Quantum Computing and Information Security

Timothy Vincent
Villanova University
800 Lancaster Ave. Villanova, PA
United States of America
timothy.vincent@villanova.edu

ABSTRACT
Quantum computing, if realized on a large and commercial scale, will provide significantly more powerful computers that could threaten global information security. Modern methods for encrypting data could become obsolete as quantum computing methods break methods used now by more traditional computing techniques. Commercial machines that make use of quantum algorithms to reduce problem sizes of cracking encryptions, if current development trends in quantum computing continue, could be completed sooner rather than later. Such super-fast computing machines would threaten data and network security, resulting in a threat to the global economy. To ease the transition to this more powerful form of computing, such as quantum safe encryption, researchers need to focus on methods for preventing data insecurity. This paper looks at methods of securing data transmission and possible security flaws that could be easily exploited by a proposed quantum computer.

KEY WORDS
Quantum Computing, Qubit, Cryptography, Quantum Key Distribution

2. BACKGROUND
2.1 Basics of Quantum Computing
Quantum Computing is based on principles of quantum mechanics. Specifically, quantum computers take advantage of superposition and entanglement. Quantum computers operate on qubits rather than classical bits. Like traditional bits, qubits can hold the values 0 and 1, but they can also be the superposition of both values. Entanglement is the property of quantum particles such that their states are always linked. The measurement of the spin of one of the particles will reveal the spin of the other particle, no matter the amount of space between the two particles.[13]

Famed Nobel Laureate Physicist Dr. Richard Feynman first suspected that quantum computation could exceed classical computation on certain tasks when he discovered the “exponential complexity of classically simulating quantum systems.”[12] He first introduced a model of quantum computation, which David Deutsch later formalized. Deutsch’s model defined both quantum Turing Machines and quantum circuits. The quantum computing model Deutsch formalized is much like the probabilistic Turing Machine because it uses the laws of probability that bind particles according to quantum mechanical processes, however it has been shown to be more powerful than a probabilistic TM.[1]

Daniel Simon's paper presents early evidence for the computational power of quantum computing models. There is a class of problems called bounded quantum polynomial that can be solved in polynomial time on a quantum computing paradigm. There is some evidence that many NP problems can be reduced to BQP problems, and there is a possibility that BQP is in NP. However, current evidence seems to show that BQP is not within NP, though the area is still being researched.[1]
2.2 Security Threat

As Arjen Lenstra describes in his paper, factoring large positive integers is an integral part of cracking public-key encryption. In theoretical mathematics, an algorithm that computes the prime factors of a given integer is a computationally very difficult.[2] The infeasability of factoring large integers using classical computing models is the main reason public-key encryption is so secure even on modern hardware.[3] Quantum Computers able to crack encryption so quickly will put sensitive personal, financial, and governmental information exposed, which would put privacy, billions of dollars, and human lives at risk.

2.3 Quantum Cryptography

With the advent of Quantum Computing, two important areas of study in algorithms (factoring and discrete logarithms) will no longer be useful, since cryptography will not need them any longer.[3] Quantum cryptography promises not only to protect against quantum methods of breaking classical encryption, but also to create more wholly secure methods that can detect eavesdropping.[4] Since keeping data stored in a quantum state is difficult at best, researchers of quantum computing seek instead to use quantum principals purely on the transfer of data. To do this, new methods of cryptography need to be developed using a quantum method of key distribution.

2.4 Quantum Security

Quantum Key Distribution is one of the methods of distributing keys between parties to communicate data encrypted that foils quantum attacks that would work on purely classical key distribution methods. If two parties are to communicate using quantum-key distribution, there generally needs to be two channels connecting them, a quantum channel for quantum signals and a classical channel to pass classical messages back and forth.[5] Charles Bennett in 1992 developed the first method of quantum key distribution.[4] Bennett's method used reference pulses so that any eavesdropper would be recognized. Bennett's plan, in practice, however is flawed, because the necessary magnitude of a pulse to carry over a large enough distance would distort any data being sent along with it. Marco Lucamarini and the other authors of "Robust Unconditionally Secure Quantum Key Distribution with Two Nonorthogonal and Uninformative States"[4] describe an improved method of Bennett's protocol. Their method includes creating new uninformative states (or channels) to accompany the two conventional signal states.[4] The method of eavesdropping that Bennett's method is supposed to protect against is called intercept resend. The eavesdropper essentially intercepts the photon from the sender, reads it, and then resends it to the original recipient.[5]

4. Proposed work

I propose to further develop current Quantum Key Distribution methods into more secure and viable methods which protect against eavesdroppers. I propose to log the many ways an eavesdropper can gain full information on a sent key without corrupting the signal, and to eliminate any of those possibilities. I aim to do this by developing the means of communication between two parties and the means of detecting third party eavesdroppers, by adding onto current theoretical protocols, new steps to ensure as near complete security as possible.

As the field of Quantum Computing grows, and the appearance of commercially available quantum computers nears, fervent work needs to be done to ensure information safety. Without adequate protection against quantum attacks, there will be no such thing as secure information or privacy. The entire business of banking could potentially fall over the course of a very short time.

Charles Bennett helped develop the first complete protocol for Quantum Key Distribution in 1984. Since then, significant advances in both experimental and theoretical Quantum Key
Distribution have been made. [10]. Lucamarini [4] and Valerio Scarani [5] have each developed new, updated protocols which have adapted to newer quantum computing technologies. These protocols are seen as secure, but new security threats in secure systems are always found.

In order to carry out my research I will need access to prototype quantum computers connected on a fiber-optic network. I will need full protocols for Quantum Key Distribution so I can test the security and feasibility of each. The research will take place over the course of 2 months. During first month I will determine the most secure methods of Quantum Key Distribution. Then in the next month, I will update the remaining protocols with any experimentally implemented improvements I discover.

My participation in research for an open source semantic web project and as well as my knowledge of analysis of algorithms and theory of computation will help me with this project. I have experience working on my own and with others on research projects, so I will be able to evaluate and improve current Quantum Key Distribution protocols over a two month time span.

3. Conclusion

Use of quantum computers today is limited by technology. Today’s quantum computers serve little practical use and are unwieldy so we cannot yet construct a useful or general purpose quantum computer. However, just as technology develops, Computer Scientists need to evolve to be able to work with quantum algorithms which will uphold information security. There needs to be as little gap as possible between the release of commercially viable quantum computers and the encryption methods needed to keep information safe.

REFERENCES