Quantum Resilience

Josh Smith

Sunday Ogunlana

CYBR-3310.203

5/5/2023

Abstract

We are living on the frontier of quantum computing—the dawn of the qubit and the potential collapse of classical encryption. The rise of quantum computing poses a significant threat to information security, making cryptographic schemes vulnerable to cyber attacks. Therefore, novel encryption algorithms that can resist classical and quantum computational attacks are necessary. This paper scrutinizes the emerging field of Quantum Resilience as it aims to develop robust cryptography for this brave new world. This study focuses on exploring existing quantum-resistant encryption algorithms, like lattice-based and hypertree-based cryptography. Additionally, we analyze the role played by NIST in standardizing these methods. We believe that prioritizing Quantum Resilience and advocating for the widespread application of quantum-resistant encryption techniques will help us protect our digital world more effectively against the constantly-evolving quantum computers.

To understand why Quantum Resilience is essential, it should be established why classical encryption can be decrypted easily by a quantum computer. Classical cryptography algorithms—especially public key encryption (PKE)—rely on the difficulty of factoring large numbers and calculating discrete logarithms. Factoring large numbers by guessing randomly or following a linear progression takes $O(n)$ time, where n is the size of the number being factored. The amount of time can be significantly decreased by only checking numbers equal to or lower than the number's square root, leading to $O(\sqrt{n})$. However, by using a fast primality test—such as Agrawal-Kayal-Saxena (AKS)—the time complexity can be shortened to $O((\log n)^6)$ (Lenstra & Pomerance, 2019). Even in these best-case scenarios, large numbers are difficult to factor.

When quantum computers have enough qubits to break encryption, they will use Shor's Algorithm, a method of factoring numbers specialized for quantum computation. The algorithm has two parts, the classical and the quantum operations (IBM, N.D.). IBM claims that Shor's Algorithm will take $O(\log^3 n)$ operations, where $\log$ is implied base ten. This is *significantly* faster than any classical algorithm.

Even though large quantum computers are not viable—let alone even available to the public—yet, everybody is still in danger of quantum decryption because of "Store Now, Decrypt Later" (SNDL), where hackers intercept encrypted traffic now in hopes of having access to sufficient computing in the future to decrypt it. This means that any traffic using TLS, SSL, RSA, Diffie-Hellman, or any other algorithm based on the toughness of factoring is vulnerable to being intercepted and stored for future decryption. Another very unfortunate sector of the internet that will be devastated by further quantum development is cryptocurrency. A large portion of the

top fifty cryptocurrencies are founded on the Bitcoin or Ethereum blockchains which both use Elliptic Curve Digital Signature Algorithm (ECDSA) to handle PKE. This is important because all it takes for a quantum computer to break ECDSA is a minor modification of Shor's Algorithm.

Three of the four algorithms NIST chose to use as its standard quantum-resistant encryption methods are based on the mathematics of structured lattices. In math, lattices can be described as a structure created by the addition and/or subtraction of two vectors about an origin point in an infinite space. Now, notice that lattices are not confined to two-dimensional space and that the quantum-resistant algorithms propose several-hundred-dimensional space. Two parties can produce a public/private key pair using lattices. A private lattice can be constructed using two constructor vectors with relatively small magnitudes and a large angle between them. Then, the lattice can be shared publicly via two other vectors with a significantly larger magnitude and a slimmer angle between them. Herein lies the difficulty: finding the most optimal set of vector combinations to reach any given point on the lattice is trivial with the private vectors. This is much harder to do given vectors of greater magnitude that are acutely bound (Bernstein, et al., 2015).

The fourth and final NIST quantum-resistant algorithm is "Sequential PHoton Interrogation And Neutron Counting Signatures" (SPHINCS$^+$), which relies on entirely different mathematics than the other three. So, while SPHINIC$^+$ "is somewhat larger and slower than the other two, it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections" (NIST, 2022). This shows excellent foresight by NIST if one of these other, faster, algorithms fails to be secure as they seem.

The exact process that SPHINCS$^+$ uses is based on hash signature schemes (HSS), which are described as a tree of hashes (think of a Merkel Tree) where the root is the global public key. Each time a node (or leaf) in the tree is signed, a one-time signature is derived from a combination of the global private key and the node's hash. Because SHA256 and other modern hash functions are quantum-resistant, SPHINCS$^+$ implements several algorithms that use hashes like SHA256 to build the trees. The main difference between SPHINCS$^+$ and any other HSS is that SPHINCS$^+$ has the property of being stateless, which means increased versatility in the context of HSSs.

In conclusion, quantum computing will eventually cause the collapse of security in classical encryption. This paper identifies how NIST has led the effort in developing Quantum Resilience and demonstrates how the field is rapidly evolving to undermine the threat that quantum computing poses. Quantum-resistant encryption methods *must* be developed and rigorously tested long before the exponential increase in qubits leads to disaster. One analogy that puts it perfectly: if astronomers detected that an asteroid is headed for Earth that is still 100 years out, everybody would not wait to start brainstorming solutions. Governments and physicists would team up and immediately begin working on a way to avoid the danger. The same applies to Quantum Resilience.

Sources Cited

Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., ... & Wilcox-O'Hearn, Z. (2015). SPHINCS: practical stateless hash-based signatures. In Advances in Cryptology--EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I 34 (pp. 368-397). Springer Berlin Heidelberg.

Lenstra, Jr., H., & Pomerance, C. (2019). Primality testing with gaussian periods. Journal of the European Mathematical Society, 21(4), 1229–1269. https://doi.org/10.4171/jems/861

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

Suhail, S., Hussain, R., Khan, A., & Hong, C. S. (2021). On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. IEEE Internet of Things Journal, 8(1), 1–1. https://doi.org/10.1109/jiot.2020.3013019

Unknown. (2022, July 5). NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Unknown. (N.D.). Shor's algorithm - IBM Quantum. Quantum-computing. https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm