The Implications of Quantum Computing in Cybersecurity and Cryptography in the Digital Age

Ben Murphy and Coleman Pagac

CYB – 010 Cybersecurity Principles

December 13, 2023

Imagine a whole new, faster method of computing than anything we have ever seen in today's tech-driven world. That's quantum computing—a revolutionary method that uses quantum bits, also called qubits, to enable computers to solve complicated problems in previously impractical ways. However, this astronomical amount of power also presents a significant challenge: cybersecurity. Cyberattacks and hackers are a constant danger to our digital environment. The possibility that quantum computers will be able to decipher the codes protecting our data further enhances the anxiety. This implies that our data, which we had assumed to be safe, could suddenly become exposed. With everything connected in our fast-paced digital age, protecting our data and systems is more crucial than ever. In order to safeguard our data from these quantum attacks, we must develop more robust privacy solutions that can stay secure in today's new technology. In order to ensure a safer and more sustainable digital future for all of us, it is imperative that we find a balance between the incredible potential of quantum computing and the urgent need for secure digital systems. This is where the intersection of cybersecurity and quantum computing becomes critical. This paper will discuss quantum computing, its concerns, and ways to prevent it.

Quantum computing is a relatively recent method of computing or at least physical quantum computers; the idea of quantum computing was initially proposed in the 1970s but only gained more traction and interest in 1982 when Richard Feynman gave a talk on how to simulate physics with computers (Feynman 1981). Over the years, what we may perceive as small leaps in the entirety of quantum physics seen through our lens reveals itself to be massive progress; for example, in 1998, the first two-bit quantum computer was created and tested as proof that this concept was possible, so possible that currently, IBM has recently announced their 1000 Qubit

quantum chip, which is the largest of its kind and the most Qubits in a useable manner. Quantum computers are different compared to regular computers in numerous ways. Connect computers function on the ability to use qubits instead of bits like standard computers. Where bits in binary computers function as a 0 or 1 and, in turn, have two options, Qubits use something called superposition to act like bits in the zero or one stage but also every possible variant in between. Quantum computers can harness and analyze the behavior of these particles and control these qubits to allow humans to study cryptography in numerous other possibilities. Qubits are different by nature and depend on the architecture of quantum systems. Most quantum computers function in frigid environments such as 0 Kelvin(-460°F), which is 2.7 kelvins colder than space, with space being-453.8°F. The extremely cold environment allows scientists are able to trap and use ions, photons, artificial or real atoms, or quasiparticles to create different models and different possibilities for analysis.

On the contrary, binary computers use binary bits and often silicon-based chips. One of the pinnacle abilities of quantum computers is their ability to use superposition within their qubits. Superposition is the ability for a bit to be in all 16 possibilities at once compared to a 4-bit binary computer, which can only be in one state at a time. By using superposition, scientists are able to feed these superposition qubits through quantum gates to lock in the bits of data to where the data can then be analyzed. This type of advancement permits us to have only 20 qubits; however, it can generate 1,048,576 configurations at once. While a binary computer would have to check every possibility, quantum computers simply excel in this exercise and can check multiple possibilities simultaneously. One downside of superposition is the bits are constantly changing and only become locked in when sent through a quantum gate and when analysis happens. The qubit locks in its state and loses its superposition feature. Due to this,

qubits and, in turn, quantum computers can be unreliable at times as the data can be changing, but this is one of the many features that are being worked on with quantum computers to improve these marvels of technology. This important research will allow scientists to harvest consistent mass amounts of data and information.

Cyber dangers are constantly changing in today's networked digital world. The constant complexity of cyberattacks is one major obstacle. Attackers are constantly changing their strategies and using advanced methods, such as phishing, ransomware, and zero-day attacks, to break into systems and take private information. (Shruti M, 2023) Furthermore, as connected devices and cloud services expand, the attack surface expands and introduces new vulnerabilities, making it harder and harder to keep an eye on and secure every point of entry. Organizations find it difficult to protect against a surge of cyber threats due to the lack of qualified cybersecurity personnel and the worldwide employee shortage. Organizations use a variety of cybersecurity safeguards and encryption methods to prevent these threats. The first line of defense consists of firewalls, intrusion detection systems, and antivirus software, which work to stop unwanted access and identify dangerous activity. A fundamental component of cybersecurity, encryption uses algorithms to condense data and make it unrecognizable without the decryption key. Advanced encryption protocols, such as Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES), are frequently used to safeguard data while it's in transit and at rest, guaranteeing its integrity and secrecy.

