The Foundation of Quantum Computing and Its Future Global Involvement

Andrew Strimaitis

CSCI 556

Final Paper

I. ABSTRACT

Modern cryptology methods implemented in today's network systems revolve around public key encryption, pseudorandom generators and hash functions. Many methods of cryptology were thought to be secure due to their rigorously long decryption times for hackers. Problems like integer factorization, discrete logarithms, and elliptic-curve discrete logarithms are difficult decryption problems without the necessary information, thus was considered a practical method to secure systems. However, the research into quantum computing over the last two decades has finally developed technology and cryptology methods that can easily break into these systems.

The goal of this article is to provide a thorough background of quantum computing by informing the reader of its inspiration in quantum physics and mathematics, its translational application to computing, and its composite units. This article will compare the differences between quantum computing and standard computing technologies, specifically the differences between the probabilistic spectrum of quantum bits and the Boolean all-or-nothing approach of modern computers. The theory of multiple quantum states and its application to Shor's algorithm will offer insight on how to implement quantum formulas in applications, specifically the modern integer factorization problems. A comparison between the two different post-quantum processors, gate model quantum processors and the quantum annealing processors, will introduce the structure and computational strength of these systems with mention of Google's Sycamore processor and D-wave's quantum annealing processors. The article will conclude with mention of the challenges of implementing quantum technology, its current development cycle in society, and the overarching attempt to create quantum resistant cryptology for future safety.

II. QUANTUM: INSPIRATION FOR REVOLUTIONARY COMPUTING

Dating back to the 1920s, quantum physics began when Danish physicist Niels Bohr observed varying degrees of energy when electrons jumped from their orbits. Bohr, and later fellow physicist Louie de Broglie, discovered that an electron's energy distribution indicated that the electrons had both particle and wave-like properties (1). However, when future scientists began to further investigate the correlation between these two properties, they uncovered that the electrons never shared both traits at the same time. Werner Heisenberg famously licensed his Uncertainty Principle, stating that: "the position and the velocity of a particle cannot both be measured exactly, at the same time, even in theory" (1). Upon further collaboration between Bohr and Heisenberg, they jointly discovered the Copenhagen Interpretation, stating that: "A quantum particle is all of its states at the same time, rather than shifting in between its states" (1). The observed particle probabilistically chooses its state to represent at that given interval.

The Copenhagen Interpretation's notions of states introduced scientists to the concept of a *quantum state*. A quantum state "represents a physical state of a quantum system whose systems that demonstrate independent physical states yet predicts quantum theory" (2). This notion that quantum states alter their output values due to the present probability during observation upset scientists. Until this point, all states were classified with three-dimensional

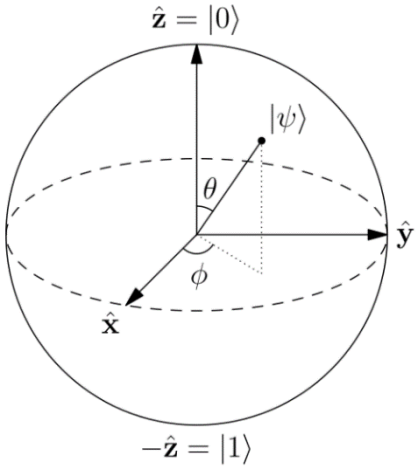
Euclidean vector calculus. To acknowledge this posing uncertainty with each state, the Euclidean notation of vector calculus was slightly altered to create the *Hilbert space*. A Hilbert space operates with the same measurements found in a Euclidean space but includes complex numbers for distances and a complex projective space (2). The complex projective space is used to keep track of the observable state at that measurement, like if the direction of a magnetic dipole pointed north or south (4). Hilbert spaces are vital to the development of quantum systems, so they will appear again later (4).

One of the fundamental proofs of quantum mechanics is called quantum superposition. Better known as Schrodinger's equation, "this states that two quantum states can be superposed together to form a new quantum state" (2). To put it simply, this means that quantum states can be combined to "form new quantum states while existing quantum states are built from old quantum states" (2). The concept of superposition and altering states means that one quantum state could hold every correct answer or every incorrect answer after numerous attempts of superposing quantum states with each other.

