ESTABLISHING A FRAMEWORK FOR ANALYZING POST-QUANTUM CRYPTOGRAPHY SCHEMES

RESPONSIBLE MANAGEMENT OF INFORMATION ON THE INTERNET

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 Computer Science

By
Ibrahim Hamdy

November 1, 2021

Technical Team Members:
Ibrahim Hamdy

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

Rider Foley, Department of Engineering and Society

James Lambert, Systems and Information Engineering

Mohammad Mahmoody, Computers Science

Introduction

Digital infrastructure is an incredibly important facet of global society, comprising up to 92% of monetary transactions and the vast majority of both short-term and long-term communications. Mathematical topics like cryptography are no longer solely used by governments and militaries. They have become a necessary aspect of almost every digital transaction. Cryptography is the backbone of credit cards, email, internet access, and almost every other facet of digital communications. However, with recent advancements in the field of quantum computing, cryptography faces a new challenge that requires immediate action. The successful implementation of Shor's Algorithm, a quantum computing algorithm for factoring large numbers, would mean the immediate obsolescence of the popular RSA encryption scheme. This would present a serious threat to the modern technological infrastructure society relies upon because all modern forms of technology would be useless against this attacker. Finding dependable cryptographic schemes is increasingly important as the field of quantum computing continues to advance and improve its computational abilities. As a supplement to standard RSA encryption, new encryption schemes, like Lattice-Based Cryptography, are being developed that are capable of withstanding the implementation of quantum computing. However, while these new schemes show promise, there is little investigation into the feasibility and overall security proofs of these schemes, as compared to traditional cryptography schemes. For my technical topic, I will develop a security framework to analyze post-quantum cryptography schemes in order to compare their security and ease of implementation to traditional RSA schemes. This framework will take into account computational work, the probability of an attack, and the different benefits and drawbacks of these new forms of cryptography.

Because of this newfound reliance on digital technology, it has become increasingly important to analyze the effects that this technology has on society and determine how it might be changed to maximize its benefits while minimizing its harm. In 2016 the UN General Assembly passed a non-binding Resolution that "declared internet access a human right." However, increasing reliance on the internet has led to debates about internet freedom, legislation, and access. While internet freedom may seem like an extension of freedom of speech, this technology creates an environment previously unknown to humans: a culture of complete anonymity and protection from consequences. Because of this, widespread use of the internet, both in the United States and abroad, has led to a misinformation epidemic, the popularization and evolution of hate speech, the rise of hate groups, and even the organization and encouragement of violent events. However, regardless of the negative effects of this culture of anonymity, the internet creates the potential for communication, learning, and activism from across the globe. For my STS topic, I will examine internet freedom to better understand how changes to digital infrastructure can affect the type and flow of information and how we can use these changes to maximize utility and minimize harm.

Technical Topic

The purpose of cryptography is to mask data in such a way that the contents of that data are unable to be understood by anyone other than the intended recipient of that data. Modern cryptographic algorithms take advantage of "trapdoor functions" in order to implement this concept. A trapdoor function is a function that is computationally easy to calculate in one direction and nearly impossible to compute in the other direction. An example of this is prime factoring for large numbers. Determining whether two prime numbers are factors of a large number is easy, you simply multiply them together and compare the result to the large number. However, finding two prime factors of a large number is considerably harder. This is known as an NP-Hard problem, a classification given to problems when they cannot be efficiently computed by modern computational techniques. However, it has been proven theoretically that a functioning quantum computer capable of implementing an algorithm known as Shor's Algorithm for Factoring Large Numbers could find the prime factors of any given large number. Runtime analysis of Shor's algorithm shows that not only is this algorithm capable of determining the prime factors of large numbers, but it is also able to do so efficiently enough to be computed, bypassing the security of the trapdoor function. Therefore, any adversary able to construct a functioning quantum computer could then construct an attack against almost all forms of modern cryptography and poses an immediate security threat.