Furthermore, secure network protocols and multi-factor authentication (MFA) improve data protection and access control, strengthening cybersecurity defenses. Even with the effectiveness of current cybersecurity defenses, classical computing is often unable to deal with complex attacks, particularly when it comes to quantum computing. Since quantum computers

have the potential to solve mathematical problems like integer factorization exponentially quicker than classical computers, the majority of security measures' cryptographic algorithms rely on this fact. Due to the possibility of quantum computers breaking commonly used encryption standards and jeopardizing the secrecy of sensitive data, this poses a threat to the security of encrypted data. The coming threat presented by quantum computing highlights the need for developing cybersecurity protocols and encryption algorithms that are resistant to the disruptive power of quantum computing. It also highlights the inherent drawbacks of classical computing in terms of defending against potential cyber threats in the future.

Quantum computing has been a staple of human progress and ingenuity in the past decades, allowing humans to compute on the same level as molecules. However, Quantum Computing has also been a staple of how cybersecurity will always have a constant stream of new threats. With quantum computing, companies may be able to protect themselves further than ever before. Since Shor's Algorithm in 1994, scientists and computing experts alike have known that one of the most secure encryption algorithms, RSA, was no longer a secure encryption method; in the next few decades, this impenetrable encryption method could be deciphered in minutes. (Michaela Lee, 2021)

To combat this, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) created a competition to have companies and teams create the best quantum-resistant algorithms; together, they came up with four new groundbreaking encryption methods. Three of the four chosen encryption methods are lattice-based Kyber, Dilithium, and Falcon, while the fourth, Spins, uses stateless hash-based signatures. Algebraic lattices have become a staple in quantum computing and, overall, will likely become the standard for encryption due to

their asymmetric nature, allowing for private and public key encryption. Overall, three lattice-based encryption methods work under the same principles.

You, as the user, create two sets of vectors. A vector is an object that has both a magnitude and a direction. With these vectors, one set should be created to be simple, easy to understand, and allow for faster decryption. The vectors that you create as a public set are a much more complicated set of vectors to increase the difficulty of decryption. These are the public vectors that will create our lattice. Using the set of public vectors, you can map out a set of points by using each vector going in the X&Y direction. All these points will combine to create something called a lattice. To encrypt, the user chooses a point on the other person's lattice, which in this case would be the public lattice, and you add a little bit of noise to shift the data slightly off of the point so that it is not precisely on the specific chosen point. This is then taken and integrated into the multiplication and encryption of the data, where the only way to decrypt is to know the specific point or slightly off of a point where the computer must approximate the closest point to our data. This concept of lattices in encryption is challenging to understand but still manageable and can be completed by a human. This is due to how the presented lattice-based encryption example has been calculated on a 2-dimensional lattice; the current and future encryption methods are calculated on 1000-plus dimension lattices. By being encrypted and calculated on 1000 plus dimensions, a regular computer struggles to understand how to decrypt, as well as a quantum computer. Even with theoretically thousands of more qubits, a quantum computer will not be able to solve these encryption methods.

The advent of quantum computing will change the trajectory of technology as we know it, offering previously unattainable computing power but posing several significant obstacles that

require careful planning. Three main areas of concern are at the forefront of these challenges: financial systems, national security, and privacy and security ethics. (Finra, 2023)

Since existing encryption techniques may be vulnerable to quantum computing, national security is the highest priority. The effectiveness of standard encryption is in jeopardy because of the increased computing capability of quantum computers, which exposes sensitive data, military plans, and intelligence assets. Protecting national interests requires immediate action to reinforce encryption standards against quantum attacks. (Quantum Exchange) The situation affecting the stability and security of international financial systems is equivalent. The potential for quantum computing to attack banking systems, transaction processes, and digital currencies could leave current security protocols ineffective. Ensuring the resilience of financial infrastructures against future quantum attacks requires immediate innovations and upgrades. Throughout this shift, ethical issues arise frequently, especially regarding the fine line between security and privacy. The potential for quantum computing to crack existing encryption techniques might reveal enormous quantities of personal information, prompting questions about how well individual privacy rights are being protected. It becomes more complex and crucial to balance protecting private rights and keeping strong security measures.

To tackle these obstacles, a coordinated and aggressive strategy is required. Governments, businesses, and specialists must work together to develop and implement quantum-resistant encryption techniques as soon as possible. Public awareness campaigns are essential in simultaneously educating people about the effects of quantum computing on privacy and data security and enabling them to adopt the appropriate safety measures. A comprehensive plan that strengthens financial systems fortifies encryption standards and negotiates the complex ethical issues of privacy. Security is necessary to prepare for the era of quantum computing. By

preparing now, we can successfully reduce hazards and guarantee a safe transition into this new technological frontier.