III. QUANTUM COMPUTING FUNDAMENTALS

Quantum computing was invented and developed using the same concepts originated in quantum physics. While modern computers hold fundamental operational units known as bits, quantum computers have their own complimentary units called *quantum bits* (or *qubits*). Like quantum particles, a quantum bit holds all the states found present in a modern computer bit, meaning that it holds both 0 and 1 (18). The difference is that the qubit will choose 0 or 1 depending on its probability distribution without strict assignment to that value. This means that 0 and 1 are not exactly values, but rather states reporting at the certain time. Standard computers are limited to the amount of computation due to information storing on bits with static assignments, while quantum bits can hold all assignments and complete operations at the same time (18).

Quantum bits hold some very impressive properties. As we mentioned before, quantum superposition operates via the superposition principle, which states that "if quantum states can exist in either one mode of operation or the other mode of operation, then there exists a state that is a combination of these two quantum states" (2). Even more impressive is quantum entanglement, which allows these qubits to hold the multiple results from superposition at the same time (18). Computationally speaking, this means that operations within qubits hold more solutions that operations with standard bits. Perhaps the most impressive development is the Schumacher compression. Benjamin Schumacher discovered that the level of data storage on a quantum bit can be compressed, so "the data will sit on less quantum states than they were operated on" (5). These states can be modeled by Bloch spheres (figure to the right), which operate similarly to Hilbert spaces. Both systems utilize a complex sphere with



imaginary coordinates to represent each quantum state (3). Bloch spheres allow quantum states to remove their amplitude constraints, allowing quantum systems to be characterized as two parameter systems. The standard equation vector representation in the Bloch sphere is: (3)

$$|\psi\rangle = \cos(\theta) \cdot |\mathbf{0}\rangle + e^{j\varphi}\sin(\theta) \cdot |\mathbf{1}\rangle$$

This equation provides enough context to begin characterization of quantum systems and advance applications within practical models. Further quantum formulas involve sphere manipulation which extracts the state found on the inverse side of the Bloch.

IV. QUANTUM SUPREMACY – Shor's Algorithm

Given their ability to operate via quantum parallelism, quantum computing has been labeled with the belief that they operate under quantum supremacy, meaning that they can solve problems that would take classical computers far too long to solve. Of the several functioning quantum decryption algorithms, the most popular is the Shor Algorithm. Licensed in 1994, Shor's focused on solving complex integer factorization by implementing the input number into the standard order-finding problem and then introduce the value into the Quantum Fourier Transform (4). This combination provides a quantum distribution to look for a specific interval of time where the guessed value equals the supposed factor.

Shor's Algorithm

Integer factorization operates under the simple premise that provided any integer, a computer must find the two factors whose product equals the integer. Integer factorization is easily solved by standard computer technology when the number is very small in value, however many computers use integers that contain up to 232-bit numbers, making the process far more challenging. In his paper, Peter Shor addressed that during the development of computers, several questioned whether quantum technology may outweigh the other technology. In doing so, Shor's Algorithm can complete integer factorization problems in polynomial time, a feat not completed by previous algorithms. To tackle integer factorization, Shor wrote that rather than "using Quantum Cryptography on the original number, we use the algorithm to find a number x that is an order of an element x that is the least integer r such that $x^r \equiv 1(\text{mod n})$." (4):

$$x^r \equiv 1(\text{mod n}) \rightarrow (x^r - 1) \equiv 0\ (mod\ n) \quad gcd\left(x^{\frac{r}{2}} - 1, n\right)$$

$$\left(x^{\frac{r}{2}} - 1\right)\left(x^{\frac{r}{2}} + 1\right) = (x^r - 1) \equiv 0\ (mod\ n)\ ;$$

