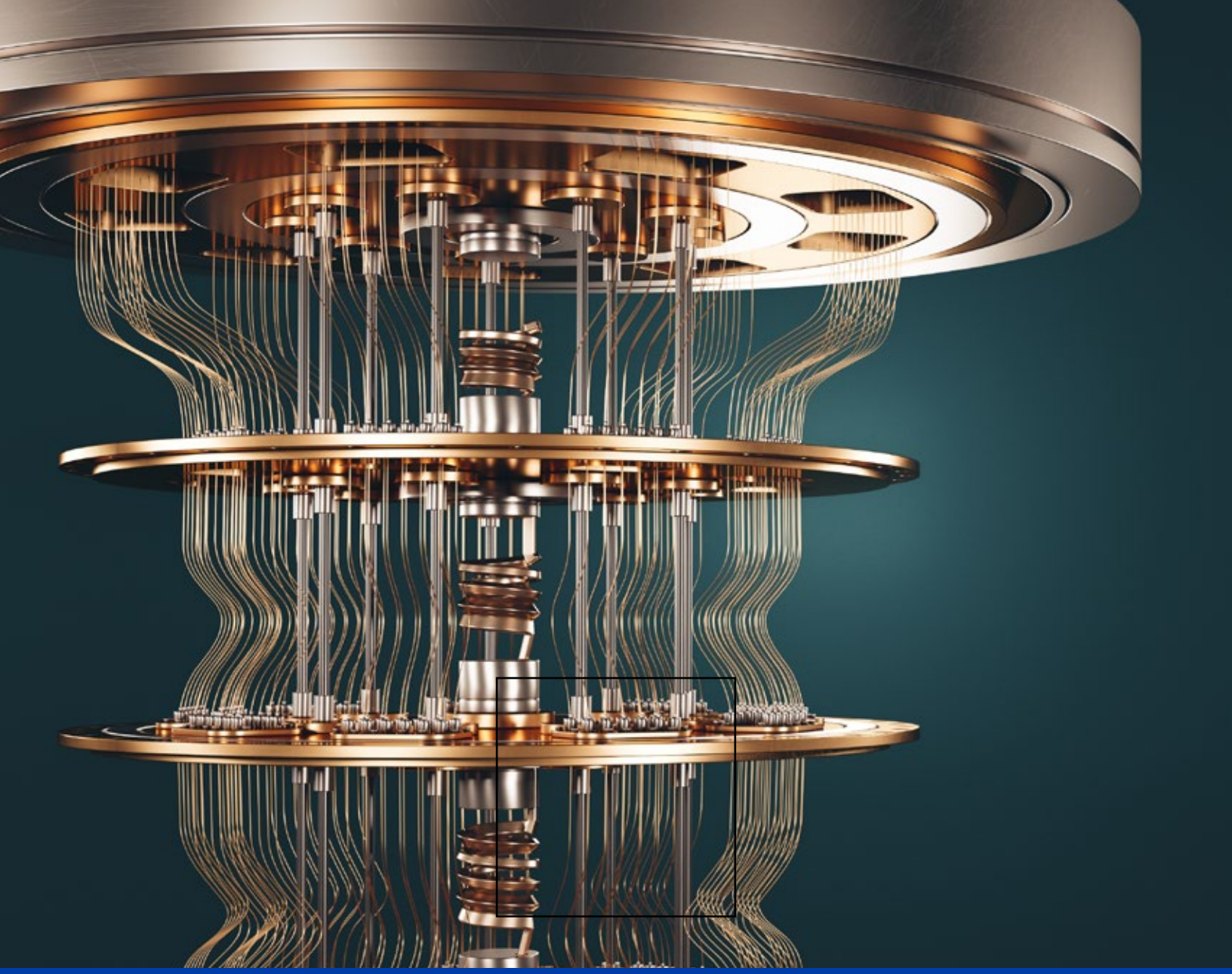


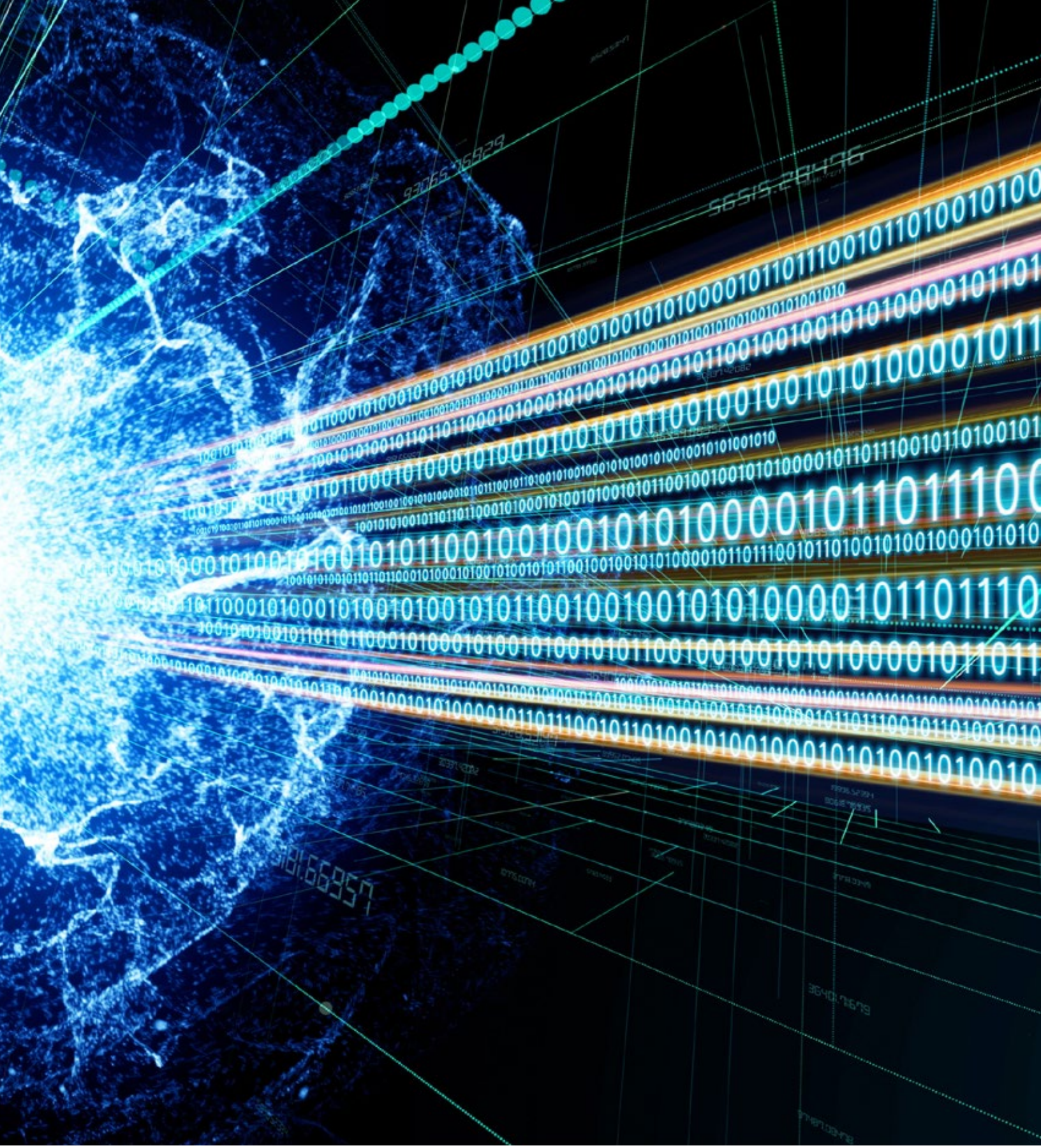
# THE EMERGENCE OF POST-QUANTUM CRYPTOGRAPHY

