California State Polytechnic University, Pomona

Quantum Apocalypse: The Death of Traditional Encryption

CS 2610

Danica Cariaga

Noah Loke and Other Members

Cryptography is a science and field of study that involves the practice of securing and authenticating people, data, and other objects that may be passed between authorized parties. This typically entails data encryption and the implementation of algorithms that protect the confidentiality, integrity, and availability of data and prevents repudiation. It's a cornerstone of cybersecurity and it's how computers and digital identities are protected from malicious manipulation by outside actors. In order to protect individual privacy, cyber security specialists rely heavily on cryptography to encrypt data. However, this practice has come under threat with the advent of quantum computing. In theory, quantum computers can exploit Shor's algorithm and crack even the most advanced encryption algorithms. Such an event would throw the field of cybersecurity into disarray as it destroys the very principles of cryptography itself. In order to avert the impending "quantum apocalypse", a new field of cryptography has been developed: post-quantum cryptography.

In traditional cryptography, encryption is a process in which a sender encrypts data or "plaintext" using a designated key and converts it into "ciphertext" before sending it to a recipient that can only decode the data with a compatible key [1]. The keys used during encryption and decryption can either be the same or different in processes known as symmetric encryption and asymmetric encryption respectively. The most commonly used symmetric cryptosystem is the Advanced Encryption Standard or AES and it holds the distinction of being the chosen cipher of the United States government with NSA approval for protecting classified information (NIST). Similar to many other symmetric encryption methods, AES creates the same key for encryption and decryption in addition to dividing plain text into sections known as "block ciphers" (NIST). It uses a substitution permutation network with a key expansion process which means that the initial key is used to generate new keys called round keys, with each being

generated over several rounds of modification, making it harder to break. AES adds the initial key to a block with an XOR cipher and each byte in each block is substituted with another using a predetermined table. To decrypt, receivers must reverse the process, highlighting how fast and efficient AES works [2]. On the other hand, the most commonly used asymmetric cryptosystem is Rivest, Shamir, and Adleman or RSA and it relies primarily on prime factorization for encryption, key agreements, and digital signatures [1]. RSA generates the public private key pair using the product of two very large prime numbers p and q and goes through several mathematical steps to obtain the public key, (n, e), and private key, (n, d). To encrypt and decrypt, senders and users must use the formulas $C \equiv M^e \pmod{n}$ and $M \equiv C^e \pmod{n}$ respectively (Tech Target). Similar to RSA, many encryption methods rely on the difficulty of factoring the product of very large prime numbers to secure their data since the time it takes to properly factor the right prime numbers from a large composite number increases rapidly with the size of the input [3]. While the stark contrast between the two cryptosystems highlights a wide range of data encryption methods, the entirety of modern cryptography is vulnerable to some degree in the face of quantum computers, especially asymmetric encryption and those that rely heavily on prime factorization.

"Quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers" (IBM). With a hardware system the size of a car and a quantum processor similar to that of the average processor, quantum computers are exceptionally faster and more efficient than classical computers. They are different in that they do not rely on binary bits that switch ones and zeros but rather quantum bits or "qubits" [4]. Qubits alone are useless but when placed into a state of superposition, they create "multidimensional computational spaces" in which complex problems

can be placed and solved more effectively (IBM). Superposition is a quantum mechanical state in which qubits represent all possible configurations rather than just one or zero and this allows them to perform two calculations simultaneously, resulting in their faster computational time [4]. Quantum computers alone are not enough to break modern cryptography and instead rely on Shor's algorithm, which is specifically designed to efficiently factor large composite numbers faster. This allows quantum computers to factor polynomial time or $O((\log N)^3)$ rather than the exponential time required by classical computers [3]. The main feature of the algorithm is the Quantum Fourier Transform or QFT, a derivative of the classic Fourier Transform, and it functions by allowing the algorithm to "find the period of a specific mathematical function related to the number being factored" and extract prime numbers efficiently using classical methods once found [3]. While quantum computers still remain in their infancy, precautions have been taken by the NIST to mitigate the future consequences. Once fully developed, quantum computers can use Shor's algorithm and fully harness quantum mechanics to wreak havoc on modern cryptography, rendering the "hardness" of prime factorization useless and placing the future of cryptosystems such as RSA in jeopardy.

In response to the inherent weaknesses associated with traditional cryptography in the face of quantum computing, the field of post-quantum cryptography or PQC has been developed. Also known as quantum-resistant cryptography, PQC is a branch of cryptography designed specifically to protect data against quantum attacks by employing algorithms that use mathematical problems that are too difficult for both classical and quantum computers to solve (GFG). It is essential for the future of cybersecurity since it upholds the principles of cryptography and continually secures data in spite of outside challenges, no matter how advanced. Currently, there are six approaches that have been proposed for post-quantum

cryptography and they rely on a principle known as “hardness”, which refers to the computational difficulty it takes for computers to solve mathematical problems implemented in cryptographic algorithms, or simply put, a resistance to attacks. It’s also important to understand that there is a trade-off between hardness and scalability, a trade-off that is amplified in PQC. So far, they have shown great potential in resisting attacks from quantum computers.

The first major approach is lattice-based cryptography and it relies on the difficulty of manipulating lattices, high dimensional geometric objects containing multiple points, to resist quantum attacks (GFG). For example, consider two lattices, one with 1,000 points and one with 10,000 points and randomly choose a point from each lattice. Without a key, it would be very difficult to determine which points correspond to each other but with it a recipient can properly decode the message with ease. There are two main types of lattice-based algorithms, keyed or unkeyed with keyed algorithms requiring private keys whereas unkeyed algorithms do not [5]. In addition to its variations, there are also several features that allow it to beat out conventional ciphers including improved security, faster computational times, lower energy consumption, and flexible implementation. Currently, there are only four algorithms that have been standardized by the NIST and deemed to be quantum resistant, with CRYSTALS-Kyber being used for general encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS+ being used for digital signatures. These algorithms are known as Key Encryption Mechanisms (KEM) and of the four, three are lattice based, CRYSTALS-Kyber, CRYSTALS-Dilithium, and FALCON, indicating that lattice based cryptography is currently the most successful.

The second major approach is code-based cryptography and its security is reliant on the hardness of decoding certain types of error-correcting codes (GFG). An error correcting code or ECC is an encoding scheme that transmits data as binary numbers and uses mathematical

techniques in a way that errors that may occur during transmission can be detected, corrected, and recovered [6]. The private key is randomly generated using a key generation algorithm and it is used to encode data using a chosen error-correcting code. A public key is then derived from the private key and is used along with the error-correcting code to encrypt the data, creating a ciphertext known as the "codeword". The recipient then decrypts the "codeword" using the code and private key [7]. Theoretically, this form of cryptography makes it more difficult for quantum computers to break by requiring the interpretation of high rate codes, something these computers should have trouble with.

The third major approach is multivariate cryptography, which relies on the difficulty of solving systems of multivariate polynomial equations over a finite field such as a public map [7]. It starts with selecting a set of multivariate polynomial equations with random coefficients as the public key, with the private key being the solution and the assumption that it's a hard computational problem. To encrypt, senders must substitute random values for the variables as defined by the public key and to decrypt recipients must substitute the values back. Security increases as the number of variables and degree of coefficients increase. Currently, various attempts at creating a secure multivariate encryption scheme have failed (NIST).

The fourth major approach is hash-based cryptography and it encrypts data by creating "digital signature algorithms whose security is mathematically based on the security of a selected cryptographic hash function" [8]. Hash functions convert plaintext into ciphertext of a specific length with the added benefit of fast computing and collision resistance, meaning that two inputs will not have the same hash value (GFG). Hashed-based cryptography starts with a one-time signature scheme or OTS, in which a key pair can only be used to sign one message to prevent signature forgery. The objective of this approach is to combine a large number of these one-time

key pairs into a single structure called the Merkle tree in order to achieve the goal of signing more than once albeit a limited number of times [8]. In this data structure, the root is the "master" public key and the leaf nodes are labeled with a cryptographic hash values of a data block, with the non-leaf nodes being labeled with the hash of the labels of its child nodes, ensuring efficiency and security [8]. Hash-based cryptography is one of the more promising approaches and this best exemplified by SPHINCS+, the only one of four algorithms standardized and approved by the NIST for quantum resistant digital signatures to be hash based (NIST).

