Project Paper: Quantum Computing's Impact on Cybersecurity

Old Dominion University

Elliott Pope Jr.

Introduction

Quantum computing represents one of the most game changing technological advancements of the 21st century. Unlike the computing that we are used to today, which relies on binary bits, quantum computing uses qubits that operate in superposition, which allows for unparalleled computational power. However, although these capabilities provide groundbreaking solutions for more complex problems, they also present many significant risks, mainly to current encryption standards. The arrival of quantum computers capable of running Shor's Algorithm threatens to break commonly used encryption methods like RSA and ECC, which leaves critical systems vulnerable. As adversaries prepare for a "harvest now, decrypt later" approach, it is important for organizations to transition toward post quantum cryptography (PQC) to protect sensitive data and maintain trust in digital communication. What I hope to achieve in this essay is to explore the impact of quantum computing on cybersecurity, focus on encryption vulnerabilities, emerging threats, and the need for quantum resistant cryptographic solutions.

Understanding Quantum Computing

The fundamental units of quantum computing are qubits. Qubits can exist in a state of superposition which gives them the ability of representing 0 and 1 at the same time with assigned probability. This makes them very different from classical bits, which only exist as strictly 1 or 0, and it gives qubits the capability to use this to increase computational capacity. Because of this, quantum computers can explore multiple solutions in parallel, which is important for problems that are extremely complex like integer factorization through Shor's Algorithm. (Rosa-Remedios & Caballero-Gil). Entanglement is another important part of quantum mechanics that allows the qubits to become linked. In the entangled state, the measurement of one qubit's state instantly determines the state of another, regardless of distance. This then forms the backbone of quantum

communication and computing, which supports a very efficient quantum gate, such as CNOT gate whose operation relies on entanglement. It is important to secure communication protocols like quantum key distribution because of entanglement's nonlocality and correlation properties (Einstein et al., 1935; Monroe, 2023; Rosa-Remedios & Caballero-Gil).

Shor's Algorithm, created by Peter Shor in 1994, represents a breakthrough in quantum computing because of its ability to efficiently factorize integers. Usual, or classical, algorithms like trial division and the general number field rely on steadily growing computer resources as the input size continues to increase. This makes them important for factoring large integers. On the other hand, Shor's Algorithm operates in polynomial time which solves this problem a lot faster. This efficiency is unique, and it threatens widely used public key encryption schemes like RSA and ECC that get their security from the infeasibility of integer factorization and discrete logarithms. This algorithm consists of two main phases, which are classical preprocessing and quantum computation. The application of this algorithm shows us the power of quantum mechanics when it comes to reducing computational complexity. For example, RSA encryption relies on the difficulty of factoring large numbers. If we were to use 2048 bits, it would take traditional computers millions of years to decrypt, while Shor's Algorithm could decrypt this in hours or days with a powerful enough quantum computer (Monroe, 2023). Now Grover's Algorithm, which was proposed by Lov Grover in 1996, increases the efficiency of searching through an unsorted database. As our current algorithms examine each item sequentially in a database, Grover's Algorithm takes advantage of quantum properties to speed up search processes. Even though it is not faster in an extreme amount, it does improve the performance of certain tasks by the computer. When it comes to cryptography, Grover's Algorithm presents a challenge to symmetric encryption systems like AES. It can test possible encryption keys in a

more effective and efficient way than classical methods by optimizing brute force attacks. Even though this alone does not fully compromise symmetric encryption, it does require an increase in key lengths to have the level of security stay somewhat the same. An example of this would be switching from AES-128 to AES-256 to help counteract advantages that come from Grover's Algorithm (Rosa-Remedios & Caballero-Gil; Monroe, 2023). The combined effects of these two algorithms show how significant the impact that quantum computing could possibly have on cybersecurity.