One proposed solution to the issue of quantum-based adversarial attacks on cryptographic schemes is lattice-based cryptography. Lattice based cryptography is the term used for any generic cryptographic primitive that utilizes lattices in order to construct security, including hash functions, signatures, encryption schemes, etc. Certain lattice based constructions appear to be secure against quantum-based attacks because they utilize the fact that certain well-studied

computational lattice problems cannot be solved efficiently by either classical or quantum computing. This more difficult problem supplements traditional trapdoor problems like factoring. There are many forms of lattice-based cryptography, but the most popular is the Goldreich–Goldwasser–Halevi (GGH) lattice-based cryptosystem. This method involves the construction of two matrices and their inverses. The two original matrices are then multiplied together to construct a new matrix which is then multiplied by the message to produce the cipher text. To decrypt the message, you simply have to multiply the cipher text by each of the inverted matrices. This encryption scheme, for sufficiently large enough matrices, cannot be efficiently decrypted without the knowledge of both inverse matrices.

One of the drawbacks of post-quantum cryptography schemes is that they lack the theory-based infrastructure for proving security that traditional cryptography schemes possess. Traditional cryptography schemes use “games” in order to prove their security. These games center around the question of whether or not, if given certain tools, an adversary would be able to efficiently construct an attack on the scheme. Depending on the game played, these tools usually include an encryption oracle, a decryption oracle, sample plaintext, sample cipher text, or other forms of information that an attacker may be able to gain access to in a real world environment. If an efficient attack still cannot be constructed against the encryption scheme when given these tools, then the encryption scheme is secure. However, current post-quantum cryptography games are few and under-utilized for proving security.

Additionally, while these schemes may hold in theory, there is very little work being done to determine the feasibility for these schemes to supplement current encryption schemes. One of the drawbacks of most post-quantum encryption schemes is that they require more computational work to compute both the encryption and decryption algorithms. This is because previous

schemes relied primarily on simple functions like Xors, while lattice-based cryptography utilizes more complex calculations like matrix multiplication which can take a much longer time to calculate with large matrices like the ones that would be needed to produce secure encryption schemes.

For my capstone project, I will develop a technical report that assesses the security and implementation feasibility of several post-quantum encryption schemes. This will include the construction of security games that highlight the benefits and flaws of these new encryption schemes and will present a standard for other cryptographic schemes to follow. Additionally, it will include examinations of possible computational speed-ups for these algorithms, runtime analysis and comparisons to classical encryption schemes, real-world benchmarking, and other information regarding the transition between classical encryption and post-quantum encryption.

For my technical topic, I will be establishing a framework to examine and compare the security, speed, and feasibility of several post-quantum cryptography schemes. Using this framework, I will examine Lattice-Based Encryption and Signatures, Code-Based Encryption, Multivariate-quadratic-equation signatures, and Hashing to determine whether each of these encryption schemes meets the basic qualifications of a secure encryption scheme, how these algorithms compare to classical encryption schemes in terms of runtime, and how much computational work is required to implement each of these schemes.

To establish a baseline for security, I will examine classical security games and their requirements in order to determine what properties of classical encryption algorithms make them secure. This will establish a threshold for the amount of computational work to crack the encryption scheme that is considered infeasible, thus rendering the encryption scheme secure. Then, I will adopt this definition of security under the assumption that the adversary has access

to quantum computing algorithms and hardware. These new encryption games will be used to construct security proofs that ensure the security of the encryption schemes.

To compare the speed and computational complexity of these different schemes to their classical counterpart, I will first use runtime analysis to determine how much extra computational work is required for encrypting and decrypting. Then, I will implement these algorithms and use time comparisons to determine whether or not these algorithms are capable of being implemented on classical computers, as well as their cost in both time and computational work.

