RISK ANALYSIS PERSPECTIVE ON THE SECURITY RISKS OF THE EMERGENCE OF QUANTUM COMPUTING

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Electrical Engineering

By

William John Sivolella

March 28, 2022

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.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

THE RISKS OF QUANTUM COMPUTING AND FRAME FOR ANALYSIS

On the surface, the emergence of quantum computers is exciting and leads to many new possibilities across numerous sectors. Enterprises analyzing large data sets will especially benefit as quantum computers will improve the speed of many analysis algorithms. However, like most other innovations, these benefits do not come without tradeoffs. One of these negative ramifications include security risks. Specifically, quantum computers have been theorized to break common encryption codes in a matter of minutes, including Rivest–Shamir–Adleman (RSA) encryption, which is one of the most widely used computerized security methods in the world.

Thus, the world must prepare for the emergence of quantum computing by creating optimized and standardized quantum-proof encryption algorithms, which are considered encryption algorithms that are safe against the hacking capabilities of a quantum computer. Thankfully, organizations have already begun to work on quantum-proof algorithms. International Business Machines (IBM) created an algorithm called Cryptographic Suite for Algebraic Lattices (CRYSTALS), which is theorized to be safe even against quantum computing capabilities (Bushwick, 2019). These algorithms need to be optimized and implemented across a wide scale before quantum computers become an everyday reality to protect data like banking information, government secrets, and other important information.

The STS framework of risk society is used to evaluate the following research question: when will the implementation of optimized and standardized quantum-proof algorithms across enterprises be completed and will such security measures be taken before the emergence of quantum computers that are capable of decryption? The major factors to gauge a timeline and answer this question are when useful quantum computers will become available, when quantum-

proof encryption algorithms will become optimized and backed by trustworthy organizations and when these encryption algorithms will become implemented across governments and businesses.

The technical thesis will aim to find and understand an optimal quantum-proof encryption algorithm and walk through how the algorithm is deemed quantum-proof. Technical research is coupled with the STS thesis to provide an understanding for where the world currently stands in the development of quantum-proof algorithms. This context will contribute to the projected timeline and, most importantly, whether the world will be prepared for the emergence of quantum computing.

A large portion of risk society is to discern what the experts know about a topic compared to what the media portrays to the public (Mythen, 2004). The motivation behind these discrepancies and the discrepancies themselves significantly influence one's analysis of a risk. A portion of the STS research includes such discrepancies and how these discrepancies generally influence the projected timeframes of the development of useful quantum computers versus the integration of quantum-proof algorithms.

QUANTUM COMPUTING AND HOW IT IMPACTS ENCRYPTION

THE SIGNIFICANCE OF QUANTUM COMPUTING AND HOW QUANTUM COMPUTING WORKS COMPARED TO A TRADITIONAL COMPUTER

The emergence of quantum computing will lead to many improvements across a variety of sectors in society. One sector is finance, where data analysis techniques will be able to improve a wider scope of data to improve investment portfolios (Hollebeek, 2021). Along with finance, air traffic control systems will improve since programs would be capable of considering more routes in a faster time (Hollebeek, 2021). Quantum computers will most likely be utilized by large enterprises who are working with large data sets and not necessarily by individuals to complete typical, everyday tasks on their personal computers. This reasoning is because quantum computers are theorized to be faster than normal computers for certain tasks but not all. For many tasks like scheduling flights or playing chess, quantum computers are theorized to save the same algorithmic limitations of normal computers (Aaronson, 2008). Thus, quantum computers will not be utilized by everyone like normal computers; however, the influence of quantum computers will become apparent in society in the future. It is important to note that quantum computers will become prevalent in society not necessarily when or even if they appear on the market for typical consumers, but when they are utilized by institutions for practical purposes.

