University of Texas at Arlington

Professional Practices: CSE-3314-002

The Impact of Quantum Computing on Simulations and Security

Assignment #5

15 November 2022

Landon Moon – 1001906270

This Assignment is submitted towards and in support of the partial completion of the requirements for the Professional Practices Course

**Contents**

Introduction 3

Why Quantum Computing 3

History of computing 3

Description of Quantum Computing / Encryption 4

Positive / Negative Impacts 6

The Future of Quantum Computing 7

Conclusion 7

References 8

The Impact of Quantum Computing on Simulations and Security

As the days go on, we are becoming more and more dependent on the use of computing to solve our problems. These problems can be about what the weather will be like next week or simulating the sheer stresses of a new bridge design. As our models become more complex and we demand more precise results, we require stronger, faster, and better supercomputers. Due to the physical limitations of current silicon-based computers, the development of quantum computers has started to look like the future of big data computing. Just as quantum computers will further increase our processing power and help our scientific and engineering models, this new leap will also risk how we keep our data encrypted

Almost everyone has heard about quantum computing and about how it’s the next big step for humanity’s computing power, but don’t necessarily know what to expect to come due to this new technology. The details of quantum computing are important to know because they will change how we interact with computers and the internet in the near future. At this point, quantum computers have been developed, it’s just a matter of integrating them to be commonplace in the computing world.

To understand why quantum computers are being developed now, we need to understand the history and development process of the traditional computers that are in use today. Long ago, in the 1940s modern computers were starting to be developed. These ‘modern computers’ would barely be recognizable to what we know today, but these computers worked on the same principles as an iPhone. The technology that started in the 1940s and consistently improved until today is that of the transistor. In the 1940s these transistors were made with vacuum tubes and were a “few centimeters” in size (Shkeer 2021). These transistors were large, heavy, and power-hungry. Eventually, in 1948 these vacuum tubes were replaced with modern transistors made of semiconductors (Shkeer 2021). The size of the transistor was reduced from about 40 micrometers in 1948 to 800 nanometers in 1987 and eventually to sub-5 nanometers in the modern day (Shkeer 2021). All these developments increased the processing power and reduced the energy consumption of our computers, but they have reached a limit. To give a sense of scale, the transistors that are being developed are around 2 nanometers while silicon atoms are about .2 nanometers (wafer-world 2021). This means new transistors are about 10 atoms across which leads to signal bleeding. Transistors can no longer easily get smaller without becoming unstable. This is where the idea of quantum computing comes in. Instead of avoiding the quantum interactions that are preventing traditional transistors from getting smaller, quantum computers are developed to exploit these extremely small interactions. In 1981 Richard Feynman published a paper outlining the possible applications of quantum mechanics to computing (Feynman 1981). Now because the use of quantum computing is needed to progress our ability to compute, multiple companies have started developing the foundation of quantum computers. IMB started developing its own quantum computer around 2010 and had a working prototype in 2015 (Mandelbaum 2021).

As we’ve already discussed quantum computing is a fundamental leap from the conventional computing we use today. Instead of using electrical signals that can start to be disrupted at nanometer scales, quantum computing uses the quantum effects at these scales to its advantage. The most fundamental difference between traditional computers and quantum computers is that the former used bit and the latter uses qubits. Bits can only have one value, either a one or a zero, while qubits are the analog equivalent. Qubits can hold any value between zero and one but “collapse” when we observe it (Tabb 2021). This collapse of the value is due to a phenomenon called superposition. While we think of things like atoms, light, electrons, and particles as points with a specific value, everything is more like a wave. Because these particles act as a wave, they can be “entangled” together so the waveforms interact with each other (Tabb). Similar to representing numbers as a binary number, qubits can also be entangled together to represent a number that can be determined when its waveform is collapsed. The main advantage of using qubits over traditional bits is that qubits can run through multiple possibilities at the same time. A good example of this would be solving the path through a maze. For a traditional computer to find the correct route through a maze, it has to recursively attempt every possible path until one finds the exit. A quantum computer on the other hand can have a qubit number representing the maze and introduce a qubit to ‘enter’ the maze at the start. Then by collapsing the state of the qubits, the correct path can be computed almost instantly.

Another important topic that is impacted by quantum computing is encryption. Everybody uses the process of encryption even if they don’t know about it. We all use passwords to log into websites, but our computers also automatically encrypt everything sent over an https connection. Some people also encrypt their storage devices on their computers or even utilize a cloud service that encrypts their data for them. We know this mystical ‘encryption’ process magically protects our data, but how does it work? Modern encryption works off of the difficulty to factor large numbers. With modern computers, it is very easy to multiply two numbers together but extremely difficult to work the other way around. When encrypting, your computer makes a “public key, which comprises two [prime] numbers” (Smith). The reason anyone can know the public key is that it is nearly impossible to figure out which two prime numbers generated it. When a computer tries to figure out what prime numbers a public key is made of, it must try every possible combination of them. These prime numbers are usually a couple of hundred digits long so brute forcing every combination would take years.