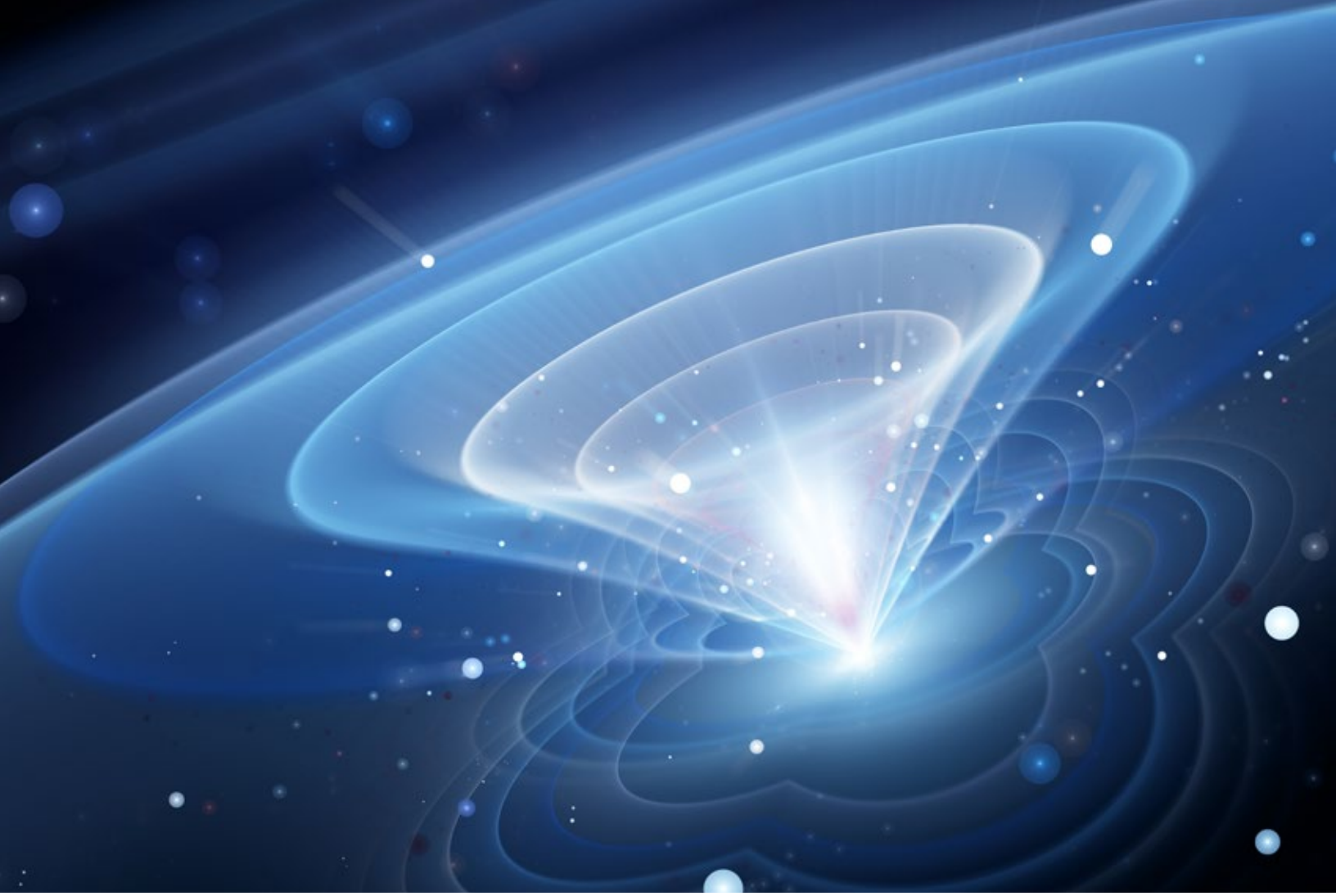
# A NEW COMPUTING ERA INTRODUCES SECURITY CHALLENGES

The prospect of quantum computing triggers a fundamental shift in computing and security principles. A quantum computer has little in common with our everyday laptops; it is a "computer" in the sense that, upon a given input, it delivers an output. However, the similarities stop there. Quantum computing devices exist today, and innovation is happening quickly. A general-purpose quantum computer is able to perform certain complex calculations that are intractable to the strongest supercomputers we can build. These calculations can solve optimization problems with potential breakthrough applications in areas such as GPS, metrology, pharmaceutical research, and machine learning.

From a security point of view, such a device will render most, if not all, of today's public-key cryptography useless. Accordingly, the long-term security of encrypted information and digital signatures could be compromised.

Although a significant amount of innovation must occur for mass adoption of quantum computing, the eventual impact it will make to society is difficult to overstate. The impact will extend across every cyber-connection imaginable, including the Internet we have grown to trust every day, from our online purchases to our private photos shared with friends. This prospect has led to widespread initiatives to develop new cryptographic algorithms, standards, and migration paths — collectively referred to as "post-quantum cryptography" (PQCrypto) — to secure against the emerging threat quantum computing presents. PQCrypto can run on classical computing hardware found in devices we use today and does not require a quantum computer.





## QUANTUM CRYPTOGRAPHY AND QUANTUM SUPREMACY

Quantum computers make use of quantum-mechanical properties such as superposition and entanglement to manipulate quantum bits (so-called "qubits") by quantum gates. Bit by qubit there has been a slow but steady progress, from the first experimental demonstration of a quantum algorithm working on 2 physical qubits in 1998, through 12 qubits in 2006, to Google's 72-qubit quantum chip in 2018.[123] This progress aligns to Neven's Law: the observation that quantum computers are gaining computational power at a double exponential rate, which is more aggressive than Moore's Law.

To put this into perspective, almost 10,000 logical qubits are required to break RSA-3072.[4] RSA is currently one of the most widely used public-key cryptographic schemes to protect our daily life.

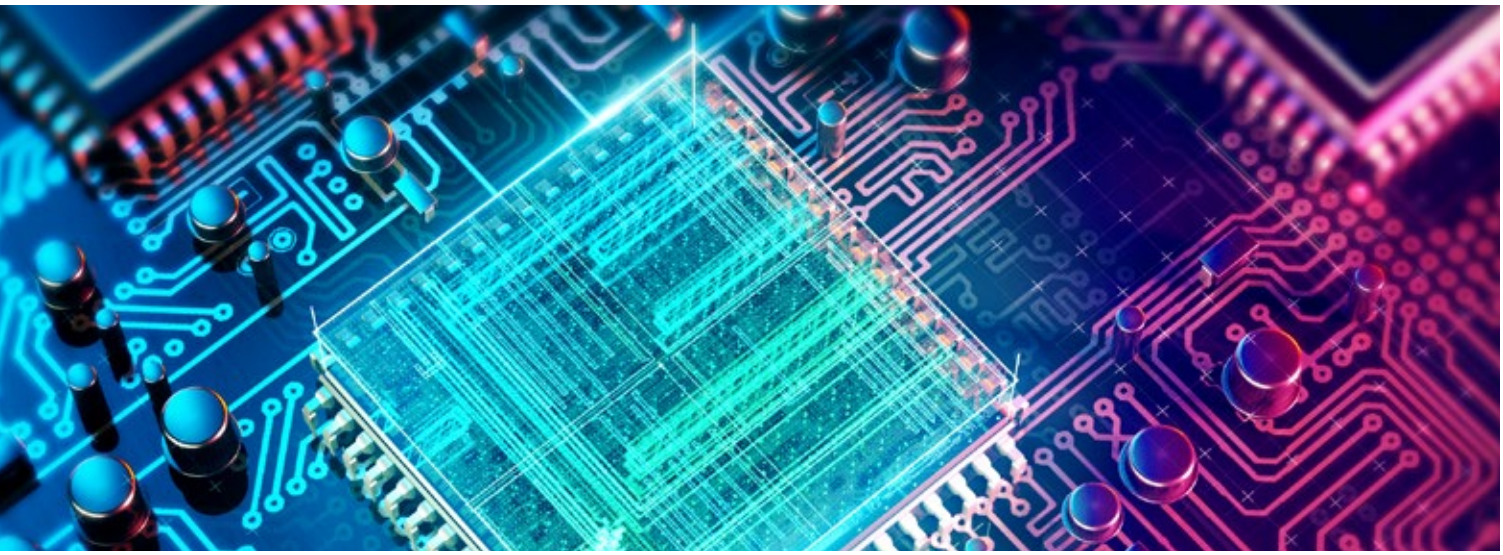
The term "quantum cryptography" is often used to refer to the implementation of cryptographic protocols based on quantum-mechanical principles, and it is not necessarily referencing the use of a quantum computer. The best-known example is a technique called quantum key distribution (QKD), in which a provably secure link between two parties is established by an exchange of polarized quantum particles such as photons over a fiber optic link. This method has been used in applications since as early as 2007, when it was used to establish secure links carrying voting results in the Swiss national election.[5]

