A Path to Supremacy: Quantum Computing

Thomas Horowitz

Binghamton University

Abstract

Quantum computing represents one of the proposed paths that the computer science field may take in order to keep increasing the power of computers. Quantum computers can provide this extra power though the use of qubits instead of bits as the basic unit of memory storage, as a qubit can store a superposition of all possible bit configurations. Up until recently, quantum computing was purely theoretical. Recently, IBM created a functioning quantum computer and its capabilities are being explored by many scientists. Quantum algorithms like Shor’s prime factorization algorithm have the potential to revolutionize the field and need to addressed. Shor’s algorithm in particular has the ability to crack modern RSA encryption and a new form of encryption must be adopted to account for this. Quantum computing uniquely has the potential to fundamentally alter the computer science field for the better, but understanding what quantum computing’s impact will be is important and discussions must be had to figure out how to responsibly implement it.

A Path to Supremacy: Quantum Computing

**Introduction**

There exists a defining law central to computer science known as Moore’s Law. Gordon Moore, the CEO of Intel, observed that about every two years computer processors can fit twice as many transistors in the same amount of space. In other words, Moore predicted that computers become twice as powerful every every two years. This trend held strong for over 40 years; however, within the last five years, processor manufacturers started to experience problems with holding to this pace. Transistors have become so small that they are only a few atoms large. Someone cannot make transistors much smaller than a few atoms, so the computer science community had started to look for other ways to increase processing power. Quantum computing presents itself a relatively new paradigm in the field of computer science that operates completely differently from conventional computers. Until recently, quantum computing was not considered a viable option for replacing conventional computers, as a quantum computer had never been built. This attitude changed when IBM created IBM Q, the one of the world’s first quantum computer. Now, quantum computing represents the most promising advancement in computer technology, as more stable alternatives like three-dimensional integrated circuits do not increase the computational capabilities of computers, and quantum computing can solve previously unsolvable problems like cracking cryptographic algorithms. Specially, the IMB Q architecture provides a well designed quantum computer that demonstrates several advantages over classical computers. In addition, quantum algorithms, like Shor’s algorithm, provide solutions to problems that previously could not be solved. To understand the potential quantum computing has to fundamentally change computer science, it is important to have a working technical knowledge of how a quantum computer operates.

**Background**

In classical computer systems, bits store information. A bit can either represent a low or high voltage, or zero and one, respectively. A collection of these ones and zeros make up all memory storage and computational functions on a computer. At this fundamental level, classical and quantum computers start to diverge. In quantum computing, bits do not exist. Instead, quantum systems rely on a basic unit called a qubit. A qubit can be represented by properties of many different particles, such as the spin of an electron or the polarization of a photon. Any of these properties have two states they can exist in; however, unlike bits, which are restricted to either one state or the other, qubits can exist in a superposition of these two states.

While this distinction may seem that minor on the surface, closer examination reveals the power of the qubit. With four bits, there are 16 possible configurations of ones and zeros. Under classical computing, these four bits can only represent one configuration at a time. With four qubits, all 16 possible configurations can be represented at the same time using the quantum superposition property. This storage potential becomes astronomical even when considering only 100 qubits, which can simultaneously representpossible configurations. This capability has implications in many different fields in computer science. For example, This property has the potential to revolutionize data storage. A petabyte (1000 terabytes), a large memory size in computing, can currently be obtained by some supercomputers in existence today. A quantum computer with the same amount of qubits would be a near infinite memory storage.

Quantum computing has a more specific ramification on cryptography. The encryption of information currently employs powers of very large prime number. The logic behind this system uses the assumption that factoring these thousands digit numbers with a classical computer would take an astronomical amount of time. A quantum computer can factor any number in just one operation, by using superposition of qubits to testing every possible factor at the same time. Considering the wealth of private and classified information hidden behind encryption on computer systems today, the ethical questions raised by quantum decryption are numerous and of immense importance. Ethical dilemmas, and other issues with quantum computing, have led some to question the validity of computing as the best path for computing. Some have championed three-dimensional integrated circuits as a superior alternative to quantum computing.