Shor noticed that the above factorization can fail if factor *r* is an odd number or if $x^{\frac{r}{2}} \equiv -1(\text{mod n})$, but still "Selecting a random value at *x mod n* will output a factor *n* at a probability of $1 - \frac{1}{2^{k-1}}$, with *k* representing the number of distinct prime factors of *n*. This works as long as n is odd and not a prime power". (4)

Next comes the quantum component. First, we initialize a *quantum register* by combining quantum states via superposition. This superposition is computed via $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The first and second registers can be displayed like this (4):

$$\frac{1}{q^{\frac{1}{2}}}\sum_{a=0}^{q-1}|a\rangle|0\rangle \qquad\qquad \frac{1}{q^{\frac{1}{2}}}\sum_{a=0}^{q-1}|a\rangle|x^a \ (mod\ n)\rangle$$

The goal of the algorithm is to extrapolate values that are generated from the quantum state registrars listed above. As noted earlier, quantum values hold all states and assign themselves a value due to probability. That means that we cannot simply observe the value, but must enter them into the *Quantum Fourier Transform* (4):

$$\frac{1}{q^{\frac{1}{2}}}\sum_{c=0}^{q-1}\exp^{2\pi iac/q}|c\rangle$$

which combines into the unitary matrix to create the figure below:

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1}\exp^{2\pi iac/q}|c\rangle\ |x^a \ (mod\ n)\rangle$$

The unitary matrix allows the system to finally become observable. This matrix allows bystanders to quantify the data over a short time interval to locate an integer c such that $\frac{cr}{n}$ leads to a probability that $e^{2\pi iacr/q} = 1$ (4). The algorithm benefits from the constructive interference of answers moving closer to the correct answers and destructive interference of answers moving away from the correct answer (4). The final output becomes a probability graph that tracks the probabilities at different intervals, allowing the algorithm to select the highest probability located among this interval and move to the next iteration.

V. MODERN QUANTUM COMPUTERS AND PROCESSORS.

There are two primary types of quantum processors: Gate Model processors and Annealing processors. Gate Model processors are represented as "a sequence of quantum gates" and are conceptually similar to standard computer gates. However, one of their defining features is that they are reversible, "allowing computations to be stored locally while switching to compute another operation" (18). This can occur because gates create qubits at every state during initialization, then allow the gates to efficiently alter their state during their computations (18). Classical computers lose information when they operate by switching operations on their logic gates. The most popular of these quantum gates is known as the Hadamard gate, which operates computations via the Hadamard matrix (18):

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

The popularity of the Hadamard gate rose because of its smooth transitions in between states, making it very efficient during superposition. These transitions operate effectively over the 180°

rotation over the x and z axis of the Bloch sphere. The most famous gate processor is Google's Sycamore processor, which boasted in October that it solved computationally intensive sampling calculation in three and a half minutes while the same sampling would take 10,000 years on standard computational computers (9). This feat sparked the controversy of whether Sycamore indeed hit quantum supremacy (9). IBM, the fiercest Gate Model competitor to Sycamore, publicly noted that their model can successfully match and perhaps exceed the Sycamore's computational ability.

Quantum Annealing looks for a global minimum within many discrete local minima through fluctuated sampling. The energy function creates a double well potential graph, showing a well for a 0 bit and a well for a 1 bit. After magnetic field operation on qubits the double well shifts its probabilities towards one of the two states, choosing its identity from the weighted probability (5). Furthermore, quantum couplers allow qubits to influence each other to selectively popularize certain outcomes. These processors are especially useful for optimization and probabilistic sampling problems by computing energy minimization over different energy states (5). The field of quantum annealing has been completely controlled by D-Wave Systems, the only company that has released any quantum annealing processors. Their company website and YouTube channel further discusses the evolution of their processors.

VI. The Difficulties of Developing Quantum Computers.

Quantum Computers, like all modern and evolving technology, face certain technological barriers throughout the development cycle. Due to the technology's youth, much of the equipment is highly expensive and fragile. Qubits highly suffer from decoherence, indicating that a qubits interaction with an environment affects the outcome of the qubit and sometimes fails to initialize its state (7). Some causes of decoherence include temperature, noise frequency, and magnetism. To solve this problem, qubits must be properly isolated from their environment in well managed equipment. This high barrier of entry is the primary reason that few companies enter this market.