The development of quantum computing while difficult will increase humanity's processing power and will make multiple positive impacts on society. As I mentioned before, quantum computers are the next step in the development of supercomputers. By increasing the processing power of our supercomputers, any simulation or calculations on those supercomputers can be done either faster, more accurately, or both. Additionally, because of the nature of quantum computing, it is especially well-tuned for physics-based calculations. Simulations of weather predictions, orbit degradation, and structure stresses will be specifically well-suited for quantum computers. For our weather prediction models, this means that we can more accurately determine where a hurricane will hit and exactly when it will happen. This will allow people living in those areas to have more time to evacuate, saving more lives in the process. For our engineering models, stresses, pressures, and different forces need to be simulated. Simple simulations can be done on local servers but large calculations for skyscrapers, hydroelectric dams, and airplane stresses might be done on significant supercomputers. Depending on how affordable quantum computers become in the future, both large and small engineering simulations will benefit from the introduction of quantum computers.

While the introduction of quantum computers will benefit humanity and the field of simulation computing, there are also some negative impacts of introducing the technology. The most significant downside of quantum computing is its adept ability to decipher public keys for encryption. As I described above, public keys are made up of two very large prime numbers that are multiplied together. Modern computers would have to search every combination of numbers making them very slow in the public key decrypting process, but quantum computers can ‘guess’ these two prime numbers much faster. This means that if a strong quantum computer was able to be used for this purpose, all of our encryption methods would no longer be as safe as they were before. This means that people’s data could be accessed if the power of future quantum computers were able to be used. These people could own a quantum computer or just lease some processing time for it. This could leak sensitive information traveling over the web such as emails, file transfers, and https packets. Additionally, encrypted storage drives could be cracked faster than before. This all means that traditional encryption methods will no longer be safe.

While quantum computers exist already, they are not quite common in the super-computer marketplace. Development on quantum computers is slow but progressing. Funding for quantum computer development has “more than doubled to $1.4 billion in 2021 from 2020” (McKinsey 2022). We can expect this figure to keep on increasing as the potential of quantum computing becomes more visible. As the fundamental technologies of quantum computing are solidified, we can expect some commercialized quantum computing units to be sold to companies that need computing power. Eventually, quantum computers will far exceed the abilities of traditional computers where any large super-computer will be comprised of one or more quantum chips. Once quantum computers become more commonplace, our encryption methods will have to change to accommodate the new threat to our private information. Luckily NIST has already announced four algorithms that are quantum computer resistant (NIST 2022).

In conclusion, the introduction of quantum computers as a replacement for supercomputers will take us to the next step in computing. Quantum computers would be able to simulate physical models such as weather and structure stresses much faster and better due to the nature of how quantum computers work. While better simulations will benefit humanity, quantum computers also risk our privacy with encryption. With quantum computers, our public keys can much more easily be broken into its prime factors.

References

Feynman, R. P. (1981, May 7). *Simulating Physics with Computers*. Retrieved November 13, 2022, from https://s2.smu.edu/~mitch/class/5395/papers/feynman-quantum-1981.pdf

*How quantum computing could change the world*. McKinsey & Company. (n.d.). Retrieved November 14, 2022, from https://www.mckinsey.com/featured-insights/themes/how-quantum-computing-could-change-the-world

Mandelbaum, R. (2021, August 26). *Five Years Ago Today, we put the first quantum computer on the cloud. here's how we did it.* IBM Research Blog. Retrieved November 13, 2022, from https://research.ibm.com/blog/quantum-five-years

*NIST announces first four quantum-resistant cryptographic algorithms*. NIST. (2022, July 7). Retrieved November 14, 2022, from https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Shkeer, S. (2021, August 12). *Transistors: Let's time-travel together*. Transistors: Let’s Time-Travel Together. Retrieved November 13, 2022, from https://s-shkeer.medium.com/transistors-lets-time-travel-together-b9b93b8f580f

Smith, B. (2018, January 19). *This is how prime numbers keep your online shopping secure*. ABC News. Retrieved November 13, 2022, from https://www.abc.net.au/news/science/2018-01-20/how-prime-numbers-rsa-encryption-works/9338876#:~:text=The%20reason%20prime%20numbers%20are,17%2C%20or%20187%20and%201.

Tabb, M. (2021, July 7). *How does a quantum computer work?* Scientific American. Retrieved November 13, 2022, from https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/

waferworld. (2021, November 24). *How small can transistors get?* Transistors are an essential building block used in almost every electronic device. Learn how small they can get in silicon wafers, GaAs wafers, and more. Retrieved November 13, 2022, from https://www.waferworld.com/post/how-small-can-transistors-get#:~:text=The%20size%20of%20a%20silicon,silicon%20transistor%20smaller%20than%20that.

**CSE - 4314**

**Professional Practices**

**Academic Integrity**

**In order for your Assignment/Homework/Project to be accepted you must read the following, sign this form and attach it to your papers (as the last page of your assignment).**

**Academic Integrity:** Students enrolled in this course are expected to adhere to the UT Arlington Honor Code:

*I pledge, on my honor, to uphold UT Arlington’s tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.*

*I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.*

Student Signature:



Student Id Number: 1001906270

*Note: Must be read, signed and attached (stapled) as last page of homework or assignment. If it is a team assignment then all team members must read, sign and attach a single copy of the Academic Integrity form to the team’s paper as the last page. If not properly attached as last page a 2 point penalty will be assessed after grade assigned.*