Not only is it important to understand the context for when quantum computers will significantly influence society, but it is also important to understand how quantum computers work to make the challenges associated with the development of quantum computers clear. Quantum computers have a completely different makeup than traditional computers. Traditional

computers use bits, “0s” and “1s”, to represent data and perform logical operations on such data. Meanwhile, quantum computers use qubits, which are often represented at the subatomic level by an electron and can assume the states of “1”, “0” or both simultaneously, where spin up is “1” and spin down is “0”. A qubit is deemed to exhibit both states at the same time since its state is the probability of its exhibiting a certain state, up or down, before the state is measured (Robinson, 2005). Qubits use properties of quantum physics to assume such states, which requires the computer to be in an environment where the temperature is absolute zero (Tabb, DelViscio, & Gawrylewski, 2021). Quantum properties can be observed at the atomic level, and these properties only exist in an environment where the temperature is absolute zero because there cannot be any external energy, including thermal energy, in the system. Achieving an environment of absolute zero is extremely difficult and requires extreme insulation. This difficulty is one of the reasons why it is so challenging to create a quantum computer. Maintaining an environment under these extreme conditions is also why quantum computers will most likely not be used for everyday tasks since classical computers operate in a normal environment.

It may be difficult to see the advantages of a quantum computer over a normal computer because once a tool is used to read the states of the electrons, the quantum property of each electron assuming a probability of a definite state is broken. Thus, the electrons assume definite states once they are measured. According to Hans Robinson, an assistant professor of physics at Virginia Polytechnical Institutes and State University, if a quantum computer consists of 100 electrons, and the user tries to read the states of each, the electrons would correspond to 100 bits of information just like a normal computer consisting of 100 bits. However, quantum computers can manipulate the states of the electrons without actually reading them. Quantum computers do

so by “flipping” the electrons or swapping the positions of them. Robinson also explains that what is meant by “flip" is to say an electron is 100% in the up state and 0% in the down state, a quarter flip would change it to a 75% up state and 25% down state. Unlike a traditional computer where the state of each bit is a specific number, the 100 qubits of a quantum computer can simultaneously represent all 100-bit numbers since the states of each bit are a probability. Thus, a computation can be done on all possible 100-bit numbers at once. This property is why quantum computers are exponentially faster than normal computers for running certain programs.

HOW ENCRYPTION AND DECRYPTION WORK AND WHY QUANTUM COMPUTING IMPOSES RISKS TO CURRENT ENCRYPTION METHODS

Now that the general ideas behind quantum computing are established, it is important to understand encryption to create a full picture of how the two are related. Encryption is a way of disguising information and keeping information private to prevent unwanted access to such information (Hauk, 2021). There are two popular methods of encryption, which are symmetric and asymmetric encryption. Asymmetric encryption is the type that is relevant to quantum computing. Asymmetric encryption is one of the most commonly used encryption methods and involves encrypting a message with a “public key” and decrypting it with a “private key”. It is easy to obtain access to the public key, but one needs the private key to decrypt the public key and access the wanted information. One of the most common asymmetric encryption types is RSA, which is used for a myriad of services including, email providers, web browsers, virtual private networks (VPNs), messenger services, secure communication channels, and data transfers (History Computer, 2021).

Decrypting asymmetric encryption involves solving seemingly straightforward math problems that are made complicated by using extremely large numbers. For example, RSA involves a public key, which is an extremely large prime number, and a private key, which are the prime factors of the public key. Once the factors are found, the private key is obtained, and can be used to access the information encrypted by the public key. Traditional computers can solve for the factors by taking the square root of the large number and dividing the large number by each whole number less than the square root to see which numbers factor it (Robinson, 2005). These problems are seemingly simple, but as the bit size of the keys increases, the time it takes to solve the problem increases, eventually reaching the point where normal computers cannot solve it within a reasonable timeframe. To put this trend in perspective, a traditional computer's factoring of a 9-digit number made up of two prime numbers only takes a few minutes, but a traditional computer's factoring of the product of two 256-bit prime numbers would practically take forever (Hauk, 2021).