One important milestone in quantum computing is quantum supremacy: solving a problem that no classical computer can feasibly solve. Google claimed to have achieved this in October 2019 by performing a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete on an array of 54 qubits.[6] However, this claim was not without controversy. IBM suggested the computation on a classical computer could be done in 2.5 days. In December 2020, physicists from the University of Science and Technology of China introduced a new technique with their quantum computer named Jiüzhãng, which resulted in another claim to quantum supremacy. Using one of the world's most powerful supercomputers available today, the computation performed is estimated to take a staggering 2.5 billion years. If the trends in quantum computing innovation continue, we may see quantum computations capable of solving real-world cryptographic problems in 10 to 15 years.


Quantum computing could significantly impact society's ability to secure the IoT and other Internet-based devices and infrastructure that use current cryptographic systems. If sufficiently powerful quantum computers become available in the future, systems and solutions that are regarded as reasonably secure today may be weakened or fully broken and the data and code contained within these systems could be compromised. As with other innovations, the first publicly demonstrated attacks may come from the academic community. Some of the potentially disruptive threats include:

- Confidential email messages, private documents, and financial transactions regarded as reasonably secure today may be compromised at some point in the future, even if they have been recorded and encrypted at the original time of communication.
- Firmware update mechanisms in a vehicle may be circumvented and allow dangerous modifications to be installed.
- Critical industrial and public service infrastructure for healthcare, utilities, and transportation that use the Internet and virtual private networks could become exposed, potentially destabilizing cities and creating other dangerous security breaches.
- The audit trails and digitally signed documents associated with safety, e.g., automobile certification and pharmaceutical authorizations, could be retrospectively modified or forged.
- The integrity of blockchains could be retrospectively compromised, which could even include fraudulent manipulation of ledgers and cryptocurrency transactions.

Even if immediate actions were taken to secure the Internet and IoT devices and infrastructure, it is not possible to mitigate the impact entirely. For instance, security keys issued today that are in use throughout the next two decades may be compromised when quantum computers become available. By definition, this security threat is different from many other security threats because legacy keys are not patchable, and as will often be the case, neither are legacy devices.



# THE RACE TOWARD POST-QUANTUM CRYPTOGRAPHY

Cryptography provides the building blocks to security. Determining appropriate key lengths is a difficult task. Large cryptographic key sizes offer increased computational security at the expense of performance and bandwidth.

This is where standardization bodies such as the USA's National Institute of Standards and Technology (NIST) or the German Federal Office for Information Security (BSI) play a role. By considering the use cases and assets that need to be protected, as well as the state-of-the-art mathematical research intended to break the cryptography and the anticipated increases to compute capabilities, many governing bodies are recommending fit-for-purpose key sizes for the next 10, 15, and 20 years. (See more details at keylength.com.)

With an increase of quantum computing capabilities, we can expect current public-key cryptography to be broken within the coming decade(s). For this reason, federal agencies have started issuing guidance to prepare for the potential crypto-apocalypse.

To avoid global economic impact due to the inherent reliance of our society on cryptography, a search for replacement cryptographic standards was started in a competition format by NIST in 2016.