Even though quantum computing has great potential, it is still in an experimental phase being held back by multiple challenges. The limitations are either preventing or slowing down its ability to be applied to breaking encryption systems and other large-scale applications. These limitations include error rates and stability, scalability of qubits systems, timeline for CRQCs, hardware and resources, and algorithmic implication challenges. When it comes to the first limitation I mentioned, error rates and stability, quantum systems are extremely prone to errors caused by environmental noise and decoherence. This is when qubits lose their quantum state because of external factors. Aiming to keep qubits in their quantum state for long periods of time is a big hurdle in achieving fully functional quantum systems (CISA, NSA, NIST). In order to perform reliable computations, quantum computers need advanced error correction algorithms as well as fault tolerant architectures. Both of these necessities require an increase in the number of physical qubits. For now, there is no quantum computer that exists able to achieve large scale computations needed for exploitation of quantum algorithms like Shor's for cryptographic purposes (Monroe, 2023). The scalability of qubit systems is another difficult limitation to overcome, considering quantum computers need an increasing number of qubits to handle complicated computations effectively. Even though experimental systems have had

breakthroughs with over 70 qubits operating, building these systems that would be able to handle millions of error correcting qubits is still a long term goal. While experts do predict that quantum computers capable of breaking current encryption standards could appear within the next 10 to 30 years, this timeline is still up in the air, which makes it a limitation. This estimated timeline depends on the advancements to come within quantum technology, hardware development breakthroughs and error correction techniques. Because of how complicated these challenges are, the timeline is likely to vary which does leave a window for the development and installation of quantum resistant cryptography (CISA, NSA, NIST; Monroe, 2023). Current quantum computers need to be in special facilities and low temperatures to work properly, which creates a hardware and resource limitation. For example, superconducting qubits need cryogenic environments close to absolute zero. Algorithms like Shor's and Grover's Algorithm need a significant amount of resources and precision hardware to function properly, despite them being so theoretically sound (Monroe, 2023).

Current Encryption Standards

Asymmetric cryptography supports a lot of digital security today including several communication protocols, digital signatures, and authentication systems. RSA and ECC are some of the algorithms that make up the root of these systems. Their strengths come from common computers not being able to solve specific mathematical problems. However, these problems can be addressed with quantum algorithms, which would create a severe threat. RSA heavily relies on the difficulty of factoring the product of two prime numbers that are large. This encryption security succeeds off of exponential time needed by classic, or current, computers to perform this type of task as the number sizes increase. Though, with the future of quantum computing, Shor's Algorithm will completely change this landscape by allowing prime factorization to occur in

polynomial time, compromising RSA's foundational security principle making encrypted communicating vulnerable to being decrypted (Monroe, 2023). ECC provides stronger security than RSA for the same key length by leveraging the mathematics of elliptic curves. This security does depend on the difficulty of solving the discrete logarithm problem over elliptic curve groups, making quantum computers that require the use of algorithms like Shor's to be able to solve the equations that render ECC based cryptographic systems vulnerable. Because ECC is commonly used in the security of mobile devices and Internet of Things (IoT), being vulnerable to possible quantum attacks provides challenges for future proofing these systems (Monroe, 2023; CISA, NSA, NIST).

Symmetric cryptography, another important method for keeping digital information secure, relies on a single shared key for encryption and decryption. AES and other algorithms like it are known for being robust against both regular and quantum attacks. Because they are efficient and faster than asymmetric methods they are suitable for bulk data encryption. Although symmetric algorithms are not directly affected by Shor's Algorithm, Grover's is able to make the brute force attacks stronger by reducing the time that's needed to search any possible encryption keys. To minimize the impact that Grover's Algorithm can cause, security professionals are advocating for adapting longer key lengths and periodic updates to encryption standards, such as transitioning to AES-256 because it would ensure that encryptions would remain as strong as possible against quantum advancements for the foreseeable future (Rosa-Remedios & Caballero-Gil).

Hybrid encryption models incorporate the strengths of both symmetric and asymmetric cryptography systems in order to achieve efficiency and security in data transmission. Usually, asymmetric encryption algorithms are implemented during the beginning of a communication

session to maintain a secure key exchange. This approach uses the benefits of both models to its full potential with the direct threat of quantum computing on hybrid encryption methods being caused by it undermining the security of the asymmetric component (CISA, NSA, NIST).

The Quantum Threat

Taking a more detailed look at how Shor's Algorithm actually works, it uses quantum principles to find the periodicity of a function to help solve integer factorization and discrete logarithms. Leveraging quantum Fourier transforms allows it to identify number patterns that current computers can't do in an efficient way. This process starts by selecting random numbers and calculating their greatest common divisor with the target integer. If there is a nontrivial result, then that will reveal one of the factors, otherwise the algorithm will continue to find the period of the function using quantum computing leading to the factorization of the integer. Now, expanding upon the impact it has on RSA encryption, we need to understand that it relies on the difficulty of factoring the product of two large prime numbers. For example, RSA-2048 uses a 2048-bit key, which the computers that are made available to us today would take millions of years to factorize, while Shor's Algorithm can do this in a matter of days, or even hours, with the help of a powerful quantum computer. This would diminish the security of RSA, making encrypted communications vulnerable to the possibility of decryption. And with us understanding that RSA provides equivalent security with smaller key sizes, relying on the difficulty of solving discrete logarithms over elliptic curve groups gives Shor's Algorithm a good chance to efficiently solve these equations leading to the ability to compromise ECC based systems used in mobile devices, IoT security, and other resource constrained environments (Csenkey & Bindel, 2023).

The long term implication of this is that certain types of encrypted data, such as classified military communications or exclusive corporate research, might keep its value for decades. The "Harvest Now, Decrypt Later" strategy specifically targets this type of data, and banks on its value over time. For example, diplomatic cables or intelligence reports that are encrypted using RSA today have a chance to become accessible to attackers once quantum computers are able to break RSA encryption. Financial records, personal identification information, and medical data are also at risk because their value for being exploited remain high even after years of their initial collection. Risks created by this tactic not only threaten to affect individual datasets, but also critical infrastructure. Systems in the energy, transportation, and telecommunications sectors typically rely on encrypted communications to make sure operational security is in place. Any breach of these systems could lead to widespread disruption. To counter the risks associated with "Harvest Now, Decrypt Later," governments and organizations should have proactive cybersecurity measures like Transition to Post-Quantum Cryptography (PQC), Cryptographic Inventory, and International Collaboration, put into place. Developing these is important when it comes to keeping sensitive information protected before quantum computers are even able to make a breach. Early initiatives, like the ones led by NIST, are focused on finalizing PQC algorithms like CRYSTALS-Kyber and SPHINCS+. Organizations also need to keep an inventory of cryptographic systems, identifying vulnerabilities and prioritizing critical data sets. The threat of quantum computing will have effects on systems on a global scale, which is why cross border collaboration with governments, industries, and academic institutions is needed for developing solid security frameworks (Csenkey & Bindel, 2023).

The way that supply chains are so interconnected amplifies the risks. A delay in being ready against quantum attacks by partners like payment processors or logistics companies could

slow down efforts, and make the efforts of fully transitioned entities ineffective. Transitioning to PQC includes considerable costs, technical complications, and resource distribution. Smaller organizations, that likely lack the funding to upgrade cryptographic systems, are very vulnerable and big targets, exposing themselves and their partners to quantum enabled breaches. To add onto this, a lack of clear industry standards or coordinated timelines for PQC adoption fuels the problem, making it difficult to keep consistent implementation across all supply chain participants (Csenkey & Bindel, 2023).

The RAND Corporation's report, Securing Communications in the Quantum Computing Age, emphasizes the urgency of addressing the vulnerabilities in current encryption systems and highlights the steps necessary to mitigate the risks associated with these quantum cryptographic breaches. If quantum computers capable of breaking encryption become operational, the costs that come with data breaches, intellectual property theft, and financial fraud could increase dramatically. The banking, healthcare, and e-commerce industries are all vulnerable because they rely heavily on secure digital transactions. The transition to PQC is expected to involve significant costs, including upgrading hardware, rewriting software, and retraining personnel. These expenses could affect smaller organizations and developing nations, making quantum readiness uneven (RAND Report, 2020).

Redefining Cybersecurity Risks

The infrastructure sectors that quantum computing presents a significant risk to includes national security, financial systems, and healthcare. These sectors rely on encryption to ensure the confidentiality, integrity, and availability of sensitive data. The arrival of CRQCs capable of breaking current encryption standards could have terrible consequences. Encryption supports the

security of classified government communications, military operations, and intelligence activities. A breach by a quantum attack could expose sensitive information, disrupt defense strategies, and compromise national security systems. The U.S. National Security Agency (NSA) has warned that use of quantum computing by adversaries could be catastrophic for national security. The RAND Corporation highlights that the ability to decrypt encrypted communications would provide hostile actors with access to classified data, including military plans and diplomatic communications leading to espionage, sabotage, and the lack of trust between nations (Torkington, 2024). The financial section relies on encryption to secure transactions, protect customer data, and prevent fraud. As stated previously, quantum computing could make current encryption methods outdated and expose financial institutions to breaches, jeopardizing the integrity of payment systems, online banking, and financial markets. According to the World Economic Forum, the financial sector is extremely vulnerable because of its reliance on real time data processing and secure communication. Healthcare systems store a large amount of sensitive patient data, including medical histories, genetic information, and billing records. An attack would compromise this data, and lead to identity theft, insurance fraud, and the dwindling of patient privacy. Critical infrastructure such as energy and transportation, rely on encrypted communication for real time operations, meaning that a quantum enabled breach could disrupt these systems, leading to power outages, transportation delays, and other operational failures (Torkington, 2024; Rusu & Jurgens, 2024). The interconnected nature of critical infrastructure amplifies the risks, as a breach in one sector could have a domino effect leading into others, causing widespread disruption (Rusu & Jurgens, 2024).

Quantum Machine Learning (QML) represents an approach to transforming cybersecurity, combining the principles of quantum computing with machine learning techniques

to address sophisticated cyber threats. By leveraging quantum mechanics phenomena such as superposition and entanglement, QML algorithms can process large scale datasets and identify complex patterns more efficiently than more common methods. Although still in its early stages, QML holds great promise for proactive threat detection, anomaly classification, and phishing detection. By enabling the identification of cyber threats before they can grow, QML allows organizations to implement preventive measures. They can analyze network traffic data to detect things that indicate potential cyberattacks such as Distributed Denial of Service (DDoS) attacks or unauthorized access attempts. Even though it has great potential, it is still in its "infancy" and faces the challenges of hardware limitations, noise sensitivity, and the need for specialized datasets. How it is currently implemented makes it often rely on simulations rather than actual quantum hardware, which clearly limits their scalability and how they apply to the real world (Rosa-Remedios & Caballero-Gil).

As quantum computing continues to advance, governments and organizations are facing an urgent need to adapt their cryptographic policies and infrastructure to remain strong against upcoming threats. The ability to smoothly replace and adapt cryptographic algorithms without disrupting systems, otherwise known as cryptographic agility, is a cornerstone of this effort. This approach makes sure that organizations can respond effectively to vulnerabilities in existing standards and prepare for the transition to PQC. Cryptographic agility allows organizations to replace outdated algorithms with minimal disruption to operations, which is critical in an environment where new vulnerabilities and quantum advancements can cause existing encryption to become nonexistent or very weak. The transition from SHA-1 to SHA-2 in public key certificates is a great example, as it demonstrates the importance of agility in responding to cryptographic weaknesses. In a similar way, preparing for quantum threats requires systems to be

flexible enough to integrate PQC algorithms seamlessly. Governments play a pivotal role in driving cryptographic agility as agencies like NIST have had an important part to play when it comes to developing PQC standards and providing guidance on such transitions. The U.S. National Security Memorandum 10 is a national security policy that emphasizes the need for cryptographic inventories and migration plans to safeguard critical infrastructure and sensitive data, encouraging organizations to assess their reliance on vulnerable cryptographic systems and prioritize their transition efforts (Monroe, 2023; CISA, NSA, NIST).

Transition to Quantum-Resistant Cryptography

The NIST has been at the forefront of developing PQC standards to tackle the vulnerabilities presented by quantum computing. After years of evaluation and collaboration with cryptography experts worldwide, NIST has identified algorithms that are designed to withstand quantum enabled attacks. (CISA, NSA, NIST; Monroe, 2023)

- **CRYSTALS-Kyber**: A lattice based key encapsulation mechanism (KEM) designed for secure key exchange. It is highly efficient and scalable, making it suitable for a wide range of applications, including secure communications and cloud computing. (Monroe, 2023; CISA, NSA, NIST)
- **CRYSTALS-Dilithium**: A lattice based digital signature algorithm known for its simplicity and strong security guarantees. It is optimized for performance and is resistant to quantum attacks, making it ideal for authentication and integrity verification. (Monroe, 2023; CISA, NSA, NIST)
- **SPHINCS+**: A hash based digital signature algorithm that provides strong security without relying on structured mathematical problems. Its stateless design ensures

resilience against quantum attacks, making it suitable for applications requiring long-term security. (Monroe, 2023; CISA, NSA, NIST)

- **FALCON**: Another lattice-based digital signature algorithm, FALCON is recognized for its compact signatures and efficient verification processes. It is particularly useful for resource-constrained environments, such as IoT devices. (Monroe, 2023; CISA, NSA, NIST)

NIST's selection process involved a competition lasting multiple years beginning in 2016, where cryptographers were submitting and evaluating algorithms based on their security, efficiency, and practicality. The goal was to find algorithms that are capable of resisting quantum attacks while also meeting the needs of modern cryptographic systems. The evaluation had considered the factors of computational efficiency, the complexity of it being implemented, and resilience against both common and quantum attacks. The algorithms that were selected are designed to replace methods like RSA and ECC in applications that range from secure email and online banking to critical infrastructure protection (Monroe, 2023; CISA, NSA, NIST).

Transitioning to PQC requires updates to hardware, software, and protocols, as organizations need to conduct cryptographic inventories to find systems that rely on vulnerable algorithms and prioritize their efforts. Collaboration of vendors and industry leaders is necessary to ensure the seamless integration of PQC algorithms into existing systems, as this transition has some pretty significant challenges for organizations and governments (CISA, NSA, NIST; Monroe, 2023). From hardware and software to supply chain coordination, the adoption process is covered with many complexities (CISA, NSA, NIST; Rosa-Remedios & Caballero-Gil). The supply chain for such systems is very complex and involves hardware manufacturers, software providers, cloud services, and end user organizations. Having an effective transition to PQC

means having the proper coordination across all stakeholders to avoid any vulnerabilities. A single lagging entity or setback can compromise the security of the entire ecosystem. The costs that come with transitioning are very high due to the hardware replacements, software upgrades, workforce training, and third party consulting, so for many organizations these expenses are accompanied by competing priorities like everyday operation costs and other investments. Specialized expertise, including knowledge of quantum resistant algorithms and their integration into existing systems is also needed, and ties into the already extensive list as to how complicated such a transition will be, with the current shortage of professionals trained in post-quantum cryptography adding another layer of complexity to the adoption process (CISA, NSA, NIST). Training programs and workforce development initiatives are necessary to equip professionals with the skills required to manage PQC implementations effectively (Rosa-Remedios & Caballero-Gil).

Conclusion

In conclusion, as quantum computing approaches practical application, the time for action is now. This evolving threat needs immediate and proactive measures to safeguard sensitive data and critical systems. Organizations need to prioritize conducting cryptographic inventories to assess vulnerabilities and identify systems that rely on outdated encryption methods. At the same time, global collaborations across governments and industries are essential to speed up the adoption of PQC solutions. QML is poised to offer great solutions for anomaly detection, pattern recognition, and predicting threats. However, maximizing its potential needs continued research to refine algorithms and adapt them to real world situations. The transition to quantum resilience hangs on global collaboration. Governments, industries, and academic institutions need to work together to establish scalable PQC frameworks that address technical,

financial, and logistical challenges. By embracing innovation and implementing action, we can keep the digital world safe against the challenges of the upcoming quantum era.

Works Cited

- Csenkey, T., & Bindel, R. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. Journal of Cybersecurity Studies
- Monroe, D. (2023). Post-Quantum Cryptography Cryptographers seek algorithms quantum computers cannot break. Cybersecurity Journal
- Rosa-Remedios, C., & Caballero-Gil, P. (2024). Optimizing quantum machine learning for proactive cybersecurity. Optimization and Engineering. Springer.
- World Economic Forum. (2024). Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding. https://www.weforum.org/stories/2024/04/quantum-computing-cybersecurity-risks/
- Rand Report (2023). When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret. https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html
- Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? Physical Review,
- CISA, NSA, & NIST. Post-quantum cryptography standards and transition strategies. https://csrc.nist.gov/projects/post-quantum-cryptography
- NIST. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

- CISA, NSA, & NIST. QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.

.