Engineering 21 (2023) 6–8

Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

News & Highlights

Quantum Cryptography Competition Yields Next-Generation Standard Algorithms

Chris Palmer

Senior Technology Writer

In as little as a decade from now, quantum computers may be able to break the cryptographic keys that currently protect everything from smartphone banking apps to email software. In July 2022, in anticipation of this threat, the US Department of Commerce's National Institute of Standards and Technology (NIST) announced the first group of encryption tools designed to fend off such attacks, the initial winners of a competition process initiated in 2016 [1,2].

The tools include a general encryption algorithm used to secure information exchanged across public networks, and three algorithms used to manage digital signatures, which provide identity authentication. NIST will fold the four selected encryption algorithms into its post-quantum cryptographic standard, which is expected to be finalized in about two years [1].

The announcement marks a key milestone for the competition in which NIST called upon cryptographers around the world to devise post-quantum encryption methods that could resist attacks from future quantum computers, ones far more powerful than the limited quantum machines available today [3,4]. Teams from academia and industry, with members from nearly 50 countries on six continents, submitted 82 algorithms; of these, 69 were thoroughly tested by experts around the globe [1].

Classical computers, even the world's most powerful supercomputers, struggle to quickly factor large numbers. Current public-key encryption systems leverage this difficulty to protect online bank transactions and other sensitive information (Fig. 1). While it is easy to generate sharable keys that can encrypt and decrypt data, it is nearly impossible for nefarious individuals to derive the numbers that make them work.

In 1994, AT&T Bell Laboratories researcher Peter Shor showed that future quantum computers would find such calculations trivial [5]. By 2001, scientists had demonstrated that they could run Shor's algorithm, but only to derive the prime factors of 15 [6]. While quantum-computing technology has made remarkable progress since then [3,4], running Shor's algorithm to factor the large-number keys protecting the world's data is still a long way off. Regardless, "The consensus among quantum computing engineers is that 'Q-day,' the day that quantum computers can break public encryption keys, is not an if. It is a when," said Nick Sullivan, head of research and cryptography at Cloudflare, an internet security company headquartered in San Francisco, CA, USA.

"People wonder why we are standardizing this now when a quantum computer does not yet exist. Well, you can already be at risk today from the so-called 'harvest now, decrypt later' threat," said Dustin Moody, a mathematician in the NIST Computer Security Division. This threat arises from the idea that encrypted data can be copied from the internet now and held onto until quantum computers become powerful enough to decrypt it. "Adversaries to the United States are actively harvesting data with this threat in mind. It is certainly a real concern," said Moody, who directs NIST's post-quantum cryptography project.

Moody said that the post-quantum encryption algorithms NIST selected were judged by their security level against current classical attacks, their expected security level against quantum attacks, and their efficiency, which encompasses speed and compactness. "There was a lot of public scrutiny," said Sullivan. "Many cryptographers examined the submissions and were able to identify weaknesses."

For general encryption, NIST selected the Cryptographic Suite for Algebraic Lattices (CRYSTALS)-Kyber algorithm. This algorithm

Fig. 1. Quantum computers of the future will likely be powerful enough to break the cryptographic keys that currently safeguard online data and communications. To prepare for this future, the US Department of Commerce's National Institute of Standards and Technology recently selected a handful of tools that can be implemented in the next few years to protect against quantum computer-based attacks. Credit: Pixabay (CC0).

https://doi.org/10.1016/j.eng.2022.12.002

was chosen for its overall speed and its relatively small encryption keys that can be used by two parties to easily exchange data [7]. For digital signatures, NIST selected CRYSTALS-Dilithium, Fast-Fourier Lattice-based Compact Signatures over Number Theory Research Unit (FALCON), and Stateless Practical Hash-based Incredibly Nice Collision-resilient Signatures (SPHINCS+). NIST endorses CRYSTALS-Dilithium as the primary digital signature algorithm. FALCON was preferred for applications requiring smaller signatures than Dilithium can provide [7], though Moody said it was considerably more difficult to implement.

Although SPHINCS+ is larger and slower than either of the other two digital signature algorithms, it is considered valuable as a backup. This is because, while the other selected algorithms, including the general encryption one, are based on a family of math problems called structured lattices (functions in which data are mapped to vectors within matrices of arbitrary dimensions), SPHINCS+ uses a wholly different mathematical structure based on hash functions (functions in which data of arbitrary sizes are mapped to a fixed-size value) [5].