### PQCRYPTO TIMELINE

**1994:** Peter Shor publishes a quantum algorithm to break the public-key schemes RSA and ECC in polynomial time.[7]

**1996:** Lov Grover publishes an efficient quantum algorithm to invert a function. Practically, this means all symmetric cryptographic schemes need to double their key sizes to achieve the same level of security against a quantum attack.[8]

**2006:** Traction from academia. The first PQCRYPTO conference was held in Leuven, Belgium.[9]

**AUGUST 2015:** The NSA announces preliminary plans for transitioning to quantum resistant algorithms in "the not too distant future."[10]

**APRIL 2016:** NIST announces they will lead the effort for a PQCrypto standard.[11]

**JULY 2016:** Google experiments with PQCrypto in the Chrome browser.[12]

**NOV 2017:** NIST round 1 for the new standard starts with 69 algorithms.[13]

**JUNE 2018:** Microsoft releases VPN with PQCrypto support.[14]

**JULY 2020:** NIST final round for the new PQCrypto standard. Two out of four key-exchange finalists are co-authored by NXP security experts.[15]

Contrary to previous cryptographic standardization competitions, NIST announced that there will not be a single winner: several algorithms will emerge as "good choices."[16] It is expected that each candidate algorithm will have some disadvantage, such as massive key sizes or increased latency. Otherwise, NIST would have considered a single algorithm for replacement already. Supporting multiple new cryptographic algorithms will have an enormous impact on existing public-key infrastructures as well as many products.

### MEASURING THE SECURITY THREAT

How long does your information need to be secure? **(X years)**

How long does deployment of a new crypto standard take? **(Y years)**

How long until there is a large-scale quantum computer? **(Z years)**

When **X + Y > Z** then we have a problem!

— ***Professor Michele Mosca***
*Institute for Quantum Computing*
*University of Waterloo, Canada*[17]

As quantum computing innovation and subsequent adoption is still evolving, how concerned should you be about the security threat?

## CONSIDER X-YEARS

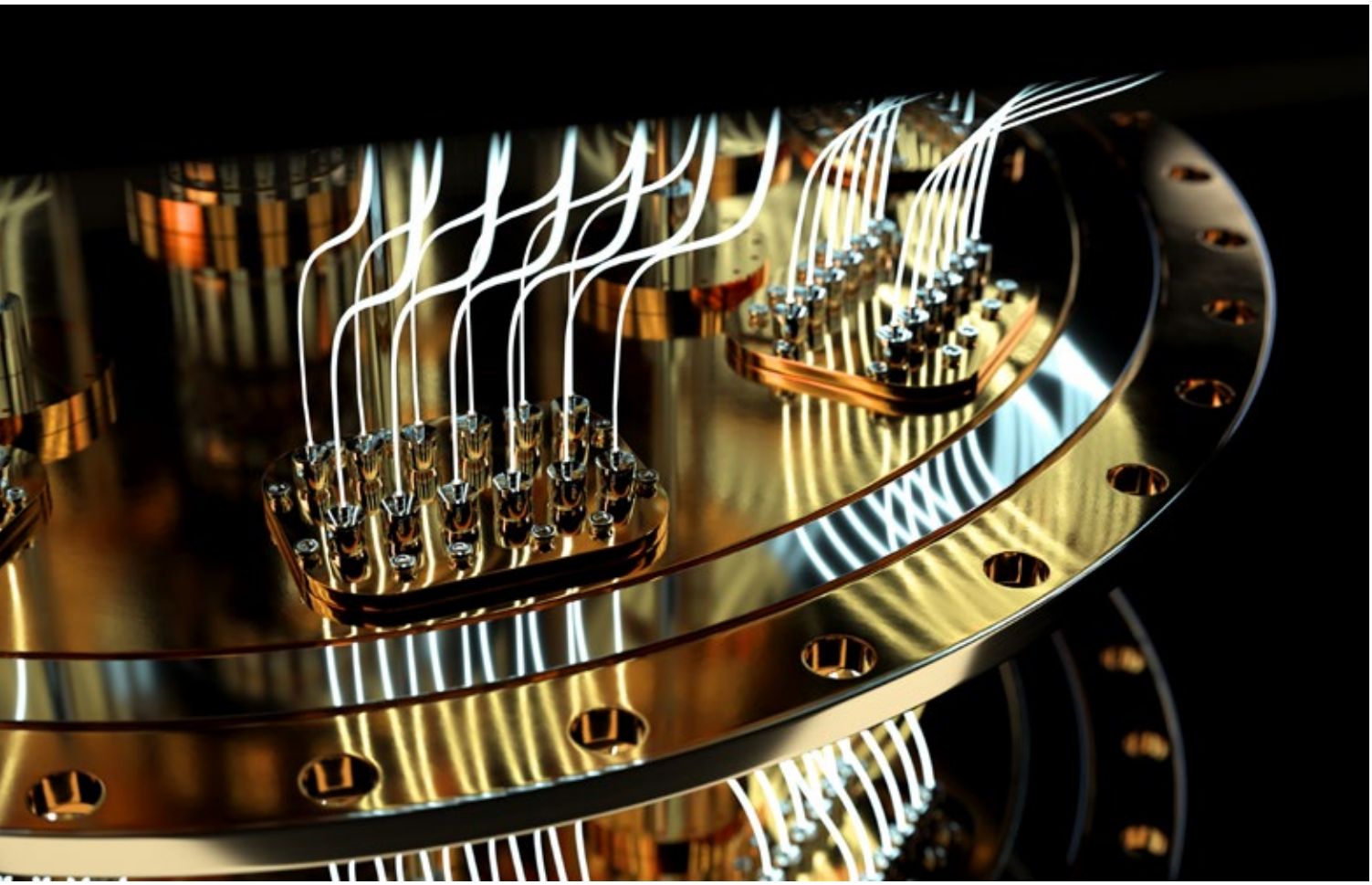
First, this will depend on how long the cryptographic keys — or the data protected by these keys — need to remain secure. This value X may vary from a short time span for session keys to very long periods in the case of sensitive data that is subject to application needs or government regulations.

