Exploring Quantum Computing Threats to Cybersecurity

Nicholas Dionne
Cybersecurity, Assumption University, Worcester, MA, United States

Abstract **-** Quantum computing holds the promise of improvements to research and development, supply-chain optimization, production, and advances in artificial intelligence and other fields. The vastly increased processing capabilities of quantum computers also exacerbates risks and poses new threats. This paper explores the threat of quantum computing in cybersecurity, especially cryptography. It briefly covers the importance of cryptography through a historical lens and then explores the contemporary challenges that newly emerging quantum computing technologies pose. By exploring the inherent vulnerabilities of traditional cryptographic systems, one can better understand the threat posed by quantum computing algorithms such as Shor's and Grover's algorithms. Moreover, these developments accentuate the need for standardization of post-quantum cryptographic techniques that resist these increasing technological advancements. Finally, anticipated and new developments in quantum computing are considered to further inform evolving approaches to ensuring cybersecurity.

Keywords: Quantum, Computing, Algorithm, Cryptography, Standard, Qubit.

1 Introduction

Cybersecurity has become an increasingly critical aspect of today's modern society as our reliance on digital technologies continues to grow. A vital part of cybersecurity is the field of cryptography, which plays a critical role in protecting sensitive information from unauthorized access. With the emergence of quantum computing, the cybersecurity field as a whole must evolve to match the heavy impact this technology will have on the world. This heavy impact can be seen in quantum computing's potential to render today's traditional cryptographic systems obsolete, posing a highly complex and challenging problem for researchers and cybersecurity professionals to solve.

This paper aims to explore the implications of quantum computing on cryptography within the cybersecurity field. In examining the evolution of cryptography in response to this new emerging threat and the vulnerabilities of traditional cryptographic systems, this paper seeks to show a glimpse of the future of cybersecurity in the post-quantum era. Furthermore, in an attempt to deliver on its promise, this paper will discuss some post-quantum cryptography and countermeasures to mitigate this rising threat.

2 Cryptographies Evolution Due to Threats

2.1 Historical Overview

Cryptography has roots from ancient civilizations, where the first rudimentary encryption methods were created to protect sensitive information, much like today [1]. One of the first known examples of cryptographic techniques is the Caesar cipher, created by shifting each letter of the alphabet by a fixed number of positions [1]. After an extended period, civilization evolved, and so did technology. As such, better cryptographic techniques were sought for more secure methods of communication [1]. During World War II, the Enigma machine was considered indecipherable due to the Axis Powers' new leap in technology, and this allowed them to secure their communications and win many conflicts, showing for perhaps the first time in history on the world stage, how integral a role cryptography plays in warfare and securing information [1]. That was until the Allied Powers broke the enigma machines' code using superior technology, successfully compromising The Axis Powers' communications [1]. Lastly, the advent of computers in the 20th century led to the development of exceptional encryption algorithms such as the Data Encryption Standard (DES), which led to the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), which are still used widely to this day [1].

2.2 Tech Advancements in Cryptography

Advancements in technology have continuously shaped cryptography, especially in terms of encryption techniques. The rise in computing power has enabled more sophisticated cryptographic algorithms, such as symmetric and asymmetric encryption methods, which are the foundation of traditional cryptography. However, quantum computing poses a significant threat to traditional cryptography. Quantum computers leverage the principles of quantum mechanics to perform computations at a never-before-seen rate compared to classical computers, and this has the potential to render many traditional cryptographic techniques vulnerable. This technological shift uncovers a vital need for a new approach to cryptographic techniques, an approach with the capability to withstand the computational power of quantum computers and the unique principles of quantum mechanics. This vital need for a new approach to cryptography with the advent of quantum computing cannot

be handled by an individual but by an organization such as NIST.

2.3 Importance of Standards (NIST)

The National Institute of Standards and Technology (NIST) is the federal agency of the United States tasked with the development and promotion of measurements, standards, and technology [8]. NIST's involvement in setting standards for cryptographic systems dates back to the early 1970s with the Data Encryption Standard (DES), which was created under the relatively new idea that digital communications and transactions should be secured in an insecure internet [8]. NIST sets standards by first identifying a problem in current cryptographic standards; this could be initiated due to new technology or research developments that have resulted in a need for a new cryptographic standard [8]. Then, once an issue is determined, NIST has researchers map out the specifics of what the new standard aims to achieve [8]. This then allows NIST to issue a public notice for cryptographic algorithm submissions that meet the specifics of the new standards outline [8]. NIST then strictly evaluates the received submissions, testing them for their practicality, efficiency, and security; this process can go on for several rounds, each lasting years at a time, and be passed through many experts during the process [8]. NIST then proposes the new standard and gets public feedback for review, which allows NIST to proceed with revisions and formalization of the standard [8]. The process for the development and implementation of standards is involved and can take years; a current example of this process is NIST's Post-Quantum Cryptography Standardization Project (PQC), which was initiated in 2016 [9]. The total number of submissions back in 2016 of NIST's PQC can be seen by type in Table 1 below [13].

Table 1

	Signatures	KEM/Encryption	Total
Lattice-based	4	24	28
Code-based	5	19	24
Multivariate	7	6	13
Hash-based	4	–	4
Other	3	10	13
Total	23	59	82

NIST's PQC is well underway; it has finalized its third round and is initializing its fourth round of selection with four new algorithms [10]. Overall, NIST has so far selected four candidates for PQC standardization since the finalization of the third round, and they are as follows: CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, and SPHINCS$^+$ [10].

3 Cryptographic Vulnerabilities

3.1 Overview of Symmetric and Asymmetric Cryptography

Traditional Cryptography, widely used today, relies heavily on symmetric and asymmetric encryption algorithms to secure data. Symmetric encryption uses a single key for encryption and decryption, making it efficient but vulnerable regarding the distribution of keys [13]. On the other hand, asymmetric encryption uses a pair of keys, public and private, thus allowing for secure communications without a pre-shared key like in symmetric encryption; however, asymmetric encryption is computationally demanding for key generation and encryption [13].

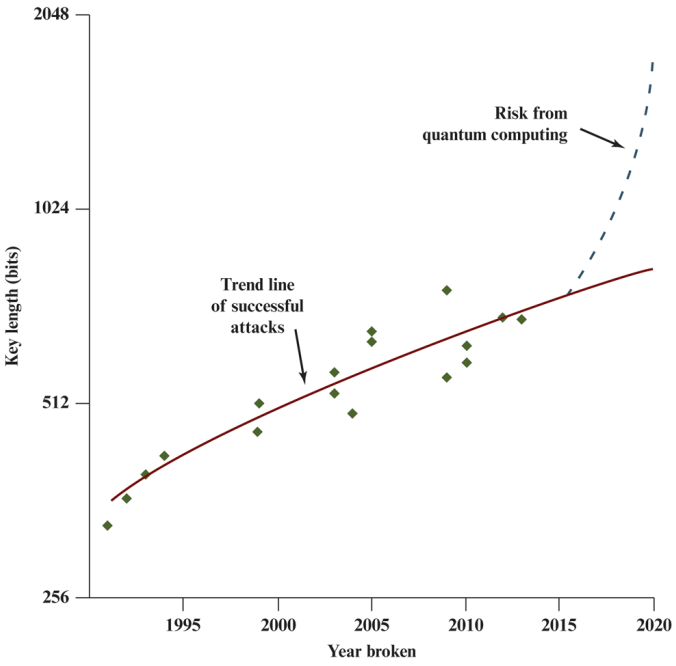
3.2 Vulnerabilities of Traditional Cryptography

Other than the issue of key distribution, traditional cryptographic systems are susceptible in various ways, including brute-force attacks, mathematical weaknesses, and flaws in implementation. Brute-force attacks, as inefficient as they might be due to systemically trying all possible keys until the correct key is found, are all too viable nonetheless, even after countering this method by lengthening keys and increasing algorithm complexity. A Mathematical weakness can be found in the factorization problem of RSA, which poses a threat to asymmetric encryption, especially when quantum computing is involved [13]. The factorization problem involves decomposing large composite numbers into their prime factors, and RSA relies on the assumption that factoring these large composite numbers into their prime factors is computationally difficult or when large enough a number, it becomes infeasible, and this is the basis of RSA's security [13].

3.3 Are Current Encryption Standards Susceptible to Quantum Attacks

There are many traditional encryption standards, such as Elliptic Curve Cryptography (ECC) and RSA, that rely on mathematical problems that are believed to be too computationally demanding for classical computers to solve efficiently [13]. First, let's take a quick look at the ability of classical computers when it comes to breaking RSA. Generally, this is a rather tricky question that depends on the algorithm used and the computational power available, like with the general number field sieve, an exceptional algorithm that's been utilized to break RSA at smaller key lengths; the solution for these compromises in security where to simply increase the required key length at regular intervals in time thus sustaining a certain level security [13][15]. However, looking at the graph below from [13], which

Figure 1



contrary to what many may believe, Figure 1 shows that these cryptographic techniques are, in fact, vulnerable at this very moment, and this is why we have standards that require security to be at a certain level [13]. Standards change quite often when technology changes; in fact, NIST now recommends 2048 bit length as the minimum requirement for RSA and has suggested that the appropriate bodies utilize 3072 bit length by the year 2030 [15]. But as can be seen in Figure 1, those security standards and RSA itself won't be able to keep up with quantum computing and, therefore quantum attacks, particularly by algorithms such as Shor's algorithm, which can efficiently factor large integers [13]. Moreover, as quantum computing technology improves, the feasibility of executing an attack increases drastically and requires the cybersecurity field to focus on the development and adoption of post-quantum cryptographic standards.

4 Quantum Computing as a Threat

4.1 Quantum Computing Fundamentals

For the sake of the author and this paper's readers, this discussion of the fundamental concepts of quantum computing will strive to minimize the use of any intensive mathematical concepts. Quantum computing is built upon its ability to leverage quantum mechanics, and it does so by using specialized technology and computer hardware in an attempt to solve complex problems that classical computers find infeasible. Quantum computing works through quantum bits known as qubits, unlike classical computers, which use bits in the fixed form of 1 or 0; qubits can exist in a state known as superposition, which allows each qubit to simultaneously be in an undetermined state of a 1 and or 0 [11]. Moreover, there are other concepts or states in quantum mechanics that can be applied to qubits as well, such as entanglement qubits can be entangled; this implies that the state of one qubit (A) is dependent on that of another qubit (B) and vice versa [11]. For example, if qubit (B) is measured or observed to be 1, then it can be determined that qubit (A) is also 1, and if qubit (A) is measured or observed to be 0, It can be determined that qubit (B) is also 0 [11]. Quantum measurement, or what has been on occasion called observation within this paper, is determined by a mathematical function called the wavefunction; this function encapsulates every state of a qubit by superposition and finds the probability of each state. Upon measurement of a qubit, the wavefunction is likely to collapse into the most probable state of the qubit 1 or 0 [11][20]. Lastly, Integral to quantum computing is the concept of gates; much as with classical computers and how logic gates manipulate bits to perform logical operations like AND and OR, quantum computers have quantum gates that manipulate qubits to perform quantum operations such as the states of superposition and entanglement [11].

4.2 Shor's Algorithm and Its Implications

Shor's algorithm was first proposed by Peter Shor in 1994 as an algorithm for quantum computers that efficiently factors large integers into their prime components [12]. Shor's algorithm operates through two main steps: period finding and prime factorization [12]. In this section of the paper, these two parts of Shor's algorithm will be briefly explained, along with their implications.

Period finding is the first step in Shor's algorithm; a vital aspect of this step is Quantum Fourier Transformation (QFT), an implementation of Discrete Fourier Transform, and that is because, without QFT, we couldn't aim to measure any specific value computed. So imagine as follows: a random number (K) is chosen for our input value (N) such that K < N, and then the two numbers are checked for a common factor; if, say, K and N do not have a common factor, then the algorithm computes k^x mod N for varying x values from 0 to N-1 which creates a periodic sequence [12]. QFT is then utilized to efficiently and quickly locate the period (r) in the periodic sequence; r is critical here, as finding it quickly is what classical computers have a hard time doing [12]. QFT is the unique aspect of Shor's algorithm, where Shor readily utilizes the abilities of quantum computing to surpass classical algorithms in quickly factoring large composite numbers into their prime factors [12].

Prime Factorization is the second step in Shor's algorithm; this step doesn't have any particularly unique aspect that utilizes quantum computing; however, it makes excellent use of the first step's result and quickly finds the prime factors of N by utilizing r to it's fullest by finding the greatest common divisor (gcd) once the gcd is located and it equals neither 1 or N it means we have p, and so if N is divided by p, the result is q (N/p = q) which means p and q have been located such that p times q equals N (p*q = N) [12]. Shor's algorithm may lose out to classical computers when factoring small or moderate sized numbers, but when it comes to truly large numbers like that of the modulus (N), which is the product of large prime numbers p and q in RSA, Shor's algorithm has the best ability to efficiently and quickly factor such a large number.

The implications are clear: Shor's algorithm has the capability to find the period r much faster than any classical computer has the potential to and, therefore, greatly surpasses their ability to find N [16]. So much so, in fact, that it puts one of the most used asymmetric cryptographic techniques entirely at risk of exploitation-as its main ability as a cryptographic tool is to obfuscate information by processing it in a way that breaking the encryption becomes so computationally demanding that classical computers cannot break its encryption within a feasible time frame [16]. However, if there's one thing quantum computers have in abundance, it's computational power, and that, along with the unique traits of quantum computing, allow it to break RSA using Shor's algorithm, as stated in this research paper on breaking RSA using Shor's algorithm [16]. "Thus, it makes it clear that a practically powerful quantum computer can break any length of RSA encryption in a feasible amount of time, even the best-known classical theories to factorize numbers are exponentially less powerful when we compare them with the time complexities of algorithms like Shor's Algo-rithm." [16]. Now, does this mean RSA will be falling apart as quickly as tomorrow? Not quite, as most companies pursuing quantum computing are still in the early stages and have yet to come close to creating a quantum computer with enough qubits to reliably utilize a demanding algorithm like Shor's algorithm [16].

4.3 Grover's Algorithm and Its Implications

Grover's algorithm was first proposed by Lov Grover in 1996; it's a quantum search algorithm built to search unsorted databases. Grover's algorithm operates through three main steps: initial state, diffusion, and measurement [20]. A classical computer, when searching for a particular N record in a database, typically needs to view a large portion or all of the N records to identify the particular N record, and this is true for a classical computer [20]. However, a quantum computer equipped with Grover's algorithm can search for the N record in a fraction of the time due to its unique properties; the following is a brief explanation of the three main steps up to the end result of Grover's algorithm followed by its implications [20].

The Initial state is that of superposition of each N record in the database [20]. This allows for a quantum computer to simultaneously search every N record in the system at once [20]. Then, a particular N record is marked to be found, and so the algorithm utilizes diffusion to amplify the probability that during the search, the algorithm will find the marked N record, and it does so by also reducing the amplification and or probability of searching any non-marked N record [20]. Finally, Grover's algorithm proceeds to the final step measurement in which the superposition state in which all N records are encapsulated at once is then collapsed into the determined or measured state of the highest probability or amplitude, and the state with the highest probability is undoubtedly the marked N record due to the previous steps, and this leads to a massive difference in the length of time required for a search of a particular N record in a database [20].