"Lattices are attractive because they are very good all-around performers. They are very fast, even a little faster than what we use for encryption today, and efficient when you implement them," Moody said. "The latter characteristic is important because we expect to implement these crypto systems everywhere."

NIST will now begin developing standards for deploying the algorithms. The institute then expects to issue its official standard in 2024 after getting additional feedback from the cryptography community over the next year. Meanwhile, Moody said, an international, volunteer-based, Internet protocol standards body called the Internet Engineering Task Force (Fremont, CA, USA) will decide how to build the algorithms into real applications. Once that work is completed, internet companies can start integrating the algorithms into web browsers, and technology providers can begin deploying the algorithms during periodic software updates.

Over the past few years, both Cloudflare and internet colossus Google (Mountain View, CA, USA), often working in tandem, have been running real-life tests of some post-quantum algorithms by including them in select beta versions of Google's Chrome web browser and in select server software [8]. Testing is crucial because, for internet communications to go smoothly, it is not enough to have perfectly compatible servers and browsers. To connect these pieces, data must also run through network devices that might block traffic with unfamiliar encryption protocols.

Google's parent company Alphabet [9] and Cloudflare [10] are among many companies assisting the relatively small number of browser developers and server providers around the globe with swapping out their encryption systems. Where the transition might be more difficult to implement is the multitude of connected Internet of Things (IoT) devices [11], such as cars, security cameras, and "smart home" gadgets, whose security features are hardwired into their chips, which are not usually replaced.

No central organization will oversee the implementation. However, NIST offers online tools to validate that the implementation of approved cryptographic algorithms has gone smoothly. While these validation tests are free, full, internet-wide implementation will not be cheap. "Of course, upgrades are going to have a cost, but those are traditionally built into the lifecycle of online products, especially software-as-a-service technologies," Sullivan said. "On the other hand, if there are places in which cryptography is implemented inside of hardware, such as IoT devices, the solution may be to just throw away the old ones and build a new generation."

Despite the costs, Sullivan said that starting now is critical, especially if Q-day arrives within 5–10 years. "It is very hard to upgrade a whole swath of technology in that amount of time, especially when dealing with something that cannot be exploited currently," he said. Even with the best of intentions, or in some cases government-enforced mandates, some companies and organizations may be resistant to updating their information technology, regardless of the clear benefits [12].

One of the more wide-ranging cryptography-technology upgrades the industry has seen, switching from the hash function Secure Hash Algorithm-1 (SHA-1) to SHA-2 [13], provides a useful roadmap for implementing post-quantum encryption. Hash functions take a string of data of any length and produce a fixed-length hash value, or digital fingerprint. SHA-1 was created by the US National Security Agency (NSA) and published as a standard by NIST in 1995. Knowing it would one day be broken, NSA software engineers began developing the stronger SHA-2 in 2002. The new hash function was widely implemented starting in 2015, two years before SHA-1 was successfully broken [14]. SHA-2's eventual replacement, SHA-3, also developed by NIST via a public contest and adopted in 2015, is currently waiting in the wings. "It took the industry more than five years to make SHA-2 close to ubiquitous. And that was with a very active and practical attack against the algorithm," Sullivan said. "And despite the massive migration effort, SHA-1 still is used for some applications."

Post-quantum and current encryption methods may end up operating together for a decade or so before the new algorithms are used exclusively. "Some folks think that hybrid operation will be useful in perpetuity," Sullivan said. "Others think that once these post-quantum algorithms have been out there for long enough, they will be as battle tested as the traditional algorithms and hybrid use will no longer be necessary. In the end, it comes down to how much confidence we have in the new algorithms."

Regardless of how confident the world's cryptography experts are in NIST's selections, some countries, including China and Russia, will go their own way [15]. China, which has historically used different cryptographic algorithms than the rest of the world, ran its own post-quantum encryption competition in 2018 and 2019 and announced a handful of winners, also based on structured lattices, in 2020 [15]. "China's competition was smaller and a lot quicker than ours," Moody said. "But they ended up selecting some algorithms that are very similar to the ones we landed on."

"We had such a very long and rigorous selection process because you cannot go back. If an algorithm is weak mathematically, it is incredibly difficult to change post-implementation," Sullivan said. "We are pretty sure, though, that this process led to some excellent choices that will protect data for years and years."

One day, the concept of post-quantum encryption could be made obsolete with the advent of a quantum internet in which the principles of quantum physics could make information exchange essentially hacker-proof [16,17]. Nevertheless, given that one of NIST's encryption algorithm semifinalists, Supersingular Isogeny Key Encapsulation (SIKE), was recently broken with relative ease using a simple classical computer [18], Moody said NIST is currently evaluating four additional post-cryptography encryption algorithms not based on lattices to serve as backups to its current selections. NIST has also launched a new competition to identify additional backup algorithms for digital signatures [19]. "If there is some breakthrough in the field, and new vulnerabilities are discovered, we want other encryption algorithms in our back pocket to pivot to quickly," Moody said.

References

[1] Castelvecchi D. These 'quantum-proof' algorithms could safeguard against future cyberattacks [Internet]. London: Nature; 2022 Jul 11; [cited 2022 Oct 30]. Available from: https://www.nature.com/articles/d41586-022-01879-6.
[2] Boutin C. NIST asks public to help future-proof electronic information [Internet]. Gaithersburg: NIST; 2016 Dec 20 [cited 2022 Oct 30]. Available

from: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information.
[3] Palmer C. Google takes a big step toward quantum computing. Engineering 2020;6(4):381–3.
[4] Palmer C. Quantum computing quickly scores second claim of supremacy. Engineering 2021;7(9):1199–200.
[5] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science; 1994 Nov 20–22; Santa Fe, NM, USA. New York: IEEE; 1994. p. 124–34.
[6] Vandersypen LMK, Steffen M, Breyta G, Yannoni CS, Sherwood MH, Chuang IL. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature 2001;414(6866):883–7.
[7] O'Shea D. NIST picks initial post-quantum security standards [Internet]. New York: Fierce Electronics; 2022 Jul 7 [cited 2022 Oct 30]. Available from: https://www.fierceelectronics.com/electronics/nist-picks-initial-post-quantum-security-standards.
[8] Venables P. How Google is preparing for a post-quantum world [Internet]. Mountain View: Google; 2022 Jul 6 [cited 2022 Oct 30]. Available from: https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world.
[9] Smith DI. Data is vulnerable to quantum computers that don't exist yet [Internet]. New York: IEEE Spectrum; [cited 2022 Oct 30]. Available from: https://spectrum.ieee.org/post-quantum-cryptography.
[10] Westerbaan B, Rubin CD. Defending against future threats: Cloudflare goes post-quantum [Internet]. San Francisco: Cloudflare; 2022 Oct 3 [cited 2022 Oct 30]. Available from: https://blog.cloudflare.com/post-quantum-for-all/.
[11] Carlson EK. New standards release sets stage for 5G future. Engineering 2021;7(3):275–6.
[12] Leslie M. Legacy information technology compounds pandemic pain. Engineering 2021;7(4):415–7.
[13] Grimes RA. All you need to know about the move from SHA-1 to SHA-2 encryption [Internet]. Needham: CSO; 2017 Jul 6 [cited 2022 Oct 30]. Available from: https://www.csoonline.com/article/2879073/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html.
[14] Lomas N. Security researchers announce "first practical" SHA-1 collision attack [Internet]. San Francisco: TechCrunch; 2017 Feb 23 [cited 2022 Oct 30]. Available from: https://techcrunch.com/2017/02/23/security-researchers-announce-first-practical-sha-1-collision-attack/.
[15] Liu N. China, Russia to adopt 'slightly different' PQC standards from US [Internet]. Denver: SDX Central; 2022 Oct 19 [cited 2022 Oct 30]. Available from: https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/.
[16] Whalen J. Chicago scientists are testing an unhackable quantum internet in their basement closet [Internet]. Washington, DC: Washington Post; 2022 Oct 9 [cited 2022 Oct 30]. Available from: https://www.washingtonpost.com/technology/2022/10/09/quantum-internet-chicago-argonne/.
[17] Leslie M. Quantum cryptography via satellite. Engineering 2019;5(3):353–434.
[18] Ropek L. Supposedly quantum-proof encryption cracked by basic-ass PC [Internet]. New York: Gizmodo; 2022 Aug 2 [cited 2022 Nov 13]. Available from: https://gizmodo.com/quantum-encryption-algorithm-nist-broken-single-core-pc-1849360898.
[19] Post-quantum cryptography: digital signature schemes. Gaithersburg: NIST; 2022 Aug 29 [cited 2022 Nov 16]. Available from: https://csrc.nist.gov/Projects/pqc-dig-sig/standardization.