be answered

- What are the strengths and weaknesses of post-quantum public key cryptosystems?
- Can quantum computing also be used to defeat hashing algorithms?
- How soon will quantum computers be available for general consumer
- If post quantum cryptography schemes must replace current public key cryptography schemes, what impact does this change have on current encrypted data? Will it be backward compatible, or will a mass re-encryption of all data be required?
- What are the strengths and weaknesses of Shor's algorithm?
- What are the strengths and weaknesses of Grover's algorithm?

Time schedule

Date	Goal
September 25	• Complete project specification
October 4	• Research history of quantum computing complete. • Complete draft of history section of paper
October 11	• Research quantum computing today • Demonstrate understanding of quantum computing and Shor's Algorithm
PROGRESS REPORT COMPLETE	
October 18	• Analyze threat posed to current public key cryptography
October 25	• Research Post Quantum Cryptography and other methods used to protect against quantum computing attacks against public key cryptography
November 1	• Continue research and correlate all findings. • Demonstrate understanding of post quantum cryptography • Analyze effectiveness of post quantum cryptography against attacks based on quantum computers. • Analyze additional protection methods found during research
PROGRESS REPORT COMPLETE	
November 8	• Continue analysis of findings. • Determine if quantum computing has an impact on popular hashing algorithms
November 15	• Document brief description for current public key cryptography and its weaknesses against quantum computing, and the possible global effect if a solution is not found.
PROGRESS REPORT COMPLETE (Presentation Final Draft Complete)	
November 22	• Finalize and practice presentation
November 29	• Focus efforts to written report based on research and analysis
December 6	• COMPLETE WRITTEN REPORT

Tentative table of contents of your final report

Tentative List of literature

[1] A. Pathak, *Elements of Quantum Comptation and Quantum Communication*

[2] A. Ferrer. (2012, Sept 25.). Why Cybersecurity is So Important in Government IT Infographic. *Fed Tech*. [Online]. *21(3),* Available: http://www.fedtechmagazine.com/article/2012/09/why-cybersecurity-so-important-government-it-infographic

[3] Wikipedia. (2012 Jun 25). Multivariate Cryptography [Online]. Available http://en.wikipedia.org/wiki/Multivariate_cryptography

[4] Wikipedia. (2013 Mar 14). Hidden Field Equations [Online]. Available http://en.wikipedia.org/wiki/Hidden_Field_Equations

[5] Wikipedia (2013 May 30). Lattice-based cryptography [Online]. Available http://en.wikipedia.org/wiki/Lattice-based_cryptography

[6] D. Engelbert, R.Overback. A. Schmidt, "A Summary of McEliece-Type Cryptosystems and their Security," Dept of Computer Science Cryptography and Computer Algebra Group., Univ. Hessen, Deutschland, May 10, 2006.

[7] C. Bouillaguet. “Supposedly Hard Problems In Multivariate Cryptography,” Versailles Saint-Quentin Univ. Versailles, France, January 20, 2012.
[8] D. Micciancio. “The Geometry of Lattice Cryptography,” February 16, 2012
[9] D. Micciancio, O Regev. “Lattice-based Cryptography,” July 22, 2008