**Precedents and Related Work**

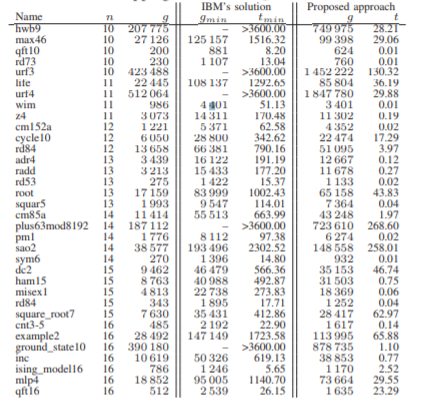
When faced with the issue of continuing the trend defined by Moore’s law, other solutions have been presented besides abandoning classical computers. Three-dimensional integrated circuits represents another path besides quantum computing. Three-dimensional integrated circuits is a computer architecture that involves stacking and vertically integrating two-dimensional circuits so they act as a singular processing unit. This process decreases power requirements and increases processing speeds when compared to a traditional two-dimensional circuit. This architecture attracts many in the computer science industry. The idea that current three-dimensional architecture uses classical computer infrastructure, but also obtains faster speeds at lower power costs would make this architecture seem like a natural choice for the future of computing. However, this conclusion is nearsighted. While three-dimensional integrated circuits do offer a clear speed advantage over current computers, they offer no computational advantage. The processes completable by a two-dimensional circuit are exactly the same as the ones for a three-dimensional integrated circuit. This limits the innovations of three-dimensional integrated circuits to purely faster performance and the effects of this improvement. Three-dimensional integrated circuits also encounter issues at the atomic level. In their research at the Korea Advanced Institute of Science and Technology, Jinwook Song, Seungtaek Jeong, Shinyoung Park, Jonghoon Kim, Seokwoo Hong, and Joungho Kim (2017) investate three-dimensional integrated circuits and uncover a glaring issue with them. They found that with so many circuits in such a small place, the electrons inside the circuit start to interfere with each other and corrupt data (Song et al., 2017). One cannot claim that the increased speed provided by three-dimensional integrated circuits outweighs its hardware limitation and the issue of data corruption. When compared to quantum computing, the increased speed of three-dimensional integrated circuits has less innovative potential than qubits, while electron interference has the potential to cause just as much memory corruption as quantum noise.

**Support**

**Technical Detail**

Computer science benefits from having a well understood and stable environment in which to conduct research. Developing anything for a computer, such as an algorithm or data structure, produces testable and observable results. However, quantum computing did not have this luxury until recently. Quantum computing has been discussed in the theoretical realm since the 1980s. Shor’s Algorithm, one of the most famous quantum computing algorithms, was created in 1994. Without a quantum environment to test the theory, quantum computing had limited impact on the computer science field.

In March of 2017, IBM launched its IBM Q program, which by June of 2017, had yielded a 16-qubit quantum computer available to the public to use through the cloud. In their article on the IBM Q program, researchers Alwin Zulehner, Alexandru Paler, and Robert Wille from Johannes Kepler University (2018) discuss how access to a functioning quantum computer will allow computer scientists to progress the field of quantum computing in a way that has never been possible before (Zulehner, Paler & Wille, 2018, p. 1135). Before quantum research can reach its maximum potential; however, an effective instruction set needs to be developed. On classical computers, there exists a series of instructions that are translated directly into machine code that all other computations are built upon. These operations can be seen with their operation speeds in figure 1 (Zulehner, Paler & Wille, 2018, p. 1138).

Figure 1: List of Zulehner’s, Paler’s, and Wille’s operations with speeds 

Operations like arithmetic, bitwise boolean operations, storing and loading data in memory, and conditional jumps are represented directly in machine code on classical computers. If these operations are not represented on the IBM Q architecture, the value of this computer has limits.

Classical logic gates can assign a value to a bit by simply reading present voltage and assigning a zero for low voltage and a one for high voltage. Trying this on a quantum computer forces the superposition of a qubit to collapse into zero or one and reduces the quantum system into a classical computer. By employing quantum gates that can read the probability of a qubit existing in the different superpositions, the superposition will not collapse (Zulehner, Paler & Wille, 2018, p. 1136). Using the Hadamard gates present in the IBM Q architecture, Zulehner, Paler and Wille developed a mapping of these circuits to some basic computer operations. This mapping satisfies all the basic functions required to create high level computing and algorithms, but also improves upon the previous solution created by IBM in both time complexity and memory usage. This improvement allows for researchers to explore more complex quantum computations, such as Shor’s decryption algorithm.