This implies Grover's algorithm is currently one of the only quantum algorithms with a real potential to compromise symmetric cryptography [17]. The idea is that by utilizing Grover's algorithm, which is a quantum search algorithm, symmetric cryptography standards such as Advanced Encryption Standard (AES) can be targeted, as stated in the following paper on how Grover's algorithm is a threat to modern cryptography "Thus, a direct application of the algorithm is searching for symmetric keys in key spaces, which are essentially unstructured databases. Since AES is pretty much vulnerable to brute-force attacks only, this is precisely how Grover's algorithm threatens it." [17]. Grover's algorithm's ability to search is an extraordinary tool that could even have the potential to compromise AES, but although it's already being tested, the scale is small, and the results even smaller as, again, quantum computers aren't at a threshold of having enough qubits to manage algorithms such as Grover's or Shor's [17].

5 Post-Quantum Countermeasures

5.1 Overview of Post-Quantum Cryptographic Algorithms

Suppose quantum computing is such an impactful technological development that quantum algorithms utilizing their potential can target and easily dismantle some of society's most critical cryptographic techniques with ease; what's the next step to protecting our systems and information? Luckily, organizations like NIST exist specifically for situations such as this, and with their PQC project well underway and the many submissions receiving rigorous testing, it can be seen that a significant effort is being made to develop and standardize quantum-resistant cryptographic techniques in time for a post-quantum world. So far, NIST's progress toward standardization of post-quantum resistant techniques has been slow but methodical, and there have been four selected candidates for PQC standardization as previously mentioned in section 2.3; these four candidates include one KEM/Encryption algorithm known as CRYSTALS-KYBER (Lattice-based) and three digital signatures known as CRYSTALS-Dilithium (Lattice-based), FALCON (Lattice-based), and SPHINCS$^+$ (Hash-based) [10].

5.2 Evaluation of Current Post-Quantum Cryptography Standards

The most promising type of post-quantum technique is Lattice-based, which received the most submissions to NIST's PQC (refer to Table 1 in section 2.3) [13]. Lattice-based cryptography: what is it? In short, Lattice-based cryptography is a set of "hard questions around spaces formed by combining sets of vectors to form new vectors. All the new vectors you can form by these combinations are called a lattice." these lattices are usually represented as vectors in a 2D or 3D space [18]. Alright, now that we know generally what a lattice is, how does it help in creating post-quantum cryptographic techniques? Think this over for a second: cryptographic techniques are typically made of mathematical problems with difficult-to-solve aspects, just as RSA uses the

difficulty of factoring really large integers to stay secure. Ultimately, lattice-based cryptography does the same, and there are a few of these difficult problems that can be utilized; first and foremost, it's really difficult to find a vector that's closest to a given vector in a lattice, to find the shortest vector in a lattice, or to find a lattice with the shortest possible vectors [18]. All three of these problems "have been rigorously proved to be equivalent (solving any one of them solves the others). While there have been proposed cryptographic systems that use these problems directly, most proposals use other problems and try to show that these other problems are equivalent to one of these three problems." [18]. One of these other problems is Module Learning with errors (MLWE), and it is used to secure the CRYSTAL-KYBERS key encapsulation mechanism by adding small errors to linear equations in the encryption process which deviates the result drastically, meaning that any attempt made to break CRYSTAL-KYBERS involves finding all the unknown small errors [18]. Many lattice-based post-quantum cryptographies involve MLWE, not just CRYSTAL-KYBERS, but also CRYSTAL-Dilithium [18].

