AGILEPQ

A Guide to Post-Quantum Security for IoT Devices

Q3 2019

Table of Contents

Abstract

> *A sufficiently large quantum computer, if built, would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures.*
>
> *-National Security Agency*[1]

This white paper provides a detailed outline of the key issues facing the cryptography community, and the broader business community, in regard to the potential of quantum computing and the Internet of Things (IoT). The target audience is technical and non-technical executives, with supporting research to inform the curious reader.

The *Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity*[2] provides guidance and solutions to CEOs and CIOs regarding what quantum computers are, what they threaten, and how to prepare today, such that quantum computing does not disrupt the security and integrity of critical data. This report will expand on these threats and the technologies that businesses must begin migrating today amid anticipated exponential, and perhaps even super-exponential, growth in quantum computing in the years ahead.

[1] National Security Agency. (January 2016). *CNSA Suite and Quantum Computing FAQ.*

[2] Herman, A. (2019). The Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity, Hudson Institute Quantum Alliance Initiative.

The Quantum Initiative

It's not a Turing machine, but a machine of a different kind.
-Richard P. Feynman, Nobel Laureate

On August 30, 2019, the President of The United States established the National Quantum Initiative Advisory Committee through Executive Order[3]. This advisory committee oversees the National Quantum Initiative Act, which became public law on December 21, 2018. The purpose of the Quantum Initiative Act is to "provide for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States"[4].

The impetus for the legislation is recognition of the importance of quantum computers and quantum technologies in general, and the need for America to be a leader in this emerging technology. As Herman has noted, there are vital national security issues associated with the development of quantum technologies.

A number of corporations, such as Google, Microsoft, IBM, D-Wave, and Rigetti are quickly moving towards the threshold of "quantum supremacy" [5] [6]. Quantum supremacy is said to be achieved when a quantum computer is able to perform a certain task that no classical (i.e., traditional transistor-based digital) computer can solve in a practical amount of time or using a practical amount of resources[7].

U.S. researchers and companies are not the only ones pursuing this goal of quantum supremacy. In 2017, China announced that it was opening a quantum research supercenter, with an investment of $10 billion[8]. Total investment in quantum technologies in China today is approaching $16 billion. The European Union is also promoting quantum research, as is the United Kingdom, but on a much more limited basis than China.

[3] White House. (2018). Executive Order on Establishing the National Quantum Initiative Advisory Committee. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-establishing-national-quantum-initiative-advisory-committee/

[4] 115th Congress. (2018). H.R.6227 - National Quantum Initiative Act. Washington D.C. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/6227/all-info

[5] Knight, M. G. (2019). Google thinks it's close to "quantum supremacy." Here's what that really means. MIT Technology Review. Retrieved from https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/

[6] Hruska, J. (2019). IBM Preps 53-Qubit Quantum Computer for Launch in October. Extreme Tech. Retrieved from https://www.extremetech.com/computing/298719-ibm-preps-53-qubit-quantum-computer-for-launch-in-october

[7] Deloitte. (2019). Technology, Media, and Telecommunications Predictions 2019. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/TMT-Predictions_2019/DI_TMT-predictions_2019.pdf

