Preparing Enterprises for the Quantum Computing Cybersecurity Threats

CSA cloud security alliance®

ACKNOWLEDGEMENTS

Main Author:

Edward Chiu

Co-chairs:

Bruno Huttner
Ludovic Perret

Reviewers:

Sameer Ahirrao
Debra Baker
Robert Clifford
Bruno Huttner
Ludovic Perret

CSA Staff:

Hillary Baron

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Quantum computing harnesses quantum mechanical phenomena, such as superposition and entanglement, to perform information processing in ways not possible or not practical by classical computing. A large-scale, general-purpose quantum computer is expected to help with the discovery of new drugs and materials, supercharge artificial intelligence, optimize a complex financial portfolio and so forth. Conversely, the same quantum computer is also expected to break existing asymmetric-key cryptosystems, thus endangering the very fabric of the cybersecurity infrastructure. Engineering challenges, such as attaining scalability with large grouping of entangled qubits and error correction schemes, must be addressed if quantum computing is to match its high expectations. However, cybersecurity threats that quantum computing may introduce must be addressed now, even though such a machine may not emerge for another decade or more.

The arrival of a powerful quantum computer poses severe consequences to cryptography; this is especially true of public-key encryption, which protects internet security and powers global e-commerce. Corporations housing sensitive information meant for long-term concealment may face quantum attack. Planning must be put in place now to mitigate harvest-and-decrypt attacks.

Enterprise leadership must maintain an ongoing inventory of all impacted information technology (IT) assets and pursue crypto-agility so vulnerable algorithms can be replaced by quantum-resistant ones to mitigate cybersecurity risks; this is particularly vital when the U.S. National Institute of Standards and Technology (NIST) standardizes quantum-safe solutions in the next several years. Leadership should experiment and plan for hybrid cryptography in which a hybrid cryptosystem can sustain and overcome both classical and quantum attacks. Finally, the enhancement of organizational capacity—through the addition of professionals with appropriate skill sets who can help mitigate security risks and reap potential economic benefits associated with quantum computing technology—is highly advised.

What is Quantum Computing?

Classical computers operate on a binary scheme. One notable example is the two-state, deterministic system, in which a series of "ones" and "zeroes" encode information.

Quantum bits (or qubits) are the basic units of quantum computing. Unlike a bit—which can only be in "one" state or "zero" state at a particular time—a qubit can be in "zero" state and "one" state simultaneously (described probabilistically). The power of a quantum computer comes from the unique features of a quantum system. Some of its main features include:

a) Superposition: This allows a quantum system to exist in a "mixture" of two states, described probabilistically.
b) Entanglement: A phenomenon that exists among two or more quantum particles which makes a description of an individual state not possible. This condition must be described as a whole system.
c) Uncertainty: This feature—also known as Heisenberg's Uncertainty Principle—ensures one cannot precisely measure the position and momentum of a particle at the same time. A quantum system forces a particle to a final state of "one" or "zero" once a measurement is taken on.

Harnessing the above quantum physical behavior increases computation power exponentially when solving certain types of problems, and empower quantum computers to process information in new ways[1].

Impact of Quantum Computing on Cryptography

Encryption is the foundation of data security. Currently, there are two types of encryption.

- Symmetric encryption is based on a single key. A sender uses a key to encrypt, and a recipient uses the same key to decrypt. The sender and receiver presumably have a way to exchange or distribute the key securely. Advanced Encryption Standard (AES) is considered the gold standard of symmetric encryption.
- Conversely, asymmetric encryption (i.e., public-key encryption) is based on a key pair. The sender uses the recipient's public key—typically in the form of a digital certificate—to encrypt. The recipient—presumably the sole owner of the private key—uses the private key associated with the digital certificate to decrypt.

Securing internet traffic is based on asymmetric encryption using transport layer security (TLS) certificates. Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC) are two asymmetric encryption schemes that play crucial roles during a TLS handshake. As TLS is the foundation of the network transport layer security of internet traffic, it is easy to imagine the chaos that may ensue if the encryption behind TLS is no longer trustworthy[2]. Besides TLS, messaging protocols such as Secure/Multipurpose Internet Mail Extensions (S/MIME) and Open Pretty Good Privacy (OpenPGP) use RSA as a standard encryption algorithm. RSA is also a conventional algorithm for digital signatures and is widely used in code signing.

The development of a general-purpose quantum computer may result in a different degree of impact for these two types of encryption scenarios.

1. **The impact on symmetric encryption can be mitigated.** Running Grover's algorithm[3] on a quantum computer provides a quadratic speedup, which has the effect of cutting the encryption strength in half. In other words, the encryption strength of AES-256 (based on a classical cryptanalytic attack) has an equivalent encryption strength of 128 bit sustaining the quantum cryptanalytic attack. The implication is that AES requires a larger key size to survive an attack from a quantum computer.
2. **Asymmetric (public-key) encryption face catastrophic consequences.** Running Shor's algorithm[4] on a quantum computer with enough qubits can crack both RSA (based on the hard

[1] National Academies of Sciences, Engineering and Medicine, Quantum Computing: Progress and Prospects, Washington, D.C., 2018, 1-2.

[2] Ritter, J., A Day without Safe Cryptography, Cloud Security Alliance Quantum Safe Security Working Group, 2018 https://blog.cloudsecurityalliance.org/2018/04/19/imagine-day-without-safe-cryptography/

[3] Grover, L.K., A fast quantum mechanical algorithm for database search, Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp 212-19, NY, 1996. http://dx.doi.org/10.1145/237814.237866

[4] Shor, P.W., Algorithms for quantum computation: discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp 124-134, Washington, DC., 1994 http://doi.org/10.1119/SFCS.1994.365700

mathematical problem of large, prime number factorization) and digital signature algorithm (DSA) (based on discrete logarithm-based problems) because Shor's algorithm provides an exponential speedup. The quantum speedup yields many mainstream cryptographic algorithms (RSA, DSA, Elliptic-curve Diffie–Hellman (ECDH), etc.) vulnerable to attack. The potential negative consequences are severe given the ubiquity of asymmetric encryption.

3. **Impact on hash functions can be mitigated.** Hashing is a one-way mathematical function that maps data, regardless of its size, to a unique, fixed-length output called hash. Many password-based authentication systems, including Microsoft Windows, implement secure hashing. The quantum impact of hashing is similar to that of symmetric encryption. The National Institute of Standards and Technology recommends using SHA-256 (Secure Hash Algorithm 256) or SHA-3 with large output to resist quantum attacks.

The following table summarizes the impact of quantum computers on cryptography.

Crypto Algorithm	Type	Purpose	Impact from large-scale QC
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3	—	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Table 1: Impact of a universal quantum computer on mainstream crypto algorithms[5]

The Time to Prepare is Now

In August 2015, the National Security Agency (NSA) recommended a pause of migration to Suite B cryptography due to growing concerns that Suite B—which includes AES, Elliptic Curve Digital Signature Algorithm (ECDSA), ECDH, and RSA-3072— might not be quantum resistant[6]. This announcement—perhaps more than any other—brought attention to the quantum computing cybersecurity threat. The statement, as cited in the "Information Assurance Directorate at the NSA," read: "For those partners

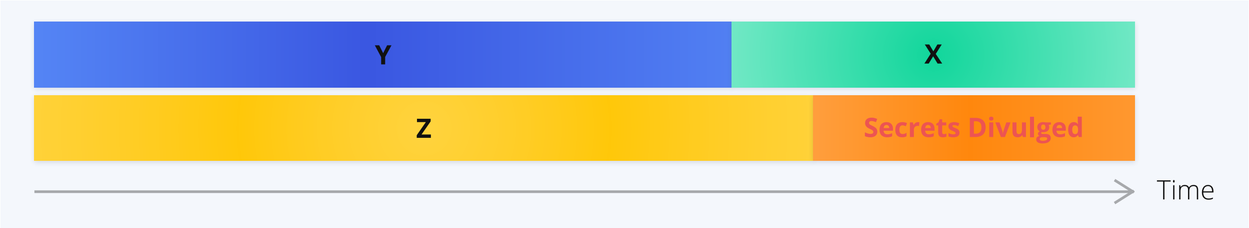
[5] Reproduced from NISTIR 8105, Report on Post-Quantum Cryptography, Feb. 2016.

[6] Dan Goodin, NSA preps quantum-resistant algorithms to head off crypto-apocalypse. https://arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/

and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.[7]"

The development timeline for a quantum computer powerful enough to break RSA-2048 is unknown. Regardless, experts believe it is essential to start planning now to prepare for this "quantum Y2K" moment[8].

Dr. Michele Mosca, a professor with the University of Waterloo's Institute for Quantum Computing, proposed the Mosca theorem[9] (shown in Figure 1) that elaborates the issue.



X – Number of years to keep encryption secure	Y – Number of years to re-tool existing infrastructure to be quantum resistant	Z – Number of years for a large-scale quantum computer to be built

Figure 1. Lead time required for quantum safety[10]

According to the Mosca Theorem, risks are most severe if X (the number of years to keep encryption secure) + Y (the number of years to upgrade existing infrastructure for quantum resistance) > Z (the number of years for a large-scale quantum computer to be built). Based on Mosca's Theorem, this equation is worrisome on two levels:

> - It is a routine corporate responsibility to keep sensitive information confidential for years, especially in certain industries.
> - Upgrading IT assets (hardware, software, and firmware) requires years, if not decades of effort. This scenario especially rings true for large, multinational corporations.

In other words, X + Y may easily exceed two decades. Unfortunately, Dr. Mosca believes companies may not have that long to prepare, as he estimates a quantum computer running Shor's algorithm[11] has a 50 percent chance to break RSA-2048-bit encryption by 2031.

[7] Bruce Schneier, NSA Plans for a Post-Quantum World https://www.schneier.com/blog/archives/2015/08/nsa_plans_for_a.html

[8] Harris, M., The quantum Y2K moment, https://physicsworld.com/a/the-quantum-y2k-moment/

[9] Mosca, M., Cybersecurity in a Quantum World: will we be ready? slide 20, https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

[10] European Telecommunications Standards Institute, Quantum Safe Cryptography and Security, Jun. 2015, Figure 4, p. 13.

[11] Mosca, M., Cybersecurity in an era with quantum computers: will we be ready?, International Association for Cryptologic Research, 2015.

A separate report entitled, “Quantum Computing: Progress and Prospects,” was recently published by the National Academies of Sciences, Engineering and Medicine (NASEM). It reached a similar conclusion. The document—written and reviewed by a team of prominent quantum computing scientists and researchers—covered a wide range of topics, including quantum hardware, software, algorithms, practical applications, and engineering challenges faced when building a scalable quantum computer. The authoring team concluded that a working quantum computer capable of breaking RSA-2048 would likely not arrive in the next decade.[12] However, it also encouraged that quantum computing risk mitigation efforts be given a high priority. According to the NASEM report, these actions are critical given the severe cryptography risks posed—especially to public-key cryptography—and the time required for upgrades, which are predicted to last more than a decade.

In 2016, in response to this emerging threat, NIST called on cryptographers to submit quantum-resistant public-key algorithms as part of its Post-Quantum Cryptography project. Sixty-plus cryptographic algorithms were presented from around the world for the standardization process during a first round of submissions in 2017. From there, NIST selected 26 algorithms, which are now slated for analysis during a second round. The goal is to find quantum-resistant replacements for existing public-key algorithms in encryption and signatures. Most of the selected proposals utilize lattice, code, multivariate and hash schemes. Unlike the factorization of large prime numbers used by RSA—which is vulnerable to quantum attack—these algorithms are based on different mathematical classes not known to be susceptible to quantum attack. This standardization process continues, and NIST expects the availability of draft standards between 2022-24.[13]

Preparation Steps for a Post-Quantum Era

IT decisionmakers should take the following steps now to prepare for a post-quantum era, despite a current lack of available replacement options for RSA and ECC.

1. Acknowledge the severe impact of a powerful quantum computer on cryptography. Opinions differ on the potential arrival date of an operational quantum computer. Some mathematicians claim errors related to noise may prohibit a quantum computer from showing quantum supremacy[14]. Others predict mainstream use of quantum computing in just five years[15]. Stakeholders must acknowledge threats and risks associated with quantum computing—as addressed in the NASEM report—regardless of its ambiguous development timeline. This acknowledgment is a precursor to active mitigation of quantum computing risks.

2. Inventory impacted IT assets. Cryptography is used pervasively in most IT assets and provides data-at-rest and data-in-transit security. Assets may include hardware (servers, laptops, mobile devices, network appliances, etc.), internally developed and vendor software, firmware embedded in the Internet

[12] National Academies of Sciences, Engineering and Medicine, Quantum Computing: Progress and Prospects, Washington, D.C., 2018, S-6

[13] NIST Post-Quantum Cryptography Workshops and Timeline. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline.

[14] Katia Moskvitch, The Argument Against Quantum Computers, Quanta magazine, Feb. 7, 2018 https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/

[15] IBM Research 5 in 5. http://research.ibm.com/5-in-5/quantum-computing/

of things (IoT) and industrial IoT devices. The potential impact of the quantum computer on each of these assets is very different, and each asset requires an independent assessment. One component especially impacted is public-key infrastructure (PKI), where certificate authorities provision digital certificates while certificate management systems manage the certificates (whether on-premise or in the cloud). Another sensitive application relates to data center interconnectivity, where large amounts of data flow daily between one data center and a backup location. Safeguarding this data now and into the future is paramount.

The ubiquitous use of cryptography demands close monitoring of IT assets. Fortunately, many enterprises routinely monitor their IT asset inventories—which allows for more manageable upgrades from impacted crypto algorithms to quantum-resistant alternatives.

3. Pursue cryptographic agility. Cryptographic agility refers to how nimble an organization is to replace existing crypto algorithms with newer ones. The concept is especially relevant today as the strength of existing cryptographic algorithms degrades over time. It is even more relevant with the emergence of the quantum threat.

Software frameworks, such as .NET cryptographic service provider or Java Cryptography Architecture, provide object-oriented classes supporting a wide range of algorithms, modes and key sizes. Developers should avoid hard-coding algorithms and key sizes in their source code. Using these classes and externalizing algorithm names and key sizes in configuration files or database tables facilitate crypto-agility.

On the contrary, the crypto-agility of hardware and network appliances are primarily the vendors' responsibility. These features are particularly relevant for IoT or industrial IoT vendors, where many of the devices with cryptographic support implemented in firmware are expected to last 10-plus years. The expectation is to patch these devices with management consoles upon deployment in the field or an automation environment. It is important to ask vendors to share their quantum-resistant product roadmap. Some of these hybrid options are still in the experimentation phase, while others are already commercially available. Once NIST standardizes post-quantum cryptography, some enterprises may have concerns with turnaround times required for massive upgrades. These organizations should consider the implementation of one or more hybrid cryptography options. Considerations should include evaluation of risks and benefits regarding interoperability with existing infrastructure, performance, and what kind of patching or upgrade mechanisms are provided to support crypto-agility.

4. Implement hybrid cryptography. Mainstream public-key algorithms, such as RSA and ECC, are susceptible to quantum attack. The National Institute of Standards and Technology predicts the completion of the draft standardization of post-quantum cryptography sometime between 2022-24. Enterprises that must store sensitive data for extended periods should consider using hybrid cryptography now to reduce the risk of a harvest-and-decrypt attack[16]. This scenario occurs when a malicious actor silently collects and stores encrypted data, then waits for the arrival of a powerful quantum computer to decrypt the information.

[16] Bauer, M.R., Quantum computing is coming for your data. https://www.wired.com/story/quantumcomputing-is-coming-for-your-data/

Hybrid cryptography refers to the combination of two different classes of algorithms or other cryptographic methods to attain a cryptographic operation, such as encryption or signature. An example of hybrid cryptography is the X.509 certificate with dual signatures. One signature is classical, and the other is quantum safe[17]. Other possible hybrid options include quantum-safe/quantum-safe, classical/ QKD (quantum key distribution),[18] and so forth.

5. Explore the use of alternative technologies. Although the use of public-key cryptography is prevalent, finding alternative technologies that are quantum-resistant—or strategies that supplement public-key cryptography—requires exploration. Examples of such innovations include data tokenization, certain types of zero-knowledge proof systems (such as zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK)), and so forth. However, each of these technologies is appropriate for only specific scenarios and are not usable as an alternative to public-key cryptography in general. The determination of suitability requires detailed analysis on a case-by-case basis. However, if utilized correctly, these various options may contribute to a layer-of-defense approach.

6. Plan on building organization capability (OC) in quantum computing and quantum technologies. While the focus of this paper addresses cybersecurity threats posed by quantum computing, many organizations may realize new opportunities once the technology becomes a reality. Even today, the initial stages of quantum computing application have begun. Examples include:

- Volkswagen hopes to use special-purpose quantum computers to optimize traffic management.[19]
- F. Hoffmann-La Roche AG, a Swiss multinational healthcare company, is engaging in molecular simulation to develop a new medicine using quantum computing technologies.[20]

There are many other applications in various industries, including quantum communication. The potential development of the quantum internet may also provide new solutions.

Running optimization algorithms and simulations on a quantum computer requires a basic understanding of numerous subject areas, including:

- Quantum physics
- Mathematics (such as linear algebra and computational complexity theory)
- Programming quantum gates
- Vendor-specific quantum software
- Classical and quantum programming languages

Undergraduate and graduate-level courses offered through quantum information science, computer science and engineering, mathematics, and physics departments often address these topics. Executive

[17] Kampanakis, P., Panburana, P., Daw, E., and Van Geest, D., The Viability of Post-quantum X.509 Certificates, Cryptology ePrint Archive, Report 2018/063, 2018. https://eprint.iacr.org/2018/063.pdf

[18] Brown, M., Faux, R., Perret, L., Mitigating the Quantum Threat with Hybrid Cryptography, Cloud Security Alliance Quantum Safe Security Working Group, 2018

[19] Volkswagen wants to use quantum computers to optimize traffic. https://www.engadget.com/2018/11/05/volkswagen-quantum-computer-traffic-management/

[20] https://www.roche.com/quantum-computing.htm

decisionmakers interested in exploring how to leverage quantum computing in their businesses should plan to build OC accordingly.

The mitigation of cybersecurity threats involved with post-quantum cryptography does not require a mastery of every skill mentioned above, although some basic knowledge in each area is helpful. Additionally, a working knowledge of classical cryptography and traditional programming skills, such as C, provide IT professionals with an opportunity to experiment with post-quantum cryptography today. Examples of open-source, post-quantum software libraries include Open Quantum Safe and Microsoft Post-Quantum Cryptography.

CONCLUSION

It is unclear whether a large-scale, publicly accessible quantum computer is buildable, according to the NASEM report on quantum computing. Therefore, an accurate quantum computing development timeline is not currently possible. However, because public-key cryptography plays a vital role in the IT infrastructure of all enterprises, it is prudent to acknowledge the emerging cybersecurity risks posed by quantum computing and plan accordingly today.

The next few years are a critical period for this nascent, yet potentially transformational, technology. Monitoring the development of quantum computing stack, the standardization of post-quantum cryptography by NIST and the implementation of alternative cryptographic methods is imperative for all stakeholders. Although a quantum computer capable of cracking RSA will likely not arrive for another decade or more, the consequences of inaction are so dire that cybersecurity professionals and decisionmakers should plan and act now.