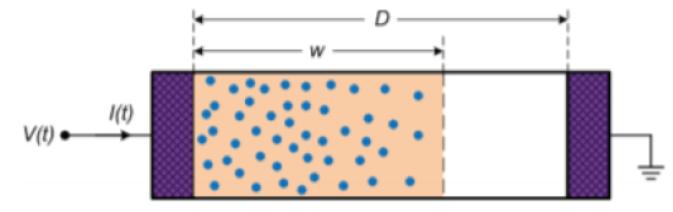
Mathematician Peter Shor developed several quantum computer algorithms. An algorithm for finding the prime factorization of a number, typically just referred to as Shor’s Algorithm has become the most famous of these algorithms. While a prime factorization algorithm might not sound revolutionary, the speed at which Shor’s Algorithm factors a number is log(n), where n is the size of the input and log(n) defines how much time it takes to run. No other algorithm can factor numbers in polynomial time. In other words, there exists no other algorithm that has an upper bound on the time it takes to calculate the prime factorization of a number. In their article, Shweta Nagaich and Y.C. Goswami (2015) explore the algorithm more on a simulation of a quantum computer to demonstrate its power and speed. Explaining how the implementation of Shor’s Algorithm worked necessitates an understanding of quantum simulations. The difficulting of representing a quantum system on a classical system comes from the need of representing qubits with bits. In their research on this issue, Ioannis Karafyllidis, Georgios Ch. Sirakoulis, and Panagiotis Dimitrakis (2018) propose the use of memristors as a solution. Memristors function like quantum logic gates, but work on classical computer systems. They mimic the states a qubit can obtain by utilizing the fundamental symmetry relations between current, voltage, charge and flux in the circuits of the computer. A visual representation of the memristor and the relations between current, voltage, charge and flux can been seen in 

Figure 2: Memristor schematic

figure 2 (Karafyllidis, Sirakoulis & Dimitrakis, 2018, p. 2). Moving on to the algorithm itself,

Shor’s algorithm derives its speed from the efficiency of quantum Fourier transforms (Nagaich & Goswami, 2015, p. 165). Quantum Fourier transforms takes a quantum state of several qubits

and maps the qubits to a superposition of all possible states. This superposition allows for fast calculation of Euler’s Theorem for very large numbers. While a quantum computer powerful enough to factor thousands of digit long numbers numbers are currently unrealized, the simulation used by Nagaich and Goswami was strong enough to use on three-digit numbers (Nagaich & Goswami, 2015 p. 165). Nagaich and Goswami also created a visualization of the algorithm, which can be seen in figure 3 (Nagaich & Goswami, 2015 p. 166).

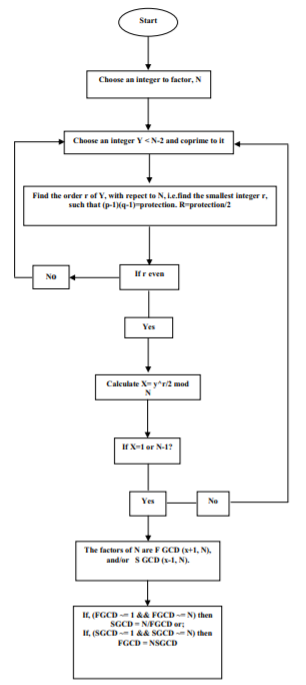


Figure 3: Shor’s Algorithm

While this may seem underwhelming, showing that the algorithm works on a quantum computer proves that when more powerful devices are created, factoring the thousands digit long numbers can happen.

Quantum computing’s use in encryption includes decryption as well. Quantum computers also allow for quantum encryption keys to be generated. These quantum keys have one important advantage over their classical counterparts: quantum keys can be transmitted without fear of being intercepted. In his article published in *Communications of the ACM*, Chris Edwards (2017) discusses a recent Chinese project to send a quantum key 750 miles from Beijing to Shanghai using quantum key distribution protocol. The Chinese used the angle of polarization of photon particles to encrypt the key. Decrypting the key requires knowledge of the angle of polarization of the photons, but guessing the wrong angle will alter the state of qubits and make the original state unobtainable. The sender can change the angle of the polarization during transmission, making the angle even harder to guess. Once the intended receiver obtains the key, The sender can safely decrypt the key with the receiver (Edwards, 2017, p. 13). In their research on quantum key distribution protocol, Walter Krawec, Michael Nelson and Eric Geiss (2017) created a useful visualization to represent the process, which can be viewed in figure 4