Unlike classical computers, quantum computers do not need to go through all the options because they can test them all simultaneously. Going back to the example of a quantum computer consisting of 100 qubits in the previous subsection, the 100 qubits can represent all 100-bit numbers at the same time by each qubit's exhibiting a probability (Robinson, 2005). Only one randomly generated 100-bit number based on the probabilities of each bit will be the outcome (Aaronson, 2008). However, good programmers can make it so the probability of the right number being generated is maximized. Scott Aaronson, a technical writer at Scientific American, explains that this is achieved through the idea that there is an amplitude associated with each outcome, and that these amplitudes are combines through constructive or destructive interference. So, there is an amplitude for all 100 electrons to spin up and for 50 to spin up and

50 to spin down. Using destructive interference, amplitudes can cancel out when a positive amplitude interacts with a negative one and good quantum computing algorithms will make it so computational paths leading to a wrong result will cancel like so. Using constructive interference, amplitudes of the same sign combine to boost the amplitude corresponding to that result. Thus, programmers can maximize the amplitude corresponding to the probability that when measured the qubits will exhibit the right state.

It is clear that quantum computers run faster than normal computers for math problems like decrypting RSA encryptions since they can consider all possibilities at once. In fact, Shor's is a quantum computing algorithm that has already been developed and can theoretically crack RSA encryptions (Hollebeek, 2021). The fact that researchers have already developed quantum computing algorithms that can decrypt a large portion of private information impresses and urgency for an initiative to create quantum-proof encryption algorithms.

RISK SOCIETY DEFINITION AND HOW IT IS APPLIED TO THE SECURITY RISKS ASSOCIATED WITH THE EMERGENCE OF QUANTUM COMPUTING

Risk society, a form Pinch and Bijker's Social Construction of Technology (SCOT), is a frame used to analyze how society is identifying quantum computers as a security risk with regards to encryption and what is being done to eliminate this risk. Risk society in general involves assessing the risk of a situation and analyses the way society organizes to identify and adapt to a risk (Zimmerman, & Cantor, 2003). This framework is applied to quantum computing to analyze the projections of how long it will take for quantum computers to become part of everyday life. Another factor of this analysis is a projection of when quantum-proof algorithms will become optimized and backed by the appropriate entities. A subsequent third factor is when these optimized quantum-proof algorithms will become integrated into businesses, government agencies and other enterprises. These factors are combined to produce an estimation of what will win the race: quantum computers or the integration of quantum-proof encryption algorithms in society.

