The Effects of Quantum Computers on Cryptography

Matthew Guidry
guidry@cs.fsu.edu

Abstract –

One of the fundamentals of cryptography is that keys or secret numbers are selected and used which are computationally infeasible for an attacker to compute the same key given the public information. Consider one of the most commonly used assumptions for cryptography, the RSA assumption, which states given a large number $n = p*q$ *such that* p *and* q *are primes,* e *such that* $GCD(e, \Phi(n)) = 1$*, and ciphertext* C*, it is computationally infeasible to compute the original message* M *such that* $C = M^e \bmod N$*. There are many other assumptions made by cryptographic protocols which rely on the computational infeasibility of an attacker having the ability to produce secret keys of different sorts. However, if there was a way to drastically increase the computational power of a machine these assumptions would not necessarily hold true. Many people optimistically speculate that one way to achieve this increase in computing power is by looking into quantum computing. What effects will this have on cryptography? Will we be able to enhance the current strategies of cryptographic methods or will new strategies have to be created? These are questions which, rightfully so, are already being asked as we verge on the barrier of the quantum computing capabilities.*

The second section of this paper describes an introduction to quantum computers, the third and forth sections discuss the new qubits and the different states of qubits, the six and seventh sections evaluate the possible consequences of quantum computing on cryptography and possible solutions or techniques against these consequences, and the paper is concluded in section eight.

II. The Basics of a Quantum Computer

A simple explanation of the current architecture of a computer is a machine which manipulates electronic signals measured to equal a 1 or a 0. These signals are then used to signify different meanings depending on which protocol is being used. Computers have become more and more powerful following Moore's Law, which states that every 18 months the number of transistors which can be fit within one square inch doubles. If this trend continues unabated, by 2015 transistors will roughly be the size of single atoms and molecules. [1] At this size the laws of physics which governed classic computers give way to the laws of quantum mechanics.

Looking forward to these advancements, some scientists have begun to examine the possibilities given this size of a transistor. For instance, the 1 and 0 of the classic electronic signal could be represented by atoms in the excited or grounded state.

However, given the multiple properties of quantum mechanics it would allow for other states to be inferred at the same time. With some study on how to achieve these new goals for computing, scientists believe we may see a quantum computer in as little as 50 years that would be capable of performing some tasks impossibly quickly by current standards. [2]

III. Qubits

The signals which are to be sent within a quantum computer are referred to as qubits. The term qubit was coined as the combination of "quantum" and "bit". These qubits are the foundation for the *magic* of quantum computers. A qubit can exist not just in one state or another such as previous bits, but it can exist in a *superposition* of different states. However, the examination of a qubit which is in a superposition forces a collapse of the wave function thus putting the qubit back into a single state as a result of the measurement. The state the qubit falls back into depends on the amplitude of the states from the superposition state. [3]

Classical bits and quantum bits share the same property that once measured they will only reveal one of two possible outcomes. However, the difference is not in the possible *answers* inferred from the bits, it is in the possible number *questions* that can be asked of them. [2] To simplify this definition think about the significance of a normal bit, a 1 or a 0 which signify two different states or answers to a question. A qubit has the capacity to hold many different states and may give different results depending on which *question* is being asked.

IV. The States of Superposition and Quantum Entanglement

The state of a qubit alone can be thought of as a unit vector in a two-dimensional vector space with basis **{ |0>, |1> }**. Here **|0>** and **|1>** are orthogonal vectors representing quantum states such as spin up and spin down or vertical and horizontal polarization. A qubit can be in state **|0>** or in state **|1>**, but it can also be in a superposition $\mathbf{x}|0\rangle + \mathbf{y}|1\rangle$ of the two states. The complex amplitudes **x** and **y** determine which state we will see if we make a measurement. When an observer measures a qubit in this superposition, the probability that the observer will see state **|0>** is $|\mathbf{x}|^2$ and the probability of seeing **|1>** is $|\mathbf{y}|^2$. Note that because $\mathbf{x}|0\rangle + \mathbf{y}|1\rangle$ is a unit vector, the sum $|\mathbf{x}|^2 + |\mathbf{y}|^2$ must be equal to **1**. [3]

Another quantum mechanical property of interest for these qubits is referred to as *quantum entanglement*. This property engages the fact that two qubits that are passed along together in a system will have an effect on each other's respective states. Given the consequences of this interesting property, machines which intend to benefit from quantum computing would have to be sure to account for it. The state of this system cannot be represented in terms of a simple Cartesian product of individual spaces, but it must be represented as a Tensor product. Without going into too much detail of the mathematical intricacies of a Tensor product, it is important to just consider one attribute of the system; that the number of dimensions in the combined space is the product rather than the sum of the numbers of dimensions in each of the component spaces. [3] Meaning that the more qubits which are used within a system, the more states that system could have and the number of states possible would grow exponentially.

It is through these two quantum properties of entanglement and superposition that quantum computers offer the potentially exponential speedup over today's classical computers. The fact that trough entanglement we can achieve a Tensor product rather than a Cartesian product would allow for a system of multiple qubits to have the state space which grows exponentially with the number of qubits in the system. Further, "because a qubit or a system of qubits can be in a superposition of states, an operator applied to such a system can operate on all the states simultaneously." [3] This would promise for the potential exponentially faster computations than those seen in current computers.