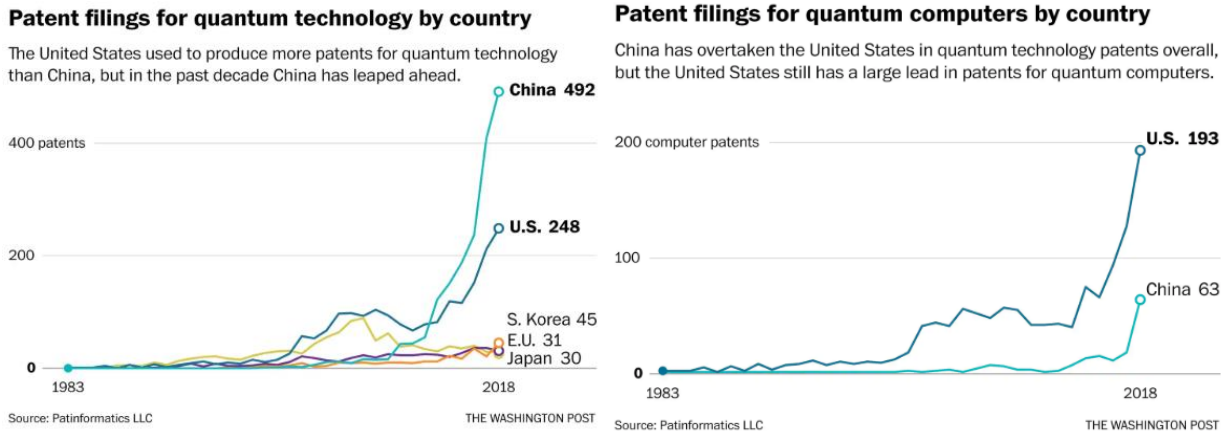
The DiVincenzo Criteria is a list of seven necessary criteria when developing quantum technology. The list is further divided into five standards for computation and two standards for communication (7). The criteria state that a quantum system must include (7):

1. A scalable, physical system populated with well characterized qubits.
2. The ability to initialize the state of all qubits to its ground, Hamiltonian state.
3. Decoherence times that are longer than the operation times
4. A universal group of quantum gates
5. "*The ability to accurately measure the outcome of the qubit*" (Direct Reference 7).
6. "*The ability to interconvert stationary and flying qubits*" (Direct Reference 7).
7. "*The ability to transmit qubits between locations*" (Direct Reference 7).

This list characterizes necessary attributes when building a quantum computer but does not encapsulate all the needs of quantum computing (7). Quantum computers are still being developed within a research setting, so there may still be additional requirements when designing an efficient, replicable quantum computer model.

VII. PATENTS AND POLITICS IN QUANTUM CRYPTOGRAPHY

Successfully filed quantum patents have risen by 430% over the past 4 years, making quantum technology one of the largest growing patent classes (8). On a global scale, China and the United States lead the world in the number of quantum technology patent filings. Patinformatics, an online database for technology patents, dictated that as of 2018 China holds 492 quantum technology patents while the United States holds 248. However, the United States holds 193 quantum computer patents while China holds 63. (8).



Intellectual property expert Steve Brachmann observed that certain companies are competing for access of different quantum technologies. As mentioned earlier, D-Wave focuses primarily on quantum annealing with 33% of their patents specifically targeting annealing and over 100 patents on qubits (8). Meanwhile, IBM and Microsoft have been competing for quantum gate-based patents.

The most notable observation was the number Chinese companies that focused on quantum cryptography discoveries. As pointed out earlier, quantum supremacy allows standard cryptography to be easily decryptable. American political officials have recently expressed a strong interest in the expansion of quantum discovery, perhaps out of fear of network security from the rise of quantum technologies or simply out of competition with Chinese developments. The first country to successfully develop manufacturable quantum technologies at a large scale will most likely usher an economic boom, becoming the only source for providing the most computationally impressive technology in the world.