Hash-based post-quantum techniques are easier to understand; the idea is to utilize the fact that hash functions are one-way functions and that any input is irreversibly changed in a way that is difficult for even quantum computers to find the original input [19]. Moreover, the structure of a hash function would necessitate that an attacker tries every single possible input to find a match, which, simply put, is not a reliable method [19]. Hash-based is used by digital signatures like SPHINCS$^+$ for these very reasons, and one of the reasons it was selected by NIST is that it utilizes another approach from the other lattice-based cryptographies while also optimizing its utility through being a stateless hash-based signature, which allows for easier implementation and enhanced security by reducing the human capacity for mistakes in deployment [19].

5.3 Implementation Challenges and Considerations

Now, even with all this good news that we have viable options in regard to protecting our systems from quantum computing. There stands to be some implementation challenges and considerations. Firstly, it cannot be stressed enough that even with the analytical ability of NIST and its experts, these new cryptographic techniques that are meant to be quantum resistant, especially the lattice-based, although promising, are essentially the first of their kind, and due to this fact there are still many opportunities for substantial attacks that shave down the security of these approaches to be discovered [18]. Hash-based has been long standing and therefore more thoroughly tested overall and so suffers less than lattice-based approaches with regards to having its security features shaved down; however, the only post-quantum hash-based cryptographic techniques available as of now are stateful and require tricky implementations due to deployment issues that are now solved with the standardization of SPHINCS$^+$ a stateless digital signature. However, this digital signature comes with some of its own problems like a ridiculously large digital signature, in fact, it's anywhere between 8KB and 49KB compared to CRYSTAL-Dilithium which generates a signature of about 4KB in size for similar security [18][19].

6 Future Directions

6.1 Anticipated Developments

There's a lot happening in cybersecurity as a whole at just about any time, and quantum computing is arguably at the forefront of research right now, so in this section, we'll take a short look into some recent or future developments in quantum computing. An interesting blog was written by the Apple Security Engineering and Architecture team (SEAR) in February of 2024, where they announced an update to the cryptography used to secure iMessage, which will now be called PQ3 [21]. PQ3 utilizes Apple's previous use of ECC for securing messages, but since this classical approach to securing messages is only effective against classical computers, as we could see in sections 4.2 and 3.3 that show how algorithms such as Shor's are particularly effective against the mathematical problems ECC and RSA utilize to remain secure [21]. In short, Apple is aiming to make use of NIST's third round candidate for PQC standardization, a KEM called CRYSTAL-KYBERS, which has a lattice-based approach to cryptography, to protect against a new kind of attack called harvest now, decrypt later where attackers harvest large amounts of encrypted data today and decrypt this data in the future when quantum computers with that capability become available [21].

Other future developments can be viewed through the lens of Google or IBM's quantum computing roadmaps. IBM's quantum computing timeline shows us that consistent developments in quantum computing are being made; in fact, they have the anticipated research developments mapped out from 2024 to 2033+, showing milestone achievements in reaching an error-corrected quantum computer [22][23]. However, IBM focuses more on the hardware and software of quantum computers, where they're constantly attempting to raise the overall number of available qubits [22]. Google, on the other hand, truly focuses on error correction in hopes of making advancements to creating a truly useful quantum computer in the next decade, according to their quantum roadmap [23]. The reason error correction in quantum computers is so anticipated to the point that quantum computers are only considered useful after the fact is that quantum computers suffer from quantum noise when attempting complex computations, which causes the results of those computations to have errors, making the calculations of quantum computers unreliable [23]. This impart is what allows our classic cryptographic techniques to still operate as intended as no one's achieved an error corrected quantum computer yet [23]. However, the status quo will most definitely change with time now that large corporations and governments are pursuing this technology with avarice, and it won't just change cybersecurity forever-it will bring advancements and answers to some of humanity's most pressing questions.