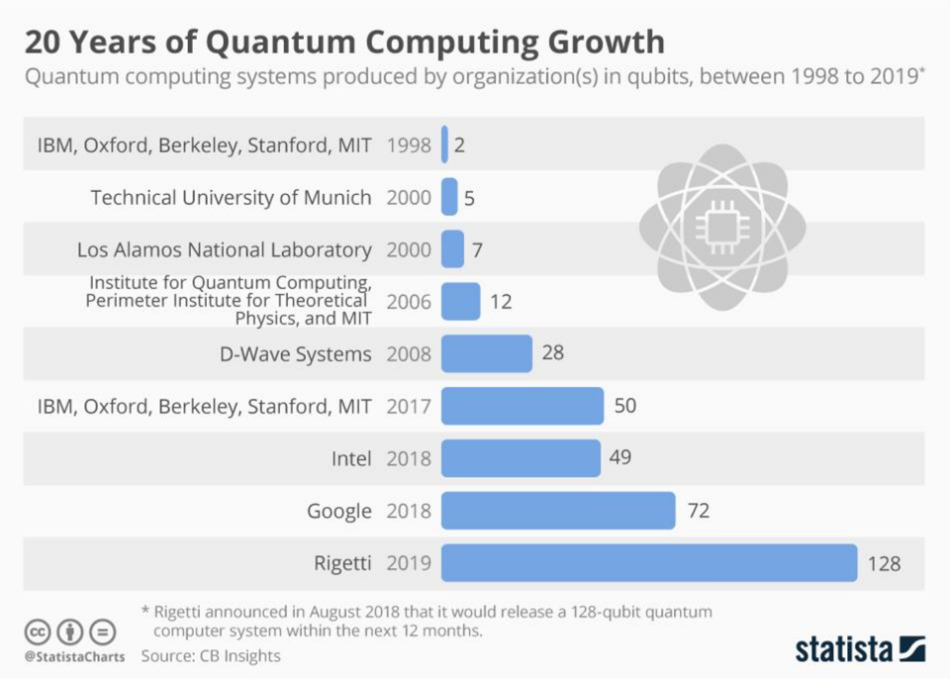
[8] Jeffrey Lin, P. S. (2017). China is opening a new quantum research supercenter. Popular Science. Retrieved from https://www.popsci.com/chinas-launches-new-quantum-research-supercenter/

Quantum Supremacy

> *If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use.*
> *-National Institute for Standards and Technology*

The idea of a quantum computer was first proposed in 1981 by renowned physicist Richard Feynman[9]. These quantum machines are capable of "simulating physics," and they do not operate at all like the computers we use today. Instead, they leverage the properties of quantum-electro-dynamics to perform computations far outside the realm of standard computers. This means that a quantum computer with sufficient quantum bits, or qubits, can find solutions to problems that are difficult, even intractable, for classical computers.

Quantum computing technology is advancing at an accelerating pace. In 1998, researchers at IBM, Oxford, Berkeley, Stanford, and MIT produced a 2-qubit computing system. By 2018 Google confirmed that it was able to produce a 72-qubit computing system. Rigetti announced it would be going further than that, releasing a 128-qubit system within the year[10].



* Rigetti announced in August 2018 that it would release a 128-qubit quantum computer system within the next 12 months.

Source: CB Insights

Figure 1. 20 years of Quantum Computing Growth

[9] Feynman, R. P. (1981, 05 07). Simulating Physics with Computers. Retrieved from https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf

[10] Feldman, S. (2019). Manufacturing.net. Retrieved from https://www.manufacturing.net/data-focus/2019/05/20-years-quantum-computing-growth

Classical Cryptography

The term "classical cryptography" in this document refers to today's modern security standards - in use today - which protect data confidentiality, and which are threatened by quantum computing attacks. Classical cryptography refers to ciphers that have fallen into disuse because of known attacks discovered by cryptanalysts that circumvent their security.

A cryptosystem is a suite of cryptographic primitives which provide guarantees such as authentic digital signatures, data integrity, data confidentiality, forward secrecy, and trust in a digital world.

Cryptography Definitions and Terminology

Components are talked about in terms of three primary categories:

1. Hashes
2. Public/private key (asymmetric) cryptography
3. Private key (symmetric) cryptography

A cipher is a symmetric component which encrypts data by using "key material" – a secret possessed by both parties that is not feasible to guess. This secret can be exchanged hand-to-hand, but on the internet, this is not feasible. A cipher utilizing a truly random one-time-pad the same length as the message is known to have perfect information-theoretic secrecy; however, the ciphers in-use today use some form of cryptographically secure random number generation based on a key that is much smaller than the length of the message.

Key exchange methods and digital signatures are asymmetric components which allow two remote parties to establish key material and verify identity. A cryptosystem, or cryptographic protocol, combines these elements to create a robust and secure communication system over the Internet.

Numerous methods exist for each category and these methods are chosen because of their mathematical "hardness." This means that to find the solution of the problem, it requires either a large amount of space (memory), or time (computational cycles), and the time or space required exceeds that of a lifetime and the available computing power in the universe.

All encryption in use today relies on certain mathematically hard problems. Unfortunately, and problematically for businesses, governments and individuals that rely on them, these are the exact types of problems that are efficiently solved on a quantum computer.

The one cipher used in nearly all standards today – Advanced Encryption Standard (AES) – was proposed in 1997 in a NIST competition and standardized in 2001 as a replacement for the broken Data Encryption Standard (DES)[11]. The key exchange mechanism – Rivest Shamir Adelman (RSA) – was standardized for use on government systems through NIST Special Publication 800-15. Elliptic Curve Cryptography (ECC) was proposed as an improvement to RSA systems in 2015 and is part of the Federal Information Processing Standards (FIPS) 186.

In 1994, American mathematician Peter Shor, while working at Bell Labs, developed a new algorithm. Shor's Algorithm is a quantum computing algorithm which efficiently solves the prime factorization and discrete logarithm problem which underpin RSA and ECC. Grover's Algorithm is a

[11] NIST. (2001). Cryptographic Standards and Guidelines. Retrieved from NIST: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

quantum computing algorithm which reduces the difficulty of finding a pre-image attack on a symmetric cipher such as AES, reducing the difficulty by a factor of a square root.

It is straightforward, for example, to multiply two large numbers together. However, given a large number, it is "mathematically hard" to find those two numbers, or "prime factors." This is known as the prime factorization problem. Another cryptographic building block is the discrete logarithm problem in use by Elliptical Curve Cryptography.

Apart from the discrete logarithm and prime factorization problems, one mathematically hard problem is the *black-box-output problem* – finding the unique input of a black box which produces a particular output. This difficult-to-solve problem is the basis for symmetric ciphers and hashing algorithms that protect confidentiality and integrity of data and is commonly referred to as a pre-image attack. If an adversary knows the ciphertext and the steps of the algorithm, a pre-image attack reveals what the inputs were that produced the ciphertext: the key and the message.

The Quantum Threat to Security

> *"Quantum is going to get us to a point where we're going to have to rethink encryption."*
> *-Rep. Will Hurd (R-Texas)*

Peter Shor was the first to discover that quantum computers could be used for efficiently solving certain types of mathematically hard problems[12]. This research was groundbreaking, and the implications were eye-opening to mathematicians and cryptographers around the world. Shor's research was published in the 1990's, and it motivated many researchers to expand on and discover new quantum attack techniques.

The researcher Lov K. Grover invented a "fast quantum mechanical algorithm for database search"[13], which showed that quantum computers could find solutions faster than classical computers by orders-of-magnitude for certain types of searching problems, i.e. the black-box-output problem. Many other researchers, such as Daniel R. Simon, have invented other unique ways to leverage quantum-computation to solve traditionally hard problems.

Why Do Quantum Attacks Matter?

Since the first cryptographic ciphers were put into use, the breaking of these codes became a top priority for adversaries wishing to gain access to critical information. Ciphers such as Caesar, Vigenère, Enigma, and more recently RC4, DES, SHA1, were thought to be permanently unbreakable; however, codebreakers constantly search for ways to break the unbreakable. During the second World War, a U.S. spy revealed to the Germans that the Enigma was broken and that British codebreakers were reading the messages. The Germans were so convinced that the Enigma was unbreakable that they ignored this warning[14]. The NSA has issued warnings[15] that common

[12] Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. doi:10.1.1.123.5183

[13] Grover, L. K. (n.d.). A fast quantum mechanical algorithm for database search. Retrieved from https://arxiv.org/pdf/quant-ph/9605043.pdf

[14] Ralph Erskine, M. S. (2001). Action This Day. Bantam Press.

[15] National Security Agency. (2016). CNSA Suite and Quantum Computing FAQ, January 2016

encryption in use today, such as AES128, is threatened, but the industry has made no movement towards change.

All the critical, secret, and important data on the internet is protected through the applications of cryptography. The goal of cryptography is to allow only the intended party to read the information by keeping it confidential, to prove the information has integrity, to validate the identity of the party is authentic, and establish a trusted communication channel between two or more parties.

Shor's algorithm and Grover's algorithm show that the classical methods and standards in place today must change in the near term to avoid a major disruption. The following table outlines the core classical cryptography components in use by all secure communication protocols today.

Component Name	Category	Function	Attack	Security Functions
RSA / ECDH / DH	Asymmetric	Key Establishment	Shor's Algorithm	Forward Secrecy Secure Key Establishment Identity Proof
DSA / ECDSA	Asymmetric	Digital Signature	Shor's Algorithm	Identity Verification Data Integrity Signature Non-repudiation
AES / 3DES / ChaCha20	Symmetric	Data Encryption	Grover's Algorithm	Confidentiality
SHA-*	Symmetric	Hashing	Grover's Algorithm Simon's Algorithm	Integrity

Figure 2. Classical Cryptographic Components

The following table quantifies the security levels for the most used cryptographic schemes today[16]:

Crypto Scheme	Key Size	Classical Computing Effective Key Strength/Security Level (in bits)	Quantum Computing Effective Key Strength/Security Level (in bits)
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	128	128	64
AES-256	256	256	128

Figure 3. Security on Classical and Quantum Computers

Lifetime of Data Protection

Cryptography underpins nearly all security features across all electronic devices. From trusting and verification on websites, transacting with the blockchain, securely transmitting banking information, discussing sensitive matters with family, and protecting intellectual property from getting into the hands of competitors. Cryptosystems provide the security and guarantee that this information is safely protected today and in the future.

Corporations use cryptography daily to authorize front-door entry with badges, broadcast video meetings, allow workers to securely connect through VPNs, digitally interface with customers and vendors and sign corporate documents. Virtually every aspect of day-to-day operations for a modern company. Governments use cryptography with greater impact; from transmitting code-

[16] Vasileios Mavroeidis, K. V. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, Vol 9, No 3.

word instructions to spies and nuclear submarines, coordinating troops on the ground, to protecting the communications of world leaders and government organizations.

The protection of these operations and information is critical, and some data must be protected for a longer time due to its sensitive nature. With proper planning and proactive decisions by leadership, the risk of a data compromise or disruption of service is nearly eliminated.

The time to transition to new security technologies, plus the time that the data must be protected, must be less than the time that quantum computers are expected to compromise security[17]. This threshold has already been surpassed. It has taken nearly 20 years to migrate to new security systems in the past[18]. With quantum computers expected to grow exponentially more powerful within the next two decades, today is the zero day for shifting to a new quantum-safe security paradigm.

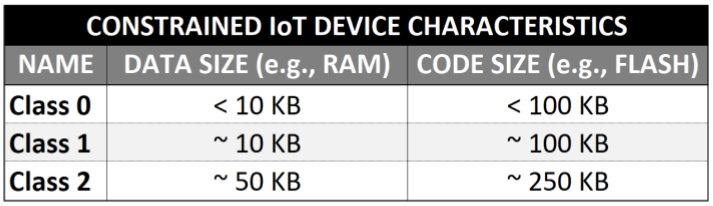
Unless action is taken immediately to move towards quantum-safe technologies, it is expected that data communications from this point forward will be subject to attack and vulnerable. By beginning the transition today, individuals, corporations, and governments will avoid the costly liabilities and risks that are imminent with the quantum age.

The Rise of IoT

The Internet of Things (IoT) reflects the growing use of the Internet. Far more devices or things are connected to the Internet today than people, and this trend is projected to continue in the future.

As IoT continues to proliferate, allowing huge amounts data to be collected that has never been collected before. Examples include radiation and other sensors in nuclear power plants, temperature controls in the home, traffic and automotive controls, smart cities, medical devices, and other monitoring devices. This adoption is happening at a faster pace than any other technology in history.

Projections show that many of these devices are very small, constrained devices. The terminology defined in IETF RFC 7228[19] categorizes these constrained devices in the following table, with KB denoting Kilobyte.



CONSTRAINED IoT DEVICE CHARACTERISTICS		
NAME	DATA SIZE (e.g., RAM)	CODE SIZE (e.g., FLASH)
Class 0	< 10 KB	< 100 KB
Class 1	~ 10 KB	~ 100 KB
Class 2	~ 50 KB	~ 250 KB

Figure 4. Constrained Device Terminology

[17] Mosca, M. (2015). Cybersecurity in an era with quantum computers: will we be ready? International Association of Cryptologic Researchers, 1075.

[18] NIST. (n.d.). Post-Quantum Cryptography. Retrieved from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[19] IETF. (2014, May). Terminology for Constrained-Node Networks. Retrieved from https://tools.ietf.org/html/rfc7228

As the chart below shows, the greatest number of connected IoT devices in the future are those with ~100 KB or less available storage, and very limited in-memory constraints.