STS Topic

The internet is a relatively new technology that has rapidly warped society in a way few other forms of technology have. A large interconnected network of computers, joinable by anyone at any time, that allows for communication of data across vast distances near-instantaneously, the internet has become a vital part of almost every country. However, technology this impactful rarely creates only positive impacts on society. Over Policing of the internet leads to almost total control over the spread of information within a certain area, which sets the stage for dangerous political ideas spread and controlled by those in power and the censoring of vital criticisms of governments and large corporations. Echoes of this can be seen in the actions of countries like China, who have censored access to information about events like the Tiananmen square massacre and Hong Kong protests. However, under policing can lead to widespread misinformation and disinformation, with the goal of spreading social unrest, giving rise to new or previously unpopular opinions, and encouraging radical change and even violence. Websites like 8chan, which operate on the principles of complete anonymity and freedom of speech, become hotspots for white nationalism, fascism, and extremist ideology which can lead to real world effects like the Christchurch Shooting in New Zealand and the Unite the Right Rally in Charlottesville, Virginia. One of the difficulties created by the uniqueness of this technology is that it is very hard to regulate. Determining how to control the spread of information responsibly with this large volume and audience is one of the greatest challenges of our time because of its scope.

While finding a solution to this issue may seem impossible, examining the internet and online infrastructure through a framework of Responsible Innovation can help identify what aspects of the internet require change in order to minimize the spread of misinformation while

maintaining the rights and freedoms of its users. Responsible Innovation is a framework of analysis that seeks to examine the role of products, processes, and business models within a society. Firstly, this framework stresses the need for innovation for a positive cause. More specifically, because technology interacts with social spaces in both positive and negative ways, this framework first analyzes how technologies interact with those social spaces. This focus is not necessarily on how the technology was designed to interact with society, but rather how it does interact with society in practice. For instance, how does the production and sale of this technology impact society, how do the business practices of those in charge of the technology impact society, what social aspects does the technology itself affect. Next, the framework looks at how ethics factored into the innovation and creation of the technology and analyzes the ethical framework under which the technology was designed. Another aspect considered is how this technology will impact consumers after long periods of time. This includes details like sustainability and environmental impact, the changing nature of how consumers interact with a technology, and the changing needs of consumers. Finally, the framework analyzes how insight played into the innovation of a given technology and what anticipated needs were being addressed with the creation of this new technology.

Using this framework, I will examine both the internet and frequently used websites, like Facebook and Twitter, to examine the origins, current status, and future of how this technology interacts with society and how it creates and changes social spaces. In doing so, I will create recommendations for changes to online infrastructure to prevent the spread of misinformation and harmful ideas while also preserving internet freedom and the rights of the individuals who interact with this technology. Additionally, I will examine policy and real world technological infrastructure, both in the United States and abroad, in order to determine how changes to these

policies and infrastructure result in changes to the interactions and effects of this technology on social spaces and how we can use these changes to create positive impacts and minimize harm. The goal of this analysis is to provide a complex set of policy recommendations for both policymaking within nations and websites' terms of service agreements and enforcement that will help combat misinformation online without instituting complete authoritarian control over the online flow of information. Additionally, this analysis will help create a template for further construction of online infrastructure that will allow for the implementation of new ideas on the internet in a responsible way that decreases the harm.

Research Question and Methods

For my STS topic, I will examine the internet, social media networks, and major websites through the lens of Responsible Innovation in order to determine the causes of misinformation and create responsible solutions to this problem through a series of technological infrastructure changes and national policies to combat misinformation without impeding on the rights of the users of these sites. To do this, I will examine the terms of service for major social media sites like Facebook, Twitter, and Instagram, as well as the algorithms and practices they use to both spread and combat misinformation. Additionally, I will use this framework to analyze the way that governments interact with the internet. To do this, I will examine policies established by separate nations, as well as by the United Nations, that involve the internet and changes to its access and use. This will include policies like Net Neutrality in the United States, the Human Rights Council's resolution that declares access to the internet as a basic human right, internet censorship in countries like Myanmar, and other forms of public policy. By doing this, an understanding can be formed about how public policy can be used to affect this technology which can be used to create changes to technological infrastructure that minimize the spread of false information in such a way that maximizes the freedoms and rights of the users of this technology.