V. Attempts to use quantum computers for gains in Cryptography

As mentioned earlier, most of the concepts for cryptography are based on the difficulty of a single mathematical problem, finding the prime factors of an integer. For instance consider 108 which is equal to $2^2 * 3^3$. It may be possible for one to calculate this without a calculator, however finding factors is such a time-consuming task for one hundred digit numbers that it is considered to be impractical. Modern applications of this principle sometimes use numbers of up to 310 digits long, which is believed to require at least a billion years to compute. [1] Thus one can feel secure that a large number with these factors is secure and the number could just be publically released. However, with quantum computers it is estimated (even shown) that one could formulate a function that could be checked for every possible input at once. Using a machine of this caliber would make almost all of the assumptions that modern cryptography rests upon false and obsolete.

Consider for instance, Shor's factoring algorithm, Peter Shor created an algorithm to factor n-digit numbers in bounded-probability polynomial time on a quantum computer and another algorithm to compute discreet logarithms quickly. [6] Although these mathematicians may not have access to a physical quantum computer, many are working away at determining feasible possibilities that could be achieved given that kind of computing power. An original highly mathematical explanation of this algorithm given by Shor is detailed in [5] or a less technical explanation can be found in [6]. It is important to realize the disastrous results Shor's algorithm would have if it were implemented on a quantum computer. As stated earlier RSA is founded on the basic principle that one cannot find the factors of a large enough number in a reasonable amount of time. If one could achieve these computational powers they could do just that. Shor's result prompted a widespread interest in quantum computing.

VI. Possible Defenses, Where will cryptography go?

It is important to note that the full potential of quantum computers is not known. An actual machine that possesses all of the wonderful attributes and capabilities is not known, at least not publically. So most of the possible methods that could be implemented with these fantastic machines will remain just that, "possible". It is also important to consider the nature of these algorithms, "since the result will be a superposition of the possible outputs, a measurement of the result will not necessarily reveal the desired answer." [3] The issue is that a function will result in any one of the many possible outputs and the difference between a good function and a poorly designed function in this sense is the

probability it has in resulting in the correct answer. This is the key to the design of the quantum algorithms that would run on these computers. It is probable that most of the cryptographic functions used for security would have to be strengthened, at the very least, and others may have to be completely abandoned if these computers are realized. However, with these new computing powers at their disposal, it is also possible that cryptographers will develop new methods as the older ones are being broken.

VII. Current State of Quantum Computers

As explained, the theories are all in place for quantum computers to jump into action but how much progress has been made on actually building a quantum computer? One hurdle that must be overcome before quantum computers could be manufactured is how to manipulate and control these single atoms. The effective method to change the state of the atom as discussed is to change them into ions (charged atoms) and develop techniques to move and retrieve them to their destination. The manipulation of the atoms would be done using an ion trap, scientists have thus far been able to trap a single atom; however, the biggest challenge lies in being able to orchestrate the millions of atoms needed to run a quantum computer.[4]

Another problem faced by the concept of a quantum computer is defined as decoherence, or the interaction of the quantum system with the environment around it. [3] Behaviors or waves occurring in the environment around a quantum system could affect the qubits traveling within it, which would disturb their quantum state and cause errors in the calculation. Scientists have endeavored for a viable solution to this problem and have had some success in combating the effects of decoherence, but there is still a long way to go. Current systems have been able to run with just a handful of quantum bits, but future systems with many more qubits and the complex sequences to operate on those bits are widely expected. [1]

VIII. Conclusion

Quantum computers have become some-what of a buzzword or a dream for those thinking of the next-best-thing in the computing industry. Many foresee them as being the dominating computers that could help to solve even the toughest of the mathematical problems that currently face us. Others see the coming of these computers with anxiety for our current cryptographic methods. Which cryptographic protocols will stand the test of these quantum computers and which protocols will have to be completely abandoned for newer unforeseen protocols is yet to be known, given these computers do pan out. However, one thing to consider is the fact that with the possibility of this new impossibly fast computing power, other previously-unattainable encryption methods could be created which would be able to more easily combat the power of these computers.

References:

[1] Quantum Information: Joining the Foundations of Physics and Computer Science

[2] Internet Article: http://arstechnica.com/science/guides/2010/01/a-tale-of-two-qubits-how-quantum-computers-work.ars . by Joseph B. Altepeter, 2010

[3] Marco A. Barreno. "The Future of Cryptography Under Quantum Computers". Dartmouth College Computer Science Technical Report. 2002

[4] Ion trap in a Semiconductor Chip, D. Stick, W. K. Hensinger, S. Olmschenk, M. J. Madsen, K. Schwab and C. Monroe, *Nature Physics* advance online publication, 2005

[5] Peter W. Shor. "Algorithms for quantum computation: Discrete logarithms and factoring". In Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, pages 124-134. IEEE Computer Society Press, 1994.

[6] Eleanor Rie_el and Wolfgang Polak. "An Introduction to Quantum Computing for Non-Physicists". arXiv:quant-ph/9809016, 1998.