The anticipated arrival of quantum computing signifies a profound transformation in the field of cybersecurity, prompting an in-depth awareness of its complex effects and a pressing appeal for intervention. The inevitable convergence of quantum computing with the fundamental principles of financial stability, individual privacy, and national security highlights the urgent need for proactive and cooperative actions. The primary problem concerns the vulnerability of present encryption protocols to the unmatched computational capacity of quantum computing. Strengthening encryption mechanisms against quantum decryption capabilities is an urgent need due to the approaching risk of breaches to national security, including revealing sensitive government data and classified information. Meanwhile, the vulnerability of international financial systems to possible quantum attacks presents a significant risk to global economic stability, needing quick and creative updates to prevent disruptions. The landscape is further complicated by ethical issues, which call for a careful balancing act between protecting individual privacy rights and robust security measures. Achieving this balance is crucial with quantum computing's ability to crack encryption that protects our private information. Governments, businesses, and experts must collaborate to create and apply newly created quantum-resistant encryption techniques. Simultaneously, massive public awareness campaigns are essential to equipping people with the knowledge they need to understand and negotiate the effects of quantum computing on privacy and data security. At this crucial point in history, the proactive actions that we take now will play an essential part in establishing a practical and ethically sound cybersecurity environment in the emerging era of quantum computing, therefore laying the foundation for a secure digital future.

Bibliography

Cho, Adrian. 2023. “Quantum Computers Take Key Step toward Curbing Errors.” Www.science.org. February 22, 2023. https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors.

“Falcon.” n.d. Falcon-Sign.info. https://falcon-sign.info/.

Feynman, Richard P. 1982. “Simulating Physics with Computers.” *International Journal of Theoretical Physics* 21 (6-7): 467–88. https://doi.org/10.1007/bf02650179.

Giles, Martin. 2019. “Explainer: What Is a Quantum Computer?” MIT Technology Review. MIT Technology Review. January 29, 2019. https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing.

Gossett, Stephen. 2022. “Quantum Computing: Everything You Need to Know.” Built In. August 17, 2022. https://builtin.com/hardware/quantum-computing.

Grumbling, Emily, and Mark Horowitz, eds. 2019. *Read “Quantum Computing: Progress and Prospects” at NAP.edu*. *Nap.nationalacademies.org*. The National Academies of Sciences, Engineering, Medicine. https://nap.nationalacademies.org/read/25196/chapter/1.

In a Nutshell, Kurzgesagt. 2015. “Quantum Computers Explained – Limits of Human Technology.” YouTube Video. *YouTube*. https://www.youtube.com/watch?v=JhHMJCUmq28&ab_channel=Kurzgesagt%E2%80%93InaNutshell.

Joseph, David, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen.

2022. “Transitioning Organizations to Post-Quantum Cryptography.” *Nature* 605 (7909): 237–43. https://doi.org/10.1038/s41586-022-04623-2.

Lee, Michaela. n.d. “Quantum Computing and Cybersecurity.” https://www.belfercenter.org/sites/default/files/2021-07/QCSecurity.pdf.

M, Shruti. 2022. “10 Types of Cyber Attacks You Should Be Aware in [2021].” Simplilearn.com. November 11, 2022. https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks.

Micciancio, Daniele, and Oded Regev. 2008. “Lattice-Based Cryptography.” https://cims.nyu.edu/~regev/papers/pqc.pdf.

Muller, Derek. 2023. “How Quantum Computers Break the Internet... Starting Now.” Www.youtube.com. April 20, 2023. https://www.youtube.com/watch?v=-UrdExQW0cs&ab_channel=Veritasium.

Nellis, Stephen. 2023. “IBM Shows New Quantum Computing Chip, Targeting 2033 for Large Systems.” Reuters. December 4, 2023. https://www.reuters.com/technology/ibm-shows-new-quantum-computing-chip-targeting-2033-large-systems-2023-12-04/.

NIST. 2022. “NIST Announces First Four Quantum-Resistant Cryptographic Algorithms.” *NIST*, July. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

Preskill, John. 2018. “Quantum Computing in the NISQ Era and Beyond.” *Quantum* 2 (2): 79. https://doi.org/10.22331/q-2018-08-06-79.

“Quantum Computing and the Implications for the Securities Industry | FINRA.org.” n.d. Www.finra.org. https://www.finra.org/rules-guidance/key-topics/fintech/report/quantum-computing#:~:text=In%20recent%20years%2C%20several%20major.

Schwabe, Peter. n.d. “Dilithium.” Pq-Crystals.org. https://pq-crystals.org/dilithium/index.shtml.

———. n.d. “Kyber.” Pq-Crystals.org. https://pq-crystals.org/kyber/index.shtml.

“SPHINCS+.” 2015. Sphincs.org. 2015. https://sphincs.org/.

“The Quantum Computing Impact on Cybersecurity | Quantum Xchange.” 2020. QuantumXC. January 24, 2020. https://quantumxc.com/blog/quantum-computing-impact-on-cybersecurity.

Think, Big , and Michio Kaku. 2023. “Michio Kaku: Quantum Computing Is the next Revolution.” Www.youtube.com. August 18, 2023. https://www.youtube.com/watch?v=qQviI1d_hFA&ab_channel=BigThink.

“What Is Quantum Computing?” 2018. CB Insights Research. 2018. https://www.cbinsights.com/research/report/quantum-computing/.