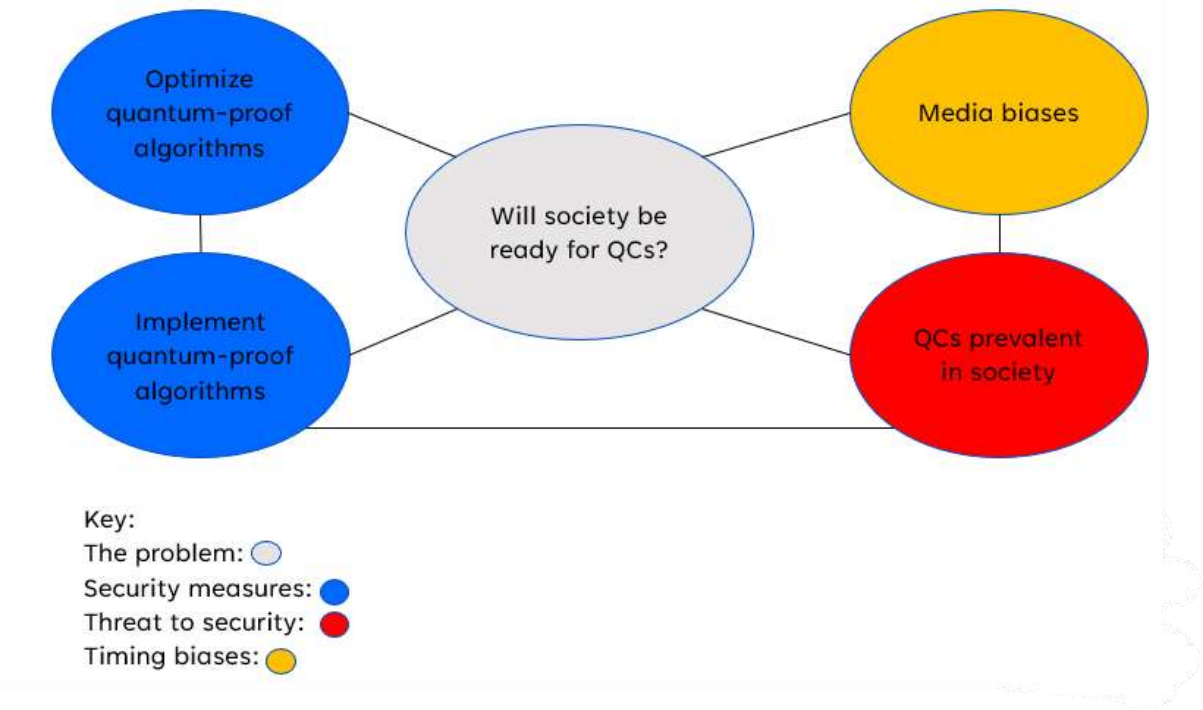

Figure 1: Risk Society Considerations: A proper analysis of the risk of quantum computers with regards to security is outlined in this figure. The major considerations for the risk society analysis as well as context for the problem are outlined in this figure (Sivolella, 2022).

The problem is not that simple, however. Risk society also involves determining what experts say about the risk of a situation and seeing if that aligns with what the media portrays to the public (Mythen, 2004). Many influential voices in tech often underestimate the time it will take to complete new projects. The motivation behind this action is that tech leaders already have good reputations, and the general public will believe what they say (Metz, 2022). Creating a lot of buzz around a project helps gain investments and improves marketing (Metz, 2022). Mainstream media also conveys quantum computers as an exciting and societal-changing innovation. With some respects that is true; however, this convection is blown way out of proportion, especially considering many experts believe quantum computing will not have a significant impact on day-to-day life for the average person. Quantum computers will most likely be utilized by certain software engineers working at large enterprises and the average

person will most likely never even have access to a quantum computer. The idea that mainstream media controls public perception is a key component to risk society (Mythen, 2004).

It is important to note that there are criticisms of the risk society framework and it does not capture the full picture of the risk the framework is used to analyze. Determining an extremely accurate analysis of a risk is much more complicated that risk analysis implies (Mythen, 2004). Also discerning between expert opinions and what the mass media portrays can be difficult since expert opinions are often distributed by mass media outlets. Any model or framework, though, has its limitations and there is no such thing as a perfect model or framework. It is impossible to accurately consider all variables of a problem, especially since there are often many unforeseen variables. However, risk society is the best STS framework for analysis of whether or not society will be ready for the emergence of quantum computers. Not only is the solution to the problem solved at a societal level, but there are also a lot of different levels of knowledge in the field of quantum computing, and it is important to use risk society to analyze expert opinions versus what the media says.

WHEN QUANTUM COMPUTING IS EXPECTED TO BECOME PREVALENT IN SOCIETY AND IF THE WORLD WILL BE READY FOR IT

PROJECTIONS AND ANALYSIS OF THE INTEGRATION OF QUANTUM COMPUTERS INTO SOCIETY

Before predictions about quantum computers can be made, it is important to outline what this future may look like. Contrary to what would be intuitive, quantum computers have already been invented. In fact, Google has a 53-qubit quantum computer able to complete math problems in 100 seconds when it would take traditional computers 10,000 years (O'Neill, 2020). However, the reason why this quantum computer is not a major news story, is that the computer does not solve a useful problem and was created for research purposes. The next step in the quantum computing industry is to develop a quantum computer that serves a practical purpose since nobody has developed a QC that is large enough or fast enough to offer any advantage over classical computers yet (Princeton University CITP, 2019).

In this future of useful quantum computers, it appears classical computers will still be used for most tasks because quantum computers do not have an advantage over normal ones for most programs. Common tasks for everyday people including sending emails, playing video games will most likely not be improved with a quantum chip in one's laptop (Harkins, 2019). If quantum computers will not improve a task, there is no need for an expensive and fragile quantum computer over a normal one.