6.2 Areas for Further Research

Previously in section 6.2, I claimed quantum computing to be at the forefront of research in cybersecurity at this time, but what might be at the forefront of research and everyone's minds, even more so, is Artificial Intelligence (AI); however, here's an idea to mull over: what's the culmination of these two critical emerging fields of technology? The answer is quantum AI. Now, what is quantum AI? Well, that's a good question with currently very limited answers. Well, according to IBM, "Quantum artificial intelligence (QAI) is an emerging field of computer science that applies the transformative power of quantum computing to the research and development of improved artificial intelligence products, such as machine learning algorithms, neural networks and large language models (LLM)." [24]. QAI is an important step in the advancement of AI, particularly as with the new advent of AI into the mainstream, models and classical hardware have been pushed to their upper limits in an attempt to get AI to its full potential [24]. However, it seems that as research progresses that, classical computers and the models they can sustain won't quite be up to the task and so with the new breakthroughs in quantum computing allowing for more consistent research in this department, attention has been turned to the potential of quantum AI [24]. In fact, expectations are high enough for companies like IBM to state the following "AI systems could unlock new frontiers in computing power, algorithm efficiency and general problem-solving capabilities. Despite their complexities, QAI may prove to be critical in overcoming humanity's most challenging obstacles." [24].

This new frontier has the potential to upturn everything, and that's exciting as it can potentially help train LLMs and the like in highly specialized fields in a fraction of the time it takes us today but with much more data [24]. This impact is impressive, and with what's being seen today with the integration of AI in just about every system imaginable, it can stand to reason that with QAI, we'll only be seeing more and more AI in our daily lives [24]. However, QAI is likely far from reach for now as quantum computing and AI have only recently left their infancy, and although both fields have seen a tremendous increase in funding, research, and tangible advancements, this is especially true for AI [24]. It's simply not feasible to expect results from this new field anytime soon and certainly not anything substantial until issues in quantum computing, such as error correction, have been dealt with to allow for practical quantum computing, as mentioned in section 6.1 [24]. Finally, consider all of* the aforementioned factors in addition to the increasingly rapid development of AI models which will likely have to be specially adapted to the quantum computing landscape [24].

7 Conclusion

7.1 Summary and Insights

Throughout this paper, the importance of cryptography and it's standardization has been detailed largely to express the impact quantum computing will have on the cybersecurity landscape. The unique aspects of quantum mechanics that are leveraged in quantum computing allow for algorithms such as Shor's and Grover's to exponentially increase the potential impact of quantum computing by breaking the foundational components of important traditional cryptographic algorithms such as RSA and AES. However, organizations such as NIST are putting forward their best research capabilities in the involved process of standardization with the PQC project to mitigate the incoming impact of this new technological development. NIST's PQC has approved four new algorithms for standardization, favoring a lattice-based solution over others in hopes of computationally challenging both quantum and classical computers. The hope is that with the adoption of these new standards, the upcoming technological disaster will be mitigated. Allowing researchers to further develop concepts utilizing quantum computing for the betterment of society such as QAI. QAI, from what little is known, has the potential to develop data and train LLMs much faster than we can today, allowing for untold potential.

7.2 Implications for Future of Cybersecurity

The implications for cybersecurity include a rocky future for new professionals in the field. However, there's still time to prepare, and that's exactly what organizations like NIST will continue to do till the last moment, ensuring that organizations adopt the appropriate quantum-resistant standards throughout the next decade. While companies like Google and IBM continue to pursue quantum error correction and to increase the number of available qubits to be able to reliably operate quantum algorithms such as Shor's and Grover's and even QAI. Moreover, Apple has already begun the process of adopting quantum-resistant algorithms into their systems by introducing a development of CRYSTAL-KYBERS from NIST PQC standardization to their IMessage encryption. In conclusion, the situation is volatile but not unsalvageable as time is still available to implement, test, and develop the most capable of our quantum-resistant algorithms to mitigate the impact of quantum computing.*

8 References

[1] William August Kotas. "A Brief History of Cryptography". University of Tennessee – Knoxville, 2000.

[2] Joseph, D., Misoczki R., Manzano M., et al. "Transitioning organizations to post-quantum cryptography". Nature, 2022.

[3] Bernstein D., Lange T. "Post-quantum cryptography". Nature, 2017.

[4] W. Diffie, M. E. Hellman. "New Directions in Cryptography". IEEE Transactions on Information Theory, vol. IT-22, no. 6, 1976.

[5] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, vol. 21, no. 2, 1978.

[6] A. Kak. "Lecture 12: Public-Key Cryptography and the RSA algorithm". Purdue University, 2024.

[7] M. Calderbank. "The RSA Cryptosystem: History, algorithm, Primes". 2007.

[8] “Cryptographic Standards and Guidelines Development Process”. NIST, 2016.
[9] “Post-Quantum Cryptography”. NIST, 2017.
[10] “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process”. NIST, 2022.
[11] Giacomo Nannicini. “An Introduction to Quantum Computing, Without the Physics”. IBM, 2020.
[12] Peter W. Shor. “Polynomial-Time algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. arxiv, 1996.
[13] William Stallings. “Cryptography and Network Security: Principles and Practice, 8e”. Pearson, 2019.
[14] Craig Gidney, Martin Ekerå. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”. arxiv, 2021.
[15] Elaine Barker, Allen Roginsky. “Transitioning the Use of Cryptographic algorithms and Key Lengths”. NIST, 2019.
[16] Siyon Singh, Eric Sakk. “Implementation and Analysis of Shor's algorithm to Break RSA Cryptosystem Security”. ResearchGate, 2024.
[17] Mina-Zicu, M., Simion, E. “Threats to Modern Cryptography: Grover’s algorithm”. Preprints, 2020.
[18] Robert Relyea. “Post-quantum cryptography - lattice-based cryptography”. RedHat, 2023.
[19] Robert Relyea. “Post-quantum cryptography: Hash-based signatures”. RedHat, 2022.
[20] Lov K. Grover. “A fast quantum mechanical algorithm for database search” Association for Computing Machinery, 1996.
[21] Apple Security Engineering and Architecture (SEAR). “Blog - iMessage with PQ3: The new state of the art in quantum-secure messaging at scale”. Apple Security Research, 2024.
[22] “IBM Quantum Computing: Technology”. www.ibm.com/quantum/technology. IBM, Accessed 2024.
[23] “Our Quantum Computing Journey”. quantumai.google/learn/map. Google Quantum AI, Accessed 2024.
[24] Josh Schneider, Ian Smalley. “What is quantum AI?”. IBM, 2024.
[25] “Shor's algorithm”. Wikipedia, Accessed 2024.
[26] “Shor’s Factorization algorithm”. www.geeksforgeeks.org/shors-factorization-algorithm/. GeeksforGeeks, Accessed 2024.
[27] “Introduction to Grover’s algorithm”. www.geeksforgeeks.org/introduction-to-grovers-algorithm/. GeeksforGeeks, Accessed 2024.
[28] “Grover's algorithm”. Wikipedia, Accessed 2024.
[29] “What is Quantum Computing?”. https://www.ibm.com/topics/quantum-computing. IBM, Accessed 2024.
[30] Matt Swayne. “NIST Releases Four PQC algorithms For Standardization”. https://thequantuminsider.com/2023/08/24/nist-releases-four-pqc-algorithms-for-standardization/. The Quantum Insider, 2023.
[31] “NIST Announces First Four Quantum-Resistant Cryptographic algorithms”. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. NIST, 2022.

Note:

References [2] - [7] haven’t really been used much but I’m keeping all relevant links for info and papers here for now.

References [25] - [31] are most of my most utilized sources for helping me break down and better understand some of the papers I used.

(I'm not sure what to do with these because they are mostly secondary unofficial sources that aren’t papers or anything, and the primary source I used was still the papers themselves. But I’ll cite them anyway just in case…)