The fifth and last major approach is isogeny based cryptography and it is primarily based on the difficulty of computing isogenies between elliptic curves [7]. An isogeny is a special map between elliptic curves that preserves the group structure of the curves (MIT). A pair of isogenous elliptic curves is generated and a base point on one is designated as the public key while the base point of the second curve is designated as the private key. The keys are exchanged and used to compute the isogeny on both sides, generating a shared secret that can then be used as a symmetric key for encryption and decryption. Examples of isogeny-based cryptography include Supersingular Isogeny Diffie-Hellman (SIDH) and Supersingular Isogeny Key Encapsulation (SIKE), which are both insecure and should not be used under any circumstances according to it's developers, highlighting the challenges that come with computing quantum resistant algorithms (NIST). Currently there are no quantum algorithms capable of solving isogenies, making it one of the more ideal algorithms.

In addition to these proposals, existing symmetric cryptosystems such as AES and SNOW 3G have already been proven to be resistant against quantum attacks given they use sufficiently large key sizes (NIST). Besides this, three algorithms have already been standardized

by the NIST for digital signatures and approved as quantum resistant including the lattice based FALCON and CRYSTALS-DILITHIUM and hash based SPHINCS+. While the five candidates and some preexisting cryptosystems display relatively promising results, there are still some major challenges developers need to overcome, especially in regards to multivariate cryptography. Besides this, developers must also solve other problems that may arise during post-quantum cryptographic development and implementation and patch any potential vulnerabilities that these cryptosystems may exhibit in the future, since the field of quantum computing is constantly evolving with the changes going hand in hand with the development of post-quantum algorithms.

While the development of post-quantum cryptography seems like an obvious solution to the impending quantum apocalypse, its implementation doesn't come without its challenges. A major problem software engineers face when developing post-quantum algorithms is the lack of preexisting compatible infrastructure and as a result, they must develop new hardware and software alongside the algorithms. Developers must partially change or completely replace the "cryptographic libraries, implementation validation tools, hardware that implements or accelerates algorithm performance, dependent operating system and application code, communications devices and protocols, and user and administrative procedures" (NIST). In addition, new standards, procedures, and best practices must be created to conform to newer quantum-resistant algorithms. This burden would also fall upon the information and operational technology organizations that depend on public key cryptography for encryption. This is because most of these organizations don't know where the cryptography is used which poses a problem since the location and purpose of the public key cryptography must be identified before migration into a post-quantum world. This would entail the creation of additional tools that

would assist in locating and finding out how the public-key cryptography is being used in the current infrastructure, making efforts towards quantum resistance even more expensive (NIST).

In addition to the various challenges faced when implementing PQC, PQC itself faces several vulnerabilities. The first major vulnerability is large key sizes. Most PQC systems require larger keys than traditional public key systems which results in longer encryption and decryption times along with larger storage space, memory, and network bandwidth requirements [9]. These factors culminate in higher performance and poorer performance costs especially when thousands of different keys run simultaneously. Besides this, PQC is incompatible with the current infrastructure or in the best case scenario strains it, as mentioned earlier. PQC may also be incompatible with resource constrained devices such as smartphones and IoTs. The second major vulnerability is non-ideal scalability. Many current PQC algorithms struggle to maintain their hardness as a result of the inherent trade-off between scalability and encryption hardness which means that they are resistant to most but not all attacks. While this may be the case now, it might only be true for the PQC systems that are currently being developed [9]. The third and most important vulnerability is its vulnerability to developments in quantum computing. Advancements in PQC and quantum computing go hand in hand like a game of cat and mouse, with each one always trying to overtake the other. Theoretically, PQC algorithms should be invulnerable to all quantum computers regardless of computing power but it is currently unknown whether or not the most current and advanced PQC algorithms will be rendered useless if the power of the contemporary quantum computers exceeds the algorithms' hardness [9]. While it seems PQC is extremely weak, the issues that may arise as a consequence of its many vulnerabilities are long term since the field of quantum computing and current capabilities of quantum computers are still under development and have yet to reach their full potential.

While it may feel like taking one step forward, two steps back, there is still hope. Several solutions have been put forth such as compression techniques to reduce the storage usage required by PQCs but the most prominent one is the PQC standardization program initiated by the NIST (NIST). Currently, NIST brings awareness to PQC and holds competitions to find the best algorithms. As mentioned earlier, only four have been standardized and they all have one thing in common, they use comparatively smaller key sizes in their algorithms, providing faster operations. It should be noted that the SPHINCS+ algorithm is hashed based and slower due to its different and complex mathematical implementations [10]. This trait was also mentioned earlier when discussing the trade off between scalability and hardness, highlighting the infeasibility in implementing large methods. Post-quantum cryptography and quantum computing are still emergent fields and as a result, many new things are still being discovered. With this in mind, quantum computers are not an immediate threat and the only real strategy in preventing them is to let it progress naturally while developing and optimizing PQC algorithms with those developments in consideration since there is no practical way stopping scientists from further research quantum computing.

Apart from its impact on the field of cybersecurity, post-quantum cryptography will also transform the military sphere and determine the future of military cryptography. With the advent of post-quantum cryptography, one of the main goals of the United States military is to create a cryptographic system that meets the standard introduced by the one time pad, a symmetric encryption method that is unbreakable in theory. This works by using a truly random key whose size is at least the length of the message and only used once. The pad is longer than the message and the frequency distribution is uniform since the shifts are random, which lends itself to the system's invincibility. However, there are three significant weaknesses. The first is that modern

computers are not capable of obtaining true randomness. The second is key distribution since one-time pads are limited to the parties included in the communication. The number of pads grows in proportion to n^2 which results in both the pads running out and the process slowing down as the number of pads increase, rendering the system ineffective. Lastly, is the problem of authentication. Although the pad is theoretically uncrackable, it is still susceptible to interception and there is no way to verify the legitimacy of the sender. Using advancements in PQC and quantum technology, the military can address weaknesses in the pad. In theory, quantum computers can produce perfectly random numbers, solving the issue of true randomness in the pad keys [11]. In addition to this, the quantum key distribution or QKD has been shown to help solve the key distribution and authentication issues with its ability to detect active eavesdropping attempts. Since it is a quantum mechanic, it inherently applies the principle of no cloning to ensure that any attempt at intercepting information will cause disturbances. This is similar to how digital signatures would be applied, allowing parties to identify whether the key exchange has been compromised. However, A major disadvantage of this would be that QKD is dependent on components manufactured on a quantum scale, making them extremely difficult and expensive to produce [11]. In addition, there is no guarantee that it will provide greater security uses than the aforementioned algorithms.

Besides military cryptography, PQC would also transform underwater and space warfare. In a maritime setting, post-quantum cryptography would mostly focus on sensing technology and with its introduction would change how submarines navigate, how mines are detected, and how naval warfare is conducted. This is because the quantum magnetometer is currently being proposed as the main tool for submarine and naval protection. With the introduction of post-quantum cryptography, these magnetometers could become more resistant and significantly

reduce the efficiency of naval mines and submarines. In addition to this, post-quantum cryptography can be used to significantly enhance sonars and implement inertial navigation in submarines. As countries such as the United States advance their space programs, space is becoming increasingly militarized and as a result, "space also will be key for placing quantum sensing and communication technology in satellites, as well as for space countermeasures" [11]. Technologies such as the quantum gravimeter and gravity gradiometer are desirable for sensing and mapping satellites in space, providing for easier navigation and detection of resources, anomalies, and threats.

The quantum apocalypse is a very real existential crisis that could serve to undo decades of efforts to secure data and the fundamental cybersecurity principles but there is still hope. Currently, the NIST has already approved three quantum resistant algorithms, with many more on the way. Post-quantum cryptography, while promising, still faces many problems during the implementation and development process along with the challenge of constantly changing as the field of quantum computing evolves. Despite this, the future of cybersecurity remains bright and only time will tell if quantum computers will succeed.

