Quantum Computing and Quantum Computers

Quantum computing, as intimidating as it sounds, has a very basic idea that was realized around 30 years ago; it is the use of quantum computers to help study the idea and applications of theoretical computation systems. Using these theoretical computation systems, the focus is to use the thoughts and processes of quantum computing and quantum mechanical phenomena to be manipulated on different data and information. To be honest I have never even heard of quantum computing until having to write this paper so this will be a great experience and research topic.

Let us start with the basics of quantum computing: a quantum computer. What exactly is a quantum computer? Well, we all understand that in a traditional computer, encoding and bit strings are evaluated to either a 0 or 1 and creates a bit string that represents something based on that sequence, but a quantum computer uses a sequence made up of *qubits*. Qubits are similiar to binary bits, the difference being that not only can it represent a 0 or 1, it can also represent any *quantum superposition* based on a single bit: 2^b, where b is the number of qubits. So for 1 qubits, it can represent 2 qubit states; for 2 qubits, it can represent 4; for 3 qubits, it can represent 8 and so. What exactly does a qubit mean though? Unlike traditional bits where it can show 2 states, either 0 or 1, a qubit allows the system to be in *quantum superposition* of both states simultaneously which is a core mechanic of quantum computing. Another differene between a traditional bit and a qubit is the idea of *quantum entanglement*. This unique feature is a property that allows the qubit to represent a higher correlation than a traditional bit. This allows the qubit access to multiple states and can be manipulated simultaneously whereas the traditional can only access one state at a win (0 or 1). This functionality is necessary for any quantum computation or quantum system that requires a higher computing power, so using a traditional computer does not work. So if a regular computer doesn't work, what do we use for quantum computing...?

Yes, that's right, *quantum computers*. At first, when I research about quantum computers, I was intimidated just by the name. The idea for a quantum computer sprouted with the idea and need for a higher computing power and capacity. From what I've read, an actual quantum computer of the theoried computing power is still many years away, but scientists have built basic quantum computers that can perform at a higher level, but none close to what the goal of a real quantum computer is. From Moore's Law, the number of transistors on a microprocessor doubles nearly every year almost, so by the time a decade passes, the processors we will be using will be on a very small scale, atomic scale most likely. Once scientists have reached that threshold, the power of quantum computing can be realized due to the massive amount of computing power and potential that can fit on a microprocessor. This progression will take the idea and power of atoms and molecules on a quantum scale and perform memory and processing tasks at unbelieveable speeds.

It all started with Alan Turing with his invention of the Turing machine; we learned about the Turing machine in previous theory classes. It is basically an infinite tape that feeds in values and applies a read-write type mechanic which produces instructions to perform in a specific sequence in a system. As explained earlier, traditional bits can house either a 0 or 1 state, where as qubits can implement states. Now, you can see that the Turing machine can also use qubits instead of traditional binary bits; each block on a Turing machine trip can either be 0 or 1 or can be a superposition of them to represent a quantum state. As confusing as it sounds, it just means that each block can be both a 0 and 1 and anywhere inbetween at the same time! Because of this special mechanic of using qubits, compared to a traditional Turing machine which can only feed in one action at a time and then perform one calculation, the quantum Turing machine can feed in multiple actions and perform any number of calculations simultaneously. The power of this is actually

on a very large scale; a mindblowing scale to be honest. Since quantum computers aren't limited to only 2 states, they can represent a large scale of computations. The qubits fed into the Turing machine represent molecules and atoms which work in junction with each other to function as a a CPU memory and processor. Since the qubits can represent multiple states at once, the theorized potential of a quantum computer can be over a million times more powerful than any computer in today's age - even supercomputers. Imagine that for a second and think of the possibilities that it can produce.

The mechanic of superposition with qubits is what makes this possible. You can have unlimited states across the board at each slot in a Turing machine. This characteristic leads to another unique quality of the quantum computer: it implements parallelism. This simple idea allows a quantum computer to be able to work millions of computations at the same time!! Compared to the computer I am using to write this which can only perform **one** at a time. In one of the article I read on the history and progress of quantum computers, a quantum computer with the implementation of 30 qubits can run trillions of floating-point opterations per second which is equal to 10 teraflops of data being processed.

I went into quantum entanglement very little earlier, but I will now explain it in more detail since it is also a very important part of quantum computers and quantum computing. To put it simply, quantum entanglement is the correlation between different parts of a system. Imagine it as all the qubits and parts *entangled* into one entity. So in theory in a normal state, if you take one piece of information and digest it, you learn about it and then you take another piece of information and digest it, you learn another part of it. But with quantum entanglement, if you do that, you will learn nothing. Why is this? It's because the information is "entangled." Meaning that if you want to learn something from the data, you must digest all of it at once and not piece by piece; the information is in the correlations between the pieces of data and you must read it all at once as a whole. Another important aspect of entanglement is that one system can read the data as a whole and another system can read the data as well, but unless they both do it at the same time, the data cannot be correlated between the 2 machines. Being entangled with a specific identity also reduces how entangled that identity can be entangled with another system (identity). The ability to be entangled, as I read, has diminishing returns. If you didn't already get the implied notion, entanglement does not require the two entities to be physically near each other, two system can be in reference with each other regardless of the spatial different. Since both entities are in direct correlation with each other, actions performed on one system will be instantly influencing any other system that it is entangled with. Even though this is all very good progress, the actual realization of quantum entanglement does not allow the transfer of data at impossible speeds. This sort of data transfer from altering one system to get another action on another sytem through entanglement is called *quantum teleportation* and has only been theorized and hardly experimented with.