(Krawec, Nelson & Geiss, 2017, p. 1155). The Chinese were the first to show that this process

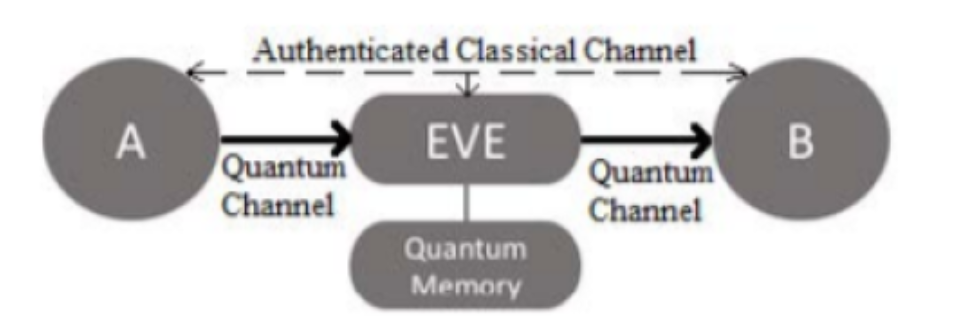


Figure 4: Quantum key distribution protocol

was possible with our current technology over a long distance. Before this transmitting, the longest a quantum key could travel without having quantum noise render the signal useless was about 100 miles. Using quantum signal boosters that would take the qubits and regenerate the key every 100 miles, the Chinese proved that the signal boosters, in conjunction with the right fiber-optic cables, could send a quantum key over any distance.

**Social Impact**

While quantum computing will impact general computing and the field of computer science, there are some areas of particular interest identified by computer scientists. In her TED talk, Shohini Ghose (2018) outlined three main fields of interest: molecular simulation, instantaneous information transfer, and quantum encryption. Molecular simulations on classical computers are limited by their inability to fully simulate the quantum realm in a binary system. However, with a computer that works in the quantum realm, these simulations can create a real quantum environment. This advancement has implications in mainly the healthcare industry and, more specifically, drug development (Ghose, 2018). Calculating interactions on both the atomic and quantum level of different drug molecules proves almost impossible to do accurately with classical computers. Modeling the quantum realm accurately presents difficulties and all the different properties of atoms are intensive to calculate. With a quantum computer, both of these issues are solved. Having a simulation that can accurately model these drugs may eliminate the need to test drugs on animals, as data on a drug’s effects can be collected just as accurately with computers. In addition to intermolecular interaction, the quantum realm also offers a pathway to instantaneous information transfer.

Instantaneous information transfer, or quantum teleportation, uses the property of quantum particles called quantum entanglement. The idea behind quantum entanglement is that two particles can become entangled, meaning that any changes in state of one particle reflects instantly in the state of the other particle (Ghose, 2018). For example, if one has a quantum computer where a clockwise or counterclockwise spin of an electron determines the states of a qubit, changing a qubit from a zero to a one will instantly change all entangled qubits from a one to a zero. While no communication system has been developed yet that takes advantage of quantum teleportation, this property could be very useful in the future for things like communication between people on different planets. It takes eight minutes for light to travel from the sun to earth. While this delay is not a prohibitively long time for communications, if humans ever tried to colonize planets beyond our solar system, this delay could become years long. With quantum teleportation, distance would no longer be an issue. Even in situations where conventional communication takes almost no time, the ability of quantum teleportation to send any information stored on a computer instantly will allow for information to spread very easily and rapidly all over the world.

Perhaps the most discussed implication of quantum computing is its impact on encryption. Quantum computing has profound impacts on both encryption and decryption. With the ability to factor arbitrarily large numbers with Shor’s Algorithm, RSA encryption becomes insecure. While there are other encryption methods that are used besides RSA, a vast majority of information on computers is encrypted with RSA. When a quantum computer is developed that can compute Shor’s Algorithm, the wrong people get their hands on the technology could become one of the largest security threats in the history of computers. Any systems encrypted with RSA could be hacked into and any data found within would be at risk. With such a large potential risk it is important to examine this issue and develop a plan for dealing with encryption before quantum computers capable of cracking RSA are created.

**Ethical Analysis**

Having sensitive data being easy to hack into and steal is clearly a violation of people’s negative right to privacy and any entity that deals with secure data has an obligation to protect it. Philosopher John Locke would argue that the right to privacy is an unalienable right and should be protected under any circumstance. Under this lens, any encrypted data should be encrypted under a different system that would be protected from quantum computing as soon as possible. However, this action could prove unnecessary, as probably an entity with a large amount of funding, like a government or research institution, would be the only ones with access to such technology. If the only people with access to quantum computers are people who are unlikely to use it for unethical purposes, one might as if there is a need to replace RSA. This argument follows the Utilitarian viewpoint held by philosopher John Stuart Mill, as the in this scenario, the extra privacy that results from implementing quantum encryption is outweighed by the costs. Also, there is a possibility that a quantum computer powerful enough for Shor’s Algorithm will not be developed for some time and any action now would be outclassed by a solution that can be done in 100 years.

Quantum encryption presents itself as a strong solution to this issue. Quantum key encryption is almost completely unbreakable and, as long as our understanding of quantum mechanics does not change drastically, this fact cannot change. While the equipment required now to send quantumly encrypted information is far too expensive for implementation on a wide scale, this limitation will disappear as quantum computers improve. Both Shor’s Algorithm and quantum encryption benefit from more powerful quantum computers, and both become cheaper and easier to implement on a large scale as these improvements are made. As long as both Shor’s Algorithm and quantum encryption progress at a similar pace, when quantum computers become powerful enough for Shor’s Algorithm, quantum encryption will be developed enough to match it.

**Conclusion**

With functioning quantum computers already in use at IBM, the quantum age of computing is very close at hand. Other alternatives, such as three-dimensional integrated circuits, have merits; however, the hardware limitations of three-dimensional integrated circuits reveal that they are not a viable alternative. The importance of understanding quantum computing and how this paradigm changes computer science cannot be understated. The instruction set developed for the IBM Q architecture proves that quantum computations are possible today and, with a powerful enough computer, eventually complex algorithms like Shor’s algorithm too. Once Shor’s algorithm is realized, data encryption will need to be adapted in order to remain secure. Quantum computing can also provide an answer to this issue through quantum encryption. As with any advancement in the computer science field, computer science professionals have an ethical responsibility to remain well versed with advancements in quantum computing. Quantum computing is complicated to understand, even for Computer Science professionals. The quantum realm exists outside the purview of classical Computer Science without much emphasis placed on it. This lack of emphasis is a grave mistake, and when quantum supremacy has arrived, knowledge of quantum computing will be necessary for the continued success of the computer science field.

**References**

Edwards, C., (February, 2018). Quantum technology forgoes unconditional security to

extend its reach. *Communications of the ACM*, 61, 2, 12-14. doi: 10.1145/3171578

Ghose, S. (2018). *Quantum computing explained in 10 minutes*. [Video file]. TED. Retrieved

from www.ted.com/talks/shohini\_ghose\_quantum\_computing\_explained\_in\_10\_minutes

Karafyllidis, I., Sirakoulis, G., Dimitrakis, P. (2015). *Representation of Qubit States using*

*3D Memristance Spaces: A first step towards a Memristive Quantum Simulator,* International Symposium on Nanoscale Architectures, Athens, 17-19 Fed 2018. doi: 0.1145/3232195.3232197

Krawec, W. O., Nelson, M. G., Geiss E. P., (2017). *Automatic Generation of Optimal Qantum*

*Key Distribution Protocols,* Proceedings of the Genetic and Evolutionary Computation Conference, Berlin, 15-19 July 2017. doi: 10.1145/3071178.3071182

Nagaich, S & Goswami Y. (2015). *Shor's algorithm for quantum numbers using MATLAB*

*simulator,* International Conference on Advance Computing and Communications Technologies, Haryana, 21-22 Feb. 2015. doi: 10.1109/ACCT.2015.16

Song, J., Jeong, S., Park, S., Kim, J., Hong, S., Kim, J. (2017). *Chip-level wireless power*

*transfer scheme design for next generation wireless interconnected three-dimensional integrated circuits*, IEEE Wireless Power Transfer Conference, Taipei, 10-12 May 2017. doi: 10.1109/WPT.2017.7953875

Zulehner, A., Paler, A., Wille, R. (2018). *Efficient mapping of quantum circuits*

*to the IBM QX architectures*, Design, Automation & Test in Europe Conference & Exhibition*,* Dresden, 19-23 March 2018. doi: 10.23919/DATE.2018.8342181