The uses for quantum computers can be described by the following analogy: "Many people own a car for traveling to work, going to the shops, and visiting friends. In our analogy, the cars are traditional computers such as your phone and desktop computer and the analogous

trait is that the cars are good at performing small tasks quickly. In contrast, the hypothesized quantum computers would be like cargo ships: Despite being slower than a car, a ship is much more efficient. While both cars and ships are similar in that they move things from A to B, they transport them in different ways and have very different purposes. A ship cannot replace the job of a car but can allow us to complete tasks that are otherwise infeasible, such as moving large amounts of stock around the world" (Harkins, 2019, para. 4). Thus, quantum computers will be used by entities who are working with and analyzing large amounts of data just like how the ships are moving large amounts of stock in the analogy. Based on the description of how quantum computers work, one can see why quantum computers work with large data sets efficiently, and that is because in many cases, quantum computers can perform operations on all the data at once.

Who will have access to quantum computers also sheds lights on who will be using quantum computers for purposes of hacking. It seems like tech leaders who are developing quantum computers themselves like Google and IBM will have uses for them like improving marketing through analyzing people's data in improved ways. Also, they can use quantum computers to analyze stock markets and improve their investments. However, it seems difficult to believe large corporations with so much to lose would use quantum computers to hack into people's personal bank accounts and such. Also, it does not appear there will be many individual hackers who use quantum computers since they will be extremely expensive initially with a market only towards large enterprises. But it does appear that governments, entities with access to large data sets and a lot of resources, will most likely use quantum computers to try to break encryption methods and spy internally and on citizens of foreign nations.

If governments were to use quantum computers to break encryptions, they would most likely do it through a third-party collection of encrypted communications in internet traffic (Accenture, 2018). Obviously, these encryptions are not yet quantum-proof. If information about keys is in encrypted messages, third parties can theoretically use quantum computers to decrypt the message and uncover the key information which could subsequently be used to decrypt other messages in transit (Accenture, 2018). Although it appears likely that just governments will be using quantum computers for hacking purposes since it will be difficult and expensive for the average person to obtain access to quantum computers, it would not be past criminals to find a way. However, it would not be expected that individually acting criminals would have access to quantum computers but more likely criminal entities.

One may believe that people are prone to security risks from quantum computers once they hit the market. On the contrary, quantum computers designed for a specific purpose like hacking can be designed much earlier than when quantum computers hit the market. IBM has announced plans to develop a quantum computer with 1,000 qubits by 2023, which shows significant development in the quantum computing sector (Kahn, 2021). Analysts at Accenture believe quantum computers that can support Shor's algorithm or algorithms like it will be available by 2025 (Accenture, 2018). There are also contradictory timeline predictions from Patrick Howell O'Neill, an expert at MIT technology review, says it will likely be over a decade before there are quantum computers that can solve useful problems (O'Neill, 2020).

It seems fitting that the later prediction has a longer timeline for the development of useful quantum computers than the prediction that was made earlier. The motivations for underestimating predictions made by technology leaders have already been established, but it is also important to note why these predictions are so difficult. Leaders in the tech industry often

publicly compare the completion of new projects to old ones to make the new projects relatable for the audience according to Cade Mentz, a technology correspondent at The New York Times. This strategy makes sense for projects that are software-based like a new iPhone application because a project like this would involve many of the same processes that have been completed before. However, Metz also explains how one cannot compare quantum computing to old problems because it is nothing like old problems. Quantum computing involves the creation of a completely different hardware system compared to normal computers. This frequent treatment of new and different problems like old problems is a significant reason why the tech industry underestimates timelines for new projects. Thus, the 2025 and decade long predictions for the emergence of practical quantum computers both could be significant underestimates. Following similar logic, it seems like the decade-long prediction (made in 2020) seems more accurate because the world knew more about quantum computing and its development in 2020 than in 2018.