## CONSIDER Y-YEARS

Second, this will depend on the time required to migrate to another cryptographic algorithm. This time Y can be relatively small if your software was designed with crypto-agility in mind. However, there is evidence that migrations take significant time. The seemingly straightforward migration from the old MD5 to the newer SHA-1 hash function took many years for some large software vendors, although the APIs are nearly identical.

Another example is the use of modern cryptographic standards in the finance and payment industry. It is expected that the majority of the infrastructure can only migrate to the Advanced Encryption Standard (AES) by 2030, which was standardized in 2001.

It is no no easy feat to migrate public-key cryptography with different key sizes, different computational requirements, and widely varying APIs. Furthermore, new countermeasures that guarantee adequate levels of physical security against side-channel and fault attacks must be developed. Additionally, this value Y should include the time for deploying the trust provisioning required for these new algorithms.



## CONSIDER Z-YEARS

Finally, the time Z denotes the expected time until a quantum computer capable of breaking currently deployed cryptosystems will arrive. Following the formulation of Professor Michele Mosca from the University of Waterloo, Canada, "if X + Y > Z then you have a serious problem" and immediate action should be taken. A wide range of estimates has been applied to Z, from "never" to "years" to the often-cited forecast of "within the next decade."[17]

Due to long-term roadmaps and practical difficulties in realizing crypto-agility, we already see industries preparing for these new cryptographic algorithms. Industries with long product lifetimes such as energy infrastructure, space technology, and avionics are investigating the impact of PQCrypto. For the design of some IoT devices and appliances, long-term security is already taken into account. Google tested the impact of PQCrypto on its infrastructure by experimenting with large scale deployment as early as 2016 and incorporating it into the cutting-edge version of its Chrome browser.[12] To guarantee security, the company used a hybrid approach; i.e., performing the post-quantum secure crypto on top of the classical one as currently standardized.

### *NXP's Effort Toward PQCrypto Standards*

Comprehensive security and cryptography expertise has led to NXP's involvement in the NIST PQCrypto standardization process. In July 2020, NIST announced the finalists for the PQCrypto standard: Two out of four key-exchange finalists were co-designed by NXP security experts.

In addition to semiconductor manufacturing, NXP has a strong history of providing solutions to ecosystems that require heightened security and privacy, including e-government, automotive, banking, industrial, and IoT.

NXP provides purpose-built, rigorously tested system solutions and services, including:

- Toolkits for our hardware, including secure boot capabilities and firmware update systems
- Cryptographic libraries, security subsystem firmware and operating systems
- Security services, including trust provisioning, secure deployment and management of devices
- Complete end-to-end security ecosystems

## *Considerations for System Solutions and Services*

Many of our products rely on classical public-key cryptography mechanisms to enable secure boot or provide secure software updates. These mechanisms are crucial when it comes to crypto-agility as they will handle the security upgrade to any future cryptographic standard. Depending on the product lifecycle, these mechanisms need to be secure for a long lifetime.

Apart from the new aspects of functional security of deploying PQCrypto, the adoption of new cryptographic techniques must encompass:

- Logical security: an attacker should not be able to bypass the security because of implementation bugs
- Physical security: an attacker should not be able to break the security by misusing physical behavior in a side channel or fault attack

### XMSS (EXTENDED MERKLE SIGNATURE SCHEME)

XMSS is the first standardized post-quantum secure signature scheme (RFC 8391, NIST SP800-208).[18,19] It is called a "stateful" scheme, which means templates for a fixed maximum number of signatures are computed in advance and later adapted after the messages to be signed are known. It is a completely different methodology with different processing and storage requirements from the classical process of signing each message as it becomes available. Furthermore, signature and key sizes are much larger than those in classical systems.

Support for new algorithms has a significant impact on many practical design parameters, including new key types and sizes as well as signature sizes and key exchange parameters. While the specific standard scheme(s) has not been identified, these facts will place stress on RAM and non-volatile memory requirements. This impact needs to be accounted for, not only in the product architectures, but also in the associated services.

This will result in a completely different approach to setting up and operating trust provisioning when, for example, the post-quantum secure digital signature algorithm XMSS is to be used. The complete flow from customer key intake or customer key generation until the final provisioning into silicon must take into account the fact that key sizes, signature sizes and parameter sizes are significantly different from existing RSA/ECC-based flows.

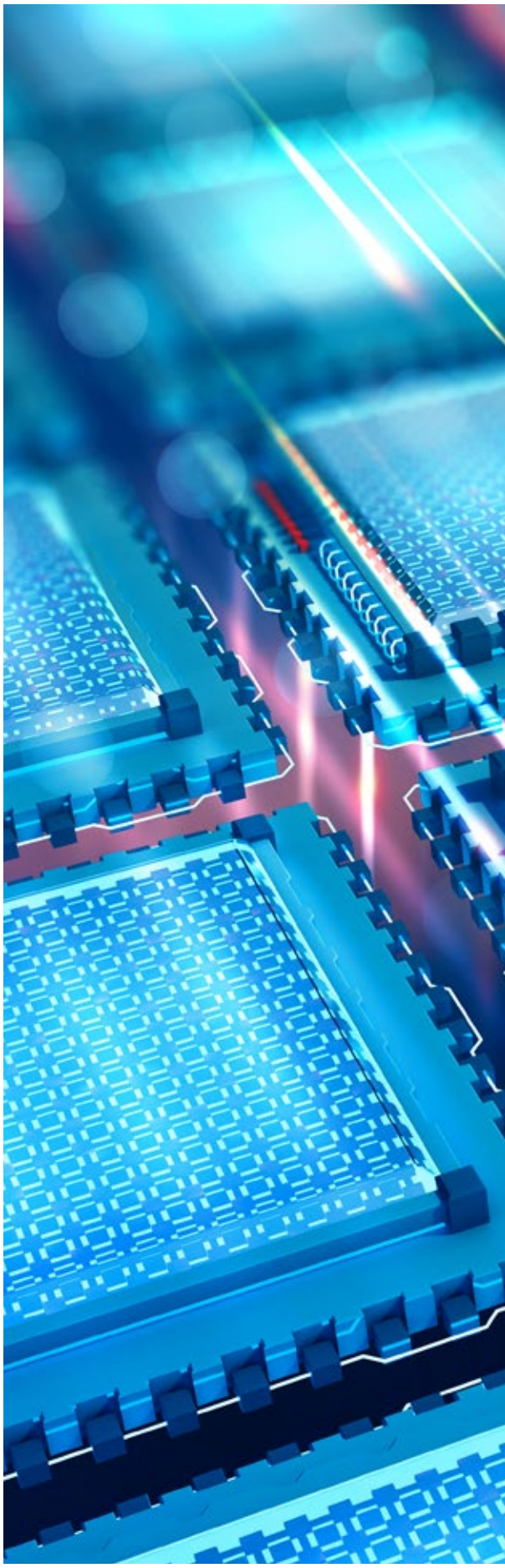
The U.S. government has outlined mitigations to be used while these new PQCrypto algorithms are developed and implemented into products. The Commercial National Security Algorithm Suite (CNSA Suite) allows one to transition to quantum-resistant algorithms. The proposed transition algorithms consist of the traditional approaches with larger key sizes and is already supported by many of NXP's products.

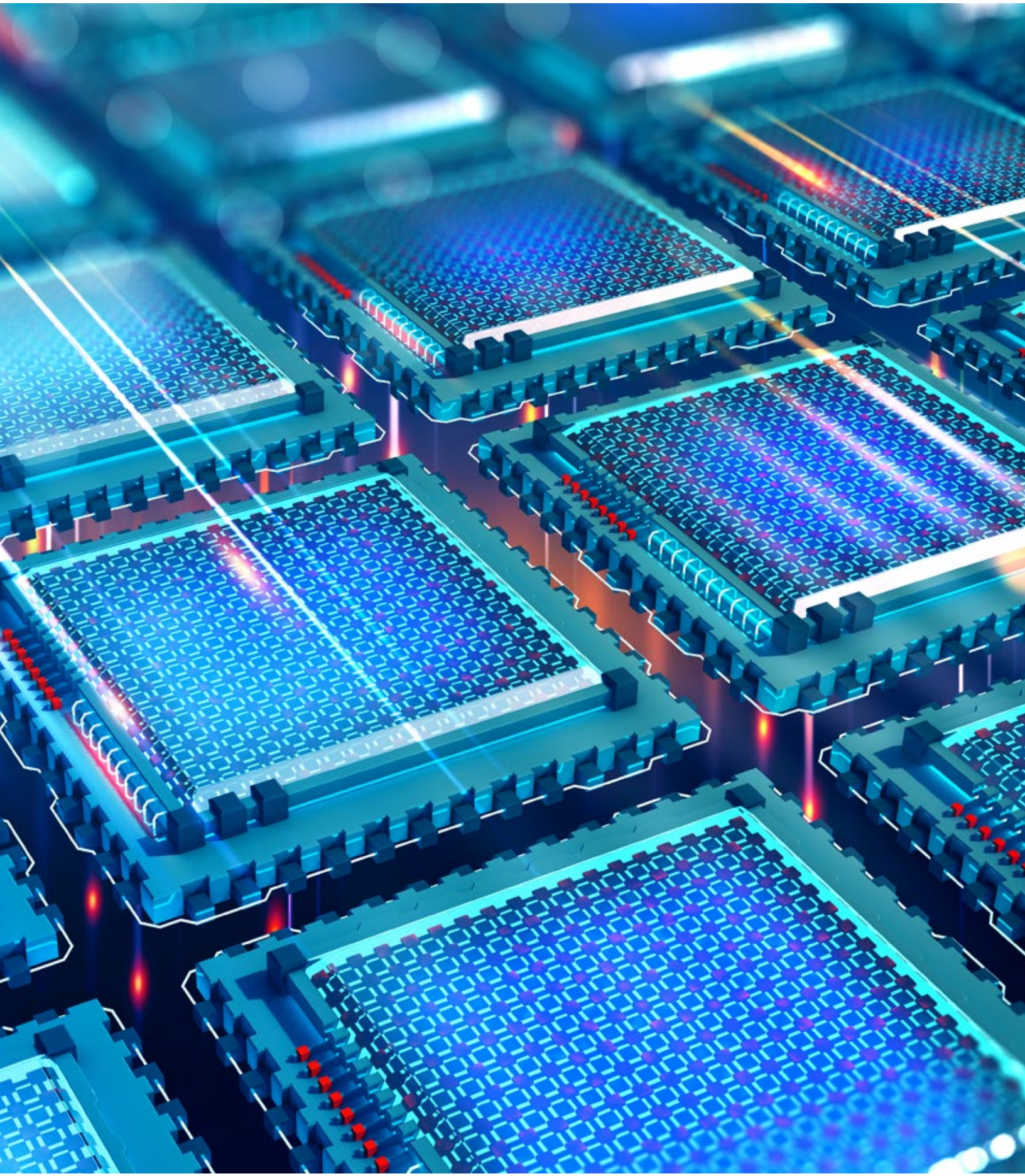
## OUR COMMITMENT

Although fundamental challenges remain and major breakthroughs might still be a while down the road, when quantum computing becomes a reality, it promises to bring us into a new computational era. Besides the positive effects on society, quantum computing also has a fundamental impact on the foundations of the security used today. The impact extends across security for the Internet, IoT devices, and legal infrastructure based on currently used cryptographic systems. Systems and solutions that are regarded as reasonably secure today may become weakened or broken when facing a quantum computer in the future.

As new public-key cryptographic standards emerge, migration to these new types of public-key cryptographic primitives will be a practical challenge due to the increase of the key-sizes, computational resources needed and higher memory requirements. Keep in mind that all past cryptographic transitions took significant amounts of time and effort — even for much simpler replacements. Preparing this transition now will ensure a smooth transition when the new standards are announced. NXP's security engineers and cryptographers are leading this transition by contributing to two of the current finalists in the NIST PQCrypto competition as well as ensuring that any upcoming PQCrypto standard takes core requirements of embedded security such as physical secure implementations and resource limitations into account.

NXP will strive to continue to ensure its products offer the long-term security protection to which our customers are accustomed. We are following the premise "the best way to predict the future is to create it."





# REFERENCES


1. Chuang, Isaac L., Neil Gershenfeld, and Mark Kubinec. "'Experimental Implementation of Fast Quantum Searching." *Physical Review Letters* 80, no. 15 (1998): 3408–11.
2. "12-Qubits Reached In Quantum Information Quest." ScienceDaily. ScienceDaily, May 8, 2006. https://www.sciencedaily.com/releases/2006/05/060508164700.htm.
3. Conover, Emily. "Google Moves toward Quantum Supremacy with 72-Qubit Computer." Science News, August 8, 2019. https://www.sciencenews.org/article/google-moves-toward-quantum-supremacy-72-qubit-computer.
4. Roetteler, M., Naehrig, M., Svore, K.M. and Lauter, K., 2017, December. Quantum resource estimates for computing elliptic curve discrete logarithms. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 241-270). Springer, Cham.
5. Greenemeier, Larry. "Election Fix? Switzerland Tests Quantum Cryptography." Scientific American. Scientific American, October 19, 2007. https://www.scientificamerican.com/article/swiss-test-quantum-cryptography/.
6. Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. *Nature* 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5.
7. Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." In Proceedings 35th annual symposium on foundations of computer science, pp. 124-134. Ieee, 1994.
8. Grover, Lov K. "A fast quantum mechanical algorithm for database search." In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212-219. 1996.
9. "Post-Quantum Cryptography." Accessed February 8, 2021. https://pqcrypto.org/conferences.html.
10. Commercial National Security Algorithm Suite. NSA/IAD. Accessed February 8, 2021. https://apps.nsa.gov/iad/programs/iad-initiatives/cnsa-suite.cfm.
11. Computer Security Division, Information Technology Laboratory. "Post-Quantum Cryptography: CSRC." CSRC. Accessed February 8, 2021. https://csrc.nist.gov/projects/post-quantum-cryptography.
12. Langley, Adam. Accessed February 8, 2021. https://www.imperialviolet.org/2016/11/28/cecpq1.html.
13. Computer Security Division, Information Technology Laboratory. "Round 1 Submissions - Post-Quantum Cryptography: CSRC." CSRC. Accessed February 8, 2021. https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions.
14. "Post-Quantum Cryptography VPN." Microsoft Research, September 14, 2020. https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn/.
15. Computer Security Division, Information Technology Laboratory. "Round 3 Submissions - Post-Quantum Cryptography: CSRC." CSRC. Accessed February 8, 2021. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.
16. Computer Security Division, Information Technology Laboratory. "Post-Quantum Cryptography: CSRC." CSRC. Accessed February 9, 2021. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs.
17. Mosca, Michele. "Cybersecurity in a Quantum World: Will We Be Ready?" CryptoWorks21, University of Waterloo, April 03, 2015.







Document Number: POSTQCRYPTOWP REV 0