Conclusion

When examining the impacts of new technologies on society, it is important to examine possible major changes that this new technology could create, and the potential harm they could cause. By preemptively exploring the possibilities of post-quantum cryptography and its integration into society as a replacement for modern cryptography, we can hopefully prevent the major security risks that come with quantum computing. We can create and implement new infrastructure that is secure from possible quantum cryptographic attacks which will allow us to continue the development of quantum computing techniques that allow us to expand the possibilities of computing without risking the creation of an attack on the network of digital communications that the world relies on.

When examining the impact of new digital technologies, it is important to examine the impact that these technologies have on the spread of the information. While the internet provides a potential avenue for learning, its uses can also be abused by both malicious users and people in power. By shifting public policy and the practices of websites on the internet, the spread of malicious information can be curbed, greatly limiting the harmful impacts that the internet can have on people. Because of this, it is important to establish a baseline for responsible control of the flow of information on the internet.

P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

Beckman, D., Chari, A., Devabhaktuni, S., & Preskill, J. (1996). Efficient networks for quantum factoring. PHYSICAL REVIEW A, 54(2). https://authors.library.caltech.edu/2179/1/BECpra96.pdf

Core, I. (2020, January 20). Quantum Encryption vs. Post-Quantum Cryptography (with Infographic). QuantumXC. https://quantumxc.com/blog/quantum-encryption-vs-post-quantum-cryptography-infographic/

Bernstein, D. (2008). Introduction to post-quantum cryptography. Department of Computer Science, University of Illinois at Chicago. http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf

Heger, M. (2021, June 24). Cryptographers Take On Quantum Computers. IEEE Spectrum. https://spectrum.ieee.org/cryptographers-take-on-quantum-computers

Bernstein, D. J., & Lange, T. (2017b). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. https://doi.org/10.1038/nature23461

Song, F. (2014). A Note on Quantum Security for Post-Quantum Cryptography. *Post-Quantum Cryptography*, 246–265. https://doi.org/10.1007/978-3-319-11659-4_15

Bernstein, D. J. A subfield-logarithm attack against ideal lattices. The cr.yp.to blog https://blog.cr.yp.to/20140213-ideal.html (2014)

Xu, X., Mao, Z. and Halderman, J., 2011. Internet Censorship in China: Where Does the Filtering Occur?. *Passive and Active Measurement*,

Wang, Y. (2016). Quantum resistant random linear code based public key encryption scheme RLCE. *2016 IEEE International Symposium on Information Theory (ISIT)*. Published. https://doi.org/10.1109/isit.2016.7541753

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145–195. https://doi.org/10.1103/revmodphys.74.145

Charles Berret (2019) *The Cultural Contradictions of Cryptography: A History of Secret Codes in Modern America* [Doctoral dissertation, Colombia University]

Holter, C., Inglesant, P., & Jirotka, M. (2021). Reading the road: challenges and opportunities on the path to responsible innovation in quantum computing. *Technology Analysis & Strategic Management*, 1–13. https://doi.org/10.1080/09537325.2021.1988070

Roberson, T., Leach, J., & Raman, S. (2021). Talking about public good for the second quantum revolution: analysing quantum technology narratives in the context of national strategies. *Quantum Science and Technology*, *6*(2), 025001. https://doi.org/10.1088/2058-9565/abc5ab

Hellegren, Z. I. (2017). A history of crypto-discourse: encryption as a site of struggles to define internet freedom. *Internet Histories*, *1*(4), 285–311. https://doi.org/10.1080/24701475.2017.1387466

Carr, M. (2013). Internet freedom, human rights and power. *Australian Journal of International Affairs*, *67*(5), 621–637. https://doi.org/10.1080/10357718.2013.817525

Warf, B., 2010. Geographies of global Internet censorship. *GeoJournal*, 76(1), pp.1-23.

Chih Wang, 2003. Internet Censorship in the United States: stumbling blocks to the Information Age. *IFLA Journal*, 29(3), pp.213-221.