TIMELINE FOR THE DEVELOPMENT AND IMPLEMENTATION OF OPTIMIZED QUANTUM-PROOF ALGORITHMS

Since an understanding of the timeline for the emergence of quantum computers used for practical purposes is established, an understanding for the development of quantum-proof algorithms can be pursued. The National Institute of Standards and Technology (NIST) began a competition, where anyone can submit quantum-proof algorithms to an open-source portal, in 2017 (Bushwick, 2019). The competition is currently at a late stage with only fifteen contenders remaining (O'Neill, 2020). NIST plans to announce the winners in 2024. Although most institutions are waiting for an approved and standardized quantum-proof cryptography technique, some companies have taken the matter into their own hands. IBM has developed CRYSTALS,

an algorithm yet to be cracked by quantum or classical algorithms, and submitted it to NIST (Bushwick, 2019). IBM submitted CRYSTALs to the NIST competition but did not wait until approval to use it to protect a magnetic tape storing drive (Bushwick, 2019).

CRYSTALS is deemed quantum-proof because it generates keys through lattice problems. According to Vadim Lyubashevsky, a quantum-proof cryptography researcher at IBM, one simple example of a lattice problem is to add three out of a set of five numbers together and give the sum to a second party to determine which three numbers were added. "Of course, with five numbers, it's not hard," Lyubashevsky says. "But now imagine 1,000 numbers with 1,000 digits each, and I pick 500 of these numbers" (Bushwick, 2019, para. 7). Even if a quantum computer produces a seemingly correct output that adds up to the right number, it is most likely not the correct output because the correct output is only one combination of numbers. Thus, the algorithm is deemed quantum-proof. Many institutions will adapt to the quantum world at different rates. Most institutions, especially institutions that do not specialize in technology, will wait until a standardized and optimized quantum-proof encryption algorithm backed by an institution like NIST is established before implementing a standardized quantum-proof algorithm.

Just like how there are contradictory predictions about the emergence of useful quantum computers, there are contradictory predictions about the development and implementation of quantum-proof algorithms. The analysts at Accenture expect quantum proof algorithms to be widely implemented by 2025-2028 (Accenture, 2018). Meanwhile Dustin Moody, a mathematician at NIST believes "it takes a long time to standardize and get cryptographic algorithms implemented and into products. It can take 10 or 20 years. We need this process done before a quantum computer is done so we're ahead of the game." (O'Neill, 2020, para. 8).