Now to go over the most recent progress of quantum computers, lets start with 1998: at this time, scientists were finally able to spread a single qubit aross nuclear spins. What does this mean? Spreading out the qubit makes the qubit harder to corrupt. This allows the implementation of quantum entanglement and allows scientists and researchers to study interactions between the quantum states and how they react. They used this to help understand what quantum information was being produced and processed. A few years later in 2000, Los Alamos National Laboratory developed a 7 qubit quantum machine. The way they constructed this machine was a very delicate and complicated process incorporating nuclear magnetic resonance and electromagnetic pulses. A few months later, IBM decided to debut their 5 qubit quantum computer, which they claimed was

the fastest and most advanced one to date with no other machine being able to match its potential and power. This machine used radio frequency pulses compared to the previous 7 qubit quantum computer. in 2005, the Institute of Quanum Optics and Quantum Information created the first qubyte. Yep, you guessed it, a qubyte is a sequence of 8 qubits. They did this using ion traps. Just for reference, an ion trpa is a combination of electric/magnetic fields that are used to capture certain particles in a vacuum; but to go more indepth on ion traps would be an entirely different research topic. In 2006, the researchers at Waterloo and Massachusetts developed very complicated and advanced methods on quantum control. This idea of quantum control they developed was created for a 12 qubit system; the complexity of quanutm control is exponential: the more qubits a system implements, the more complex the quantum control must be. Most recently in 2007, a Canadian start up company called D-Wave constructed a 16-qubit quantum computer. During the demonstration of the quantum computer, the company showed that this machine could solve sudoku puzzles and other puzzles on a large scale in seconds with relative ease. The company boasted the idea of a fully functional quantum computer within a few years, but that level of progress is not achieveable and that many claims of the company are impossible due to the fact that technology has not progressed that far enough to allow this. The future for quantum computers is very bright and the day that they are realized is when the industry will be revolutionized. Currently from various sources, Google, IBM, and NSA are working togther to create a fully-functioning quantum copmuter. Just this past March, Google just found a way to make quantum coputers more stable and have better reachability and debugging interfaces. The problem lies in quantum entanglement: by finding a way to stabilize qubits Google has found a way to program them and fix any errors.

But the most important question has yet to be presented in this paper: what is the future for cryptography with quantum computers? A few scientists and researchs claim that quantum computing threatens the end of cryptography. Why is this? From class, we learned that in MAC it is require to have signature and a key to encrypt the message. In order to break the MAC encryption efficiently, it has to be done in polynomial time. But a quantum computer is so fast that regardless of the time it takes (exponential), that the computer could break the key in seconds. Finding that key requires using a computer to perform millions of computations on very large numbers and then applying each produced key to the encryption to see if it can break the signature on the MAC with a forgery. A regular computer in today's age would take years or more to crack the signature, but using a quantum computer, time is not an issue. Quantum computers can break encryptions very easily due to the fact of quantum superposition. They can represent 0 and 1 at the same time allowing them to blast through computations with ease. But some believe that the basis of cryptography is not in jeopardy. By the emergence of quantum computers, this will also pave the way for more complicated and secure methods of encryption that will lead to a new type of cryptography (in theory). Not all quantum computing leads to bad things for cryptography. For example, take the one-time pad which we learned in class. With the one-time pad, two parties must share the same key. The problem with this was the transmission of the key itself to both parties. But with quantum computing and entanglement, the idea of Quantum Key Distribution allows the exchange and transfer of completely random keys at a distance and allows it to be done securely. Quantum computing is also a double edge sword for cryptography: it can break encryptions, but it can also produce keys that may be impossible to break. The computational power of a quantum computer may be able to produce super keys based on the polarization of photons. If someone attempts to steal or obtain this key, there will be a disturbance in the photon sequence and alter the key to which both parties will instantly recognize that their keys do not match. These keys can

be produced at immeasurbale lengths to ensure proper security.

After all the research I did, quantum computing turn out to be alot differen than I expected. Movies and culture do not depict the idea of quantum computing properly and it is a travesty. I thoroughly enjoyed learning about this topic and its effect on cryptography. Even though quantum computers are many years away, I may have found an interest in my career in which I hope to make an imprint on the history of quantum computing.