Works Cited

[1] D. Cariaga, “Introduction to Cyber Security and Digital Forensics ” CS 2610, California State Polytechnic University, Pomona, 2023.

[2] “Everything you need to know about AES-256 encryption,” Kiteworks, http://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/#:~:text=AES%20works%20by%20having%20the,another%2C%20following%20a%20predetermined%20table (accessed Dec. 10, 2023).

[3] “Shor’s algorithm,” What is Shor’s Algorithm, http://www.quera.com/glossary/shors-algorithm#:~:t ext=Shor%27s%20Algorithm%2C%20named%20after%20mathematician,known%20classical%20algorithms%20for%20factoring (accessed Dec. 10, 2023).

[4] C. Q. Choi, “Quantum Computing for dummies,” IEEE Spectrum, https://spectrum.ieee.org/quantum-computing-for-dummies (accessed Dec. 10, 2023).

[5] K. Ahmad, “What is lattice-based cryptography and why is it important?,” MUO, http://www.makeuseof.com/what-is-lattice-based-cryptography/ (accessed Dec. 10, 2023).

[6] A. Katz and S. Dash, “Error correcting codes,” Brilliant Math & Science Wiki, https://brilliant.org/wiki/error-correcting-codes/ (accessed Dec. 10, 2023).

[7] R. Overbeck and N. Sendrier, “Code-based cryptography,” SpringerLink, https://link.springer.com/chapter/10.1007/978-3-540-88702-7_4 (accessed Dec. 10, 2023).

[8] “What is hash-based cryptography?,” Utimaco, https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-hash-based-cryptography (accessed Dec. 10, 2023).

[9] R. Copil, “The weaknesses of post-quantum cryptography,” Quantropi, https://www.quantropi.com/3-weaknesses-of-post-quantum-cryptography/ (accessed Dec. 10, 2023).

[10] K. Townsend, “NIST announces Post Quantum Encryption Competition winners,” SecurityWeek, https://www.securityweek.com/nist-announces-post-quantum-encryption-competition-winners/ (accessed Dec. 10, 2023).

[11] M. Krelina, Quantum technology for military applications - springer, https://link.springer.com/content/pdf/10.1140/epjqt/s40507-021-00113-y (accessed Dec. 11, 2023).

[12] I. T. L. Computer Security Division, “Post-quantum cryptography: CSRC,” CSRC, https://csrc.nist.gov/projects/post-quantum-cryptography (accessed Dec. 10, 2023).

[13] I. T. L. Computer Security Division, “Block cipher techniques: CSRC,” CSRC, https://csrc.nist.gov/projects/block-cipher-techniques (accessed Dec. 10, 2023).

[14] M. Colbeck “Quantum Encryption in Military Communications.” Institute of Marine

[15] M. Kumar, “Post-quantum Cryptography Algorithm’s standardization and performance analysis,” Array, http://www.sciencedirect.com/science/article/pii/S2590005622000777 (accessed Dec. 10, 2023).

[16] M. Langford, “Improve post-quantum cryptography security with CSPM,” Trend Micro, https://www.trendmicro.com/en_za/devops/22/k/post-quantum-cryptography-security-cspm.html (accessed Dec. 10, 2023).

[17] “NIST announces first four quantum-resistant cryptographic algorithms,” NIST, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed Dec. 10, 2023).

[18] M. Cobb, “What is the RSA algorithm? definition from searchsecurity,” Security, http://www.techtarget.com/searchsecurity/definition/RSA#:~ :text=RSA%20is%20a %20type%20of,is%20used%20to%20decrypt%20it. (accessed Dec. 10, 2023).

[19] C. Mann, The science of encryption: Prime numbers and mod arithmetic, https://math.berkeley.edu/~kpmann/encryption.pdf (accessed Dec. 11, 2023).

[20] “What is quantum computing?,” IBM, http://www.ibm.com/topics/quantum-computing (accessed Dec. 10, 2023).