TIMELINE AND SEQUENCE OF EVENTS CONNECTIONS AND SIGNIFICANCE

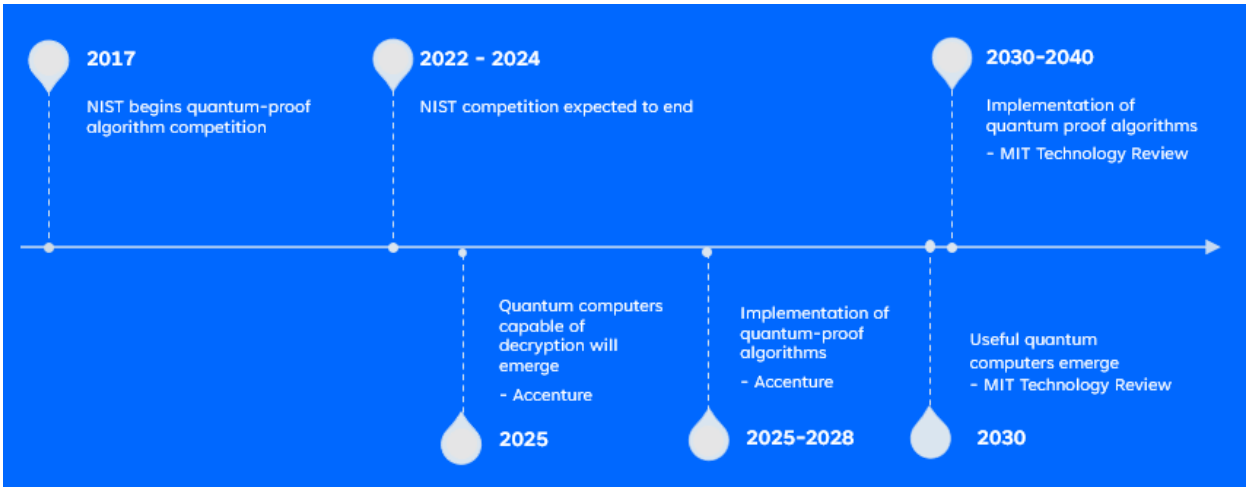

Figure 2: Projected Timeline of Quantum Computing and Encryption Events: The outline to a risk society perspective of if quantum-proof encryption methods will be implemented before quantum computing compromising current security methods. The timeline shows specific events in green and ranges of time in blue (Sivolella, 2022).

It is difficult to predict events related to quantum computing since the field is so nuanced and unlike problems seen before (Metz, 2022). It appears the predictions from experts at NIST and MIT Technology Review are more trustworthy than those made from the analysts at Accenture. This reasoning is not only because the NIST and MIT Technology Review predictions were made more recently, but also because NIST has a large influence on the release of a standardized quantum-proof algorithm. Regardless of the timeline predictions, the order of events is what matters, and both sources believe that most institutions will be ready for the security implications that come with the emergence of quantum computers. Also, as the emergence of quantum computers become more relevant, it will incentivize institutions to accelerate their implementations of quantum-proof encryption methods.

Thus, the world will most likely be ready for the emergence of quantum computing. Learning about encryption also sheds light on the idea that there is no way to eliminate all risks

of encryption methods since it is theoretically possible to hack any encryption, however; it is important to make this decryption as difficult as possible. Solving this problem has also shown how individuals and entities in society can collectively solve a problem and look out for everyone's best interest.

REFERENCES

Aaronson, S. (2008, March 1). The limits of Quantum Computers. *Scientific American*. Retrieved March 23, 2022, from https://www.scientificamerican.com/article/the-limits-of-quantum-computers/

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/

Harkins, F. (2019, September 8). Quantum computers are not faster than conventional computers. *The Quantum Insider*. Retrieved March 24, 2022, from https://thequantuminsider.com/2019/09/08/quantum-computers-are-not-faster-than-conventional-computers/

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

History Computer. (2021). *RSA encryption explained – everything you need to know*. Retrieved March 22, 2022, from https://history-computer.com/rsa-encryption/

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/

Metz, C. (2022, January 24). Why is silicon valley still waiting for the next big thing? *New York Times*. Retrieved February 16, 2022, from https://www.nytimes.com/2022/01/24/technology/silicon-valley-next-big-thing.html?searchResultPosition=1.

Mythen, G. (2004). Defining risk. Ulrich Beck: A critical introduction to the risk society. (pp. 53-73). London, England. Sterling, Virginia. Pluto Press.

Accenture. (2018). *Cryptography in a post- quantum world – accenture*. Retrieved March 22, 2022, from https://www.accenture.com/_acnmedia/pdf-87/accenture-809668-quantum-cryptography-whitepaper-v05.pdf

O'Neill, P. H. (2020, August 3). The quest for quantum-proof encryption just made a leap forward. *MIT Technology Review*. Retrieved March 22, 2022, from https://www.technologyreview.com/2020/08/03/1005891/search-for-quantum-proof-encryption-computing-nist/

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. Social Studies of Science, 14(3), 399–441.

Princeton University CITP. (2019, April 25). *Implications of quantum computing for encryption policy*. Retrieved October 22, 2021, from https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985

Robinson, H. (2005, February 21). What makes a quantum computer so different (and so much faster) than a conventional computer? *Scientific American*. Retrieved March 23, 2022, from https://www.scientificamerican.com/article/what-makes-a-quantum-comp/

Sivolella, W. (2022). *Projected Timeline of Quantum Computing and Encryption Events.* [Figure 2]. *STS Research Paper:* Risk analysis perspective on the security risks of the emergence of quantum computing(Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Sivolella, W. (2022). *Risk Society Considerations.* [Figure 1]. *STS Research Paper:* Risk analysis perspective on the security risks of the emergence of quantum computing(Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

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/

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.