In December 2018, President Trump signed the National Quantum Initiative Act which will provide $1.2 billion for quantum science research and discovery over the next five years (13). President Trump's chief technology officer Michael Kratsios lauded this act and declared that quantum information must be handled as the "Industry of the Future" (13). Additionally, members from the Department of Energy began talks with private companies like Google and Microsoft to discuss a collaboration for developing these technologies over the next five years. However, there are growing beliefs that China will invent this technology first. Over the past two years, China has outspent the United States on quantum funding 30 to 1 (11). China's QUESS quantum satellite has allowed the country to establish quantum connection over 1.3

kilometers. If these styles of quantum communication links persist and quantum computers are successfully manufactured, then China may be the only country that would have access to country-wide network security. This begs the question, what quantum cryptography methods exist to protect from quantum decryption?

VIII. THE SEARCH FOR QUANTUM RESISTANT CRYPTOGRAPHY

In April 2016, the National Institute of Standards and Technology (NIST) created a post-quantum cryptography contest. The goal of the competition was to develop cryptographic encryption algorithms that would be effective on both quantum and modern computers (10). After several years and hundreds of submissions, the NIST announced 26 semifinalists in January 2019. The semifinalists fall into three categories: lattice structure algorithms, code-based algorithms, and multivariate algorithms.

Lattice structures are perhaps the most secure and popular post quantum algorithms. The lattice structure is composed of a compilation of vectors to create a scaled sum that creates basis like the vector spaces talked about in our Hilbert space (10). The most famous Lattice problem is the Shortest Vector problem, which asks for the shortest vectors within the input grid. As the number of inputs rises, the ability to track the shortest vectors become so quantifiably challenging that even quantum computers struggle with finding a solution.

Multivariate algorithms focus on deriving polynomials with high orders into smaller level polynomial subfunctions. These algorithms operate through the Oil and Vinegar scheme, which combine variables across several different polynomials and integrate them within a multivariate polynomial (19). The only popular multivariate method for quantum encryption is the Rainbow Signature Scheme, which takes an Oil and Vinegar scheme with large levels of variables and uses the computation to secure a digital signature (19). This scheme does not have a large presence in standard computers but would be very effective as a quantum encryption.

The least used of three post quantum algorithms are code-based algorithms, which operate primarily through the usage of error-correction codes that target the errors within signal attenuation. There are many different variations of code-based algorithms, but most of them implement Gobba codes to search for redundancy (20). After publicizing the generator, code-based algorithms look for possible reverse frequency transmissions that might select individual points of error in the signal (20). Iterations from the resulting matrix probabilistically navigate to the correct error locations.

IX. Conclusion

Modern cryptography is used in nearly every industry because computers and network security are omnipresent in our economy. Many scientists don't view quantum computing as a feasible threat, but regardless it is important to prepare additional quantum algorithms to protect from quantum decryption schemes. If countries neglect to update their encryption methods, then they are in jeopardy of having their confidential data easily leaked. In order to stay relevant, the United States will must either continue searching for future applicable quantum resistant schemes or restructure its entire network communication system.

The fierce quantum competition between the United States and China parallels the Space Race between the United States and Russia in the 1960s. As the world enters a new decade, it will be interesting to observe the outcome of this competition and the revolutionary quantum products discovered along the way.

X. REFERENCES

[1] Orzel, Chad. “Six Things Everyone Should Know About Quantum Physics.” *Forbes*, Forbes Magazine, 8 July 2015, www.forbes.com/sites/chadorzel/2015/07/08/six-things-everyone-should-know-about-quantum-physics/#6e86fa857d46.

[2] Pusey, Matthew F., et al. “On the Reality of the Quantum State.” *Department of Physics, Imperial College London, Prince Consort Road, London SW7 2AZ, United Kingdom*, 11 Apr. 2012, doi:10.31988/scitrends.12804.

[3] Wickr, R. “What Is Lattice-Based Cryptography & Why Should You Care.” *Medium*, Wickr Crypto + Privacy Blog, 15 June 2018, medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717.

[4] Shor, Peter W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.” *SIAM Review*, vol. 41, no. 2, 20 Nov. 1994, pp. 303–332., doi:10.1137/s0036144598347011.

[5] Schumacher, Benjamin, and Michael Westmoreland. “Quantum Information Processing.” *Quantum Processes, Systems, and Information*, 1995, pp. 366–389., doi:10.1017/cbo9780511814006.019.

[6] Roberts, Jeff John. “Top 10 Patent Recipients for 2018 Include IBM, Apple and Microsoft.” *Fortune*, Fortune, 8 Jan. 2019, fortune.com/2019/01/07/ibm-tops-2018-patent-list-as-ai-and-quantum-computing-gain-prominence/.

[7] Meter, Van. “The DiVincenzo Criteria - Understanding Quantum Computers.” *FutureLearn*, Keio University, Mar. 2019, www.futurelearn.com/courses/intro-to-quantum-computing/0/steps/31587.

[8] Brachmann, Steve. “U.S. Leads World in Quantum Computing Patent Filings with IBM Leading the Charge - IPWatchdog.com: Patents & Patent Law.” *IPWatchdog.com | Patents & Patent Law*, IPWatchdog, 1 Dec. 2017, www.ipwatchdog.com/2017/12/04/u-s-leads-world-quantum-computing-patent-ibm/id=90304/.

[9] Hui, Jonathan. “Quantum Supremacy - Google Sycamore Processor.” *Medium*, Medium, 14 Nov. 2019, medium.com/@jonathan_hui/quantum-supremacy-google-sycamore-processor-6f30073a17fa.

[10] Materese, Robin. “NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'.” *NIST*, NIST, 31 Jan. 2019, www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals.

[11] Whalen, Jeanne. “The Quantum Revolution Is Coming, and Chinese Scientists Are at the Forefront.” *The Washington Post*, WP Company, 19 Aug. 2019, www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront/

[12] Kelly, Julian. “A Preview of Bristlecone, Google's New Quantum Processor.” *Google AI Blog*, Google AI, 5 Mar. 2018, ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

[13] Breeden, John. “How a New Law Supports Quantum Computing's Great Leap Forward.” *Nextgov.com*, Nextgov, 9 Jan. 2019, www.nextgov.com/ideas/2019/01/how-new-law-supports-quantum-computings-great-leap-forward/154039/.

[14] Boyle, Alan. “Help Wanted: U.S. Government Is Seeking Advice from Quantum Computing Experts.” *GeekWire*, 12 Sept. 2019, www.geekwire.com/2019/help-wanted-quantum-computing-experts-sought-advise-u-s-government/.

[15] Giles, Martin. “The US and China Are in a Quantum Arms Race That Will Transform Warfare.” *MIT Technology Review*, MIT Technology Review, 4 Jan. 2019, www.technologyreview.com/s/612421/us-china-quantum-arms-race/

[16] Herman, Arthur. “At Last America Is Moving On Quantum.” *Forbes*, Forbes Magazine, 20 Aug. 2018, www.forbes.com/sites/arthurherman/2018/08/20/at-last-america-is-moving-on-quantum/

[17] Aaronson, Scott. “Why Google's Quantum Supremacy Milestone Matters.” *The New York Times*, The New York Times, 30 Oct. 2019, www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html.

[18] Roell, Jason. “Demystifying Quantum Gates - One Qubit At A Time.” *Medium*, Towards Data Science, 28 Feb. 2018, towardsdatascience.com/demystifying-quantum-gates-one-qubit-at-a-time-54404ed80640.

[19] Ding, Jintai, and Bo-Yin Yang. “Multivariate Public Key Cryptography.” *Post-Quantum Cryptography*, 2004, pp. 193–241., doi:10.1007/978-3-540-88702-7_6.

[20] Bernstein, Daniel J., et al. *Post-Quantum Cryptography*. Springer, 2010.