Prevention of Quantum Computing Security Risks

(Technical Paper)

Risk Analysis Perspective on the Emmergence of Quantum Computing

(STS Paper)

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Electrical Engineering

By
Will Sivolella

November 1, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Bryn Seabrook, Department of Engineering and Society

Harry Powell, Electrical Engineering

Introduction

On the surface, the emergence of quantum computers is exciting as the processing power of computers will significantly increase leading to many new possibilities; however, the world must prepare for these new capabilities especially when it comes to security since many common encryption methods would be easily hacked with quantum computers. Studies have shown that quantum computing will become a multibillion dollar industry by 2030, and quantum computers for practical uses are projected to become prevalent in society in the next five to ten years (Fowler, G. F. (2021, April 28)). The emergence of quantum computers will lead to many possibilities across a variety of sectors. Some of which includes finance, where businesses can improve investment portfolios through optimal data analysis, healthcare, where DNA and pharmaceutical research will improve, as well as transportation, where air traffic analysis and route optimization will improve (Hollebeek, T. (2021, March 12)).

Although there are plenty of benefits to quantum computing, quantum computers will make many common encryption methods obsolete. Encryption is a way of disguising information through different mathematical algorithms in order to prevent unwanted users from accessing the information (Lake, J. L. (2020, September 24)). Once quantum computers become functional, they are able to process information exponentially faster than classical computers, which if nothing is done in foresight, will lead to the destruction of encryptions that protects data like online banks and even personal hard drives (Bushwick, S. (2019, October 8)). Although the rise of quantum computing is still some years ahead, quantum computing algorithms like Shor's algorithm has already been created and proven to crack the RSA encryption method, which is one of the most commonly used encryption methods in the world (Hollebeek, T. (2021, March 12)).

To address this issue, my technical topic will explore new encryption methods that are considered "quantum-proof" and learn the ins and outs of these methods. In the STS research paper, the STS theory of risk society, the way society organizes to identify and adapt to risk (Zimmerman, R., & Cantor, R. (2003)), will be used to assess the severity of the compromise of common encryption algorithms due to the emergence of quantum computers. There are many factors that go into assessing this risk, and risk society analysis primarily focuses on the scientific experts in the field as well as the public perception of the issue and how the two are related. It is important to make sure discrepancies between the experts and the public perception or media portrayal of the security risks of quantum computing are minimum. If there are major discrepancies, it will be important to figure out why certain information have been decided to be withheld from the public. The topic of quantum computers is just an example of one emerging technology that poses a risk to how society is currently structured. Thus, society's ability to solve an issue together and implement it on a mass scale is of momentous importance.

Technical Topic

Quantum computers have been proven to crack at least four common encryption methods (Bushwick, S. (2019, October 8)), and if nothing is done to change in anticipation of quantum computers, most private information will become public. But before "quantum-proof" encryption algorithms are explored, it is necessary to discuss how quantum computers operate and why they pose a threat to current encryption methods. The main difference between traditional computers and quantum computers is that traditional computers use binary bits, which are combinations of two different states 1s and 0s used to process information. Meanwhile, quantum computers use qubits (Martin, L. (2020, January 31)) which have four different states used to process information. Traditional computers use transitors in hardware which either allows an electrical

current to pass through it or does not. The state where the current passes through the transistor corresponds to the "on" state (or binary 1) while the other state means "off" (or binary 0). Using transistors, different logic gates can be constructed within the processors of computers. These logic gates perform logical operations on the data stored in the computer's memory based on what the user wants. These gates allow computers to work in a linear fashion in terms of problem solving. Thus, if a traditional computer wanted to find its way out of a maze, it traverse through all possible paths until it finds the solution (Tabb, M., DelViscio, J., & Gawrylewski, A. (2021, July 7)).

Quantum computers are considered revolutionary since they work completely differently allowing them to work significantly faster than traditional computers on certain problems. A quantum computer uses qubits, which are based on the theory that physics works differently at the subatomic level. One of the most common qubits which can have a "superposition" of states, so qubits can be 0 or 1 at once. The states can be classified as the spin of an electron or polarization of a photon before detection (Priya, V. (2021, October 22)). A way to think about qubit states is a spinning coin. There is a 50% chance that the coin will land on heads and a 50% it will land on tails. Thus, the can exhibit both forms at once by using probability (Martin, L. (2020, January 31)). So if a quantum computer wants to find the way out of a maze, it could consider all paths simultaneously (Tabb, M., DelViscio, J., & Gawrylewski, A. (2021, July 7)). This idea is related to how photons move with superposition and move in all directions at once until superposition collapses and the positions of the photons are measured.

The way quantum computers are able to consider numerous possibilities at once is the fundamental reasonsing behind how they are able to crack commonly used encryption methods. The most common of which is Rivest–Shamir–Adleman (RSA) encryption. To decrypt an RSA

algorithm, one must find the factors of the product of two prime numbers (so only two factors). Encrypting this algorithm is easy to do with say 15, where the prime factors are 3 and 5. However, factoring the product of two 256 bit prime numbers would practically take forever with conventional computers (Hauk, C. (2021, September 6)). With quantum computers this problem becomes exponentially faster as numerous factors are considered at once.

Human intuition makes it appear as though quantum computers are a generally faster version of conventional computers. However, this perception is not true in many cases and only applies to certain types of algorithms like RSA (Bushwick, S. (2019, October 8)). International Business Machines (IBM) has already developed an algorithm deemed safe against hackers using quantum computers called Cryptographic Suite for Algebraic Lattices (CRYSTALS). With CRYSTALS, the encryption keys are developed using algebraic lattice problems. An example of one of these problems oragnizationswould be to add four numbers out of a set of eight numbers, give the sum to someone, and ask them to determine which four numbers were added (Bushwick, S. (2019, October 8)). With a small set of numbers, this problem is not too difficult, but now consider a set of thousands of numbers with thousands of digits each, where thousands of them are added together (Bushwick, S. (2019, October 8)). This method is considered safe against quantum computers and involves much more processing to crack than RSA methods. Also, with CRYSTALS, there can be numerous combinations of numbers that lead to the sum, but there is only one right answer, so even if someone finds a single combination of numbers that fit, it may not be the correct combination. However, with RSA there is only one “right” answer. Thus, it is much more difficult to crack CRYSTALS than RSA, which is why it is the current leader in “quantum-proof” encryption methods. Regardless there are still many other encryption methods in the developmental stages and CRYSTALS is still being optimized. The goal of the technical

portion of the paper is to find the best “quantum-proof” encryption method available and explain how it works.

STS Research Topic

Many of the high-level encryption methods used by elite organizations including governments and larcge corporations across the world would currently be compromised by quantum computers. With no preperation for the emergence of quantum computers, there would be catastrophic implications for society. Private information would become public, and practically nothing stored on a computer would be safe. Thankfully, companies like IBM have already been working on quantum-proof encryption algorithms, and have developed some that work in theory (Kahn, J. (2021, September 22)). Not only have new encryption methods been researched, but businesses have also been preparing for a new world with quantum capabilities.

It is important that the “quantum-proof” algorithms completely replace encryption algorithms susceptible to hacking by quantum computers before quantum computers become practical and widely available in order to keep important data safe. The development of quantum computers at a practical scale primarily depends on one fact, which is creating an optimal environment for qubits (Tabb, M., DelViscio, J., & Gawrylewski, A. (2021, July 7)). The environment is all about getting quibit to operate at the quantum level, and that requires precise pressures and temperature for computers to operate at (Priya, V. (2021, October 22)). Circuits within the computer hardware operate at the quantum level when the temperature is at absolute zero, where practically no external energy enters the physical computer (Tabb, M., DelViscio, J., & Gawrylewski, A. (2021, July 7)). Maintaining this condition for long periods of time is quite difficult and requires extreme insulation to prevent any energy from entering or leaving the computer. It is especially difficult to create this condition in a home environment, and as of now

only a few quantum computing models have been created; however these models are way too large to be used by everyday people and even still can only create an environment stable for a small amount of qubits (Fowler, G. F. (2021, April 28)).

The STS topic of risk society theory will be used to analyze how society is identifying quantum computers as a security risk and what is being done to eliminate this risk. One of the most important factors in determining quantum computing as a risk is how quickly it's going, and when quantum computers will become available to crack current encryption methods. There are no practical quantum computers on the market, and the only models that have been developed so far are elementary and way too large to be used in a commercial setting. However, with a constant increase in the rate of funding, another important factor to consider, quantum computers could become commercialized in the next decade (Fowler, G. F. (2021, April 28)). It is also important to consider the process for developing quantum-proof algorithms. IBM currently implements the one they have developed, but also National Institute of Standards and Technology (NIST) has created a competition where anyone can submit algorithms perceived to be quantum-proof, and NIST will pick the best ones and optimize them (Bushwick, S. (2019, October 8)). This public forum creates an opportunity for anyone to collaborate in optimizing these algorithms.

Although risk analysis is a great way to perceive the security risks due to quantum computing, it is not perfect. One of the largest criticisms of sick society is that the whitholding of information to the public from an expert level is often viewed as an institutional failure using the lense of risk society (Mythen, G. (2004)). Risk society lacks the additional contenxt that provides information on why there would be a discrepancy between export and public information and instead always views a discrepancy with a negative connotation. Also, risk society primarily

focuses on the relations between experts in the relevant field and the public perception of the issue when issues can be much more complex than that (Mythen, G. (2004)). With regards to the topic of quantum computers and the compromise of encryption methods, there can be many unforeseen risks associated with quantum computers. Most of the research regarding encryptions against quantum computers and quantum computers themselves are theory based, and not necessarily tested. When quantum computers become available, so many sectors will improve making it hard to analyze how the future will change especially when using traditional computers to perform this analysis.

Research Question and Methods

To restate the research, there will be analysis of how society is preparing for the explosion of quantum computers in everyday usage with regards to security and protecting data. The research will take the lens of what experts believe about quantum computing as a security risk, and how the media portrays the topic to the public. Specifically, discourse analysis will be used to organize and evaluate literature and divide public perception from expert knowledge of the research topic. With regards to what will specifically be researched, the first step is finding what is necessary for quantum computers to become commercialized and where current tech and government leaders are in their research. This will help provide a timeline for when the risk becomes and issue. The next step is to find the leading quantum-proof algorithms and how it would be difficult for quantum computers to crack them. To put the research in a broader context, research on what companies are doing to adapt to a world of quantum capabilities will be gathered. Lastly, the practicality of changing security encryption methods across a variety of sectors will be evaluated. All these factors together will help determine how large of a risk quantum computing poses to the protection of our data and if anything needs to change.

Conclusion

To reiterate, the technical portion of my research topic is to determine optimal “quantum-proof” encryption to prevent against hackers using quantum computers. There is a lot of new and developing encryption methods that are said to be “quantum-proof,” and it is important that only the best are implemented at a large scale. Also, there is no one right answer for everybody as not all data are the same. Some encryption methods may take too much processing power to encrypt the data for some institutions. The main deliverable for the technical portion will be to find the optimal large scale algorithms different sectors of society such as private businesses or governemnt that is deemed “quantum proof” and explain how they work.

With regards to the STS research topic, risk society will be used to determine the security risks due to the emergence of quantum computer and the different perceptions of these risks. It is important that the risks are passed down from the experts in the field effectively. Obviously a lot will be at stake during the societal transition to quantum computers and it is important the risks are accurately taken into account and communicated effectively. Thus, risk society will be used to accurately determine the secitury risks of quantum computing and assess any discrepancies between expert knowledge and the media portrayal of this issue.

References

Bushwick, S. (2019, October 8). *New Encryption System Protects Data from Quantum Computers*. Scientific American. Retrieved October 24, 2021, from https://www.scientificamerican.com/article/new-encryption-system-protects-data-from-quantum-computers/#

Fowler, G. F. (2021, April 28). *When Will Quantum Computers Impact Our Day-To-Day?* Forbes. Retrieved October 19, 2021, from https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/04/28/when-will-quantum-computers-impact-our-day-to-day/?sh=5f0ffe8b43d9

Hauk, C. (2021, September 6). *Common Encryption Types Explained*. Pixel Privacy. Retrieved October 24, 2021, from https://pixelprivacy.com/information-security/common-encryption-types-explained/

Hollebeek, T. (2021, March 12). *The impact of quantum computing on Society*. SSL Digital Certificate Authority - Encryption & Authentication. Retrieved October 4, 2021, from https://www.digicert.com/blog/the-impact-of-quantum-computing-on-society.

Kahn, J. (2021, September 22). *IBM is getting business ready for a future with quantum computing*. Fortune. Retrieved October 24, 2021, from https://fortune.com/2021/09/22/ibm-quantum-computing-accelerator-training/

Lake, J. L. (2020, September 24). *Common encryption types, protocols and algorithms explained*. Comparitech. Retrieved October 20, 2021, from https://www.comparitech.com/blog/information-security/encryption-types-explained/

Martin, L. (2020, January 31). *Is quantum computing the end of security as we know it?* TechBeacon. Retrieved October 22, 2021, from https://techbeacon.com/security/quantum-computing-end-security-we-know-it

Mythen, G. (2004). Defining Risk. *Ulrich Beck: A Critical Introduction to the Risk Society*. (pp. 53-73). London, England. Sterling, Virginia. Pluto Press.

Tabb, M., DelViscio, J., & Gawrylewski, A. (2021, July 7). *How does a quantum computer work?* Scientific American. Retrieved October 4, 2021, from https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/.

Priya, V. (2021, October 22). *What is quantum computing? And How quantum computers work*. R2 Consulting. Retrieved October 17, 2021, from https://blog.r2c.io/what-is-quantum-computing-and-how-quantum-computers-work/

Zimmerman, R., & Cantor, R. (2003). State of the Art and New Directions in Risk Assessment and Risk Management: Fundamental Issues of Measurement and Management. In T. McDaniels & M. Small (Eds.), *Risk Analysis and Society: An Interdisciplinary Characterization of the Field* (pp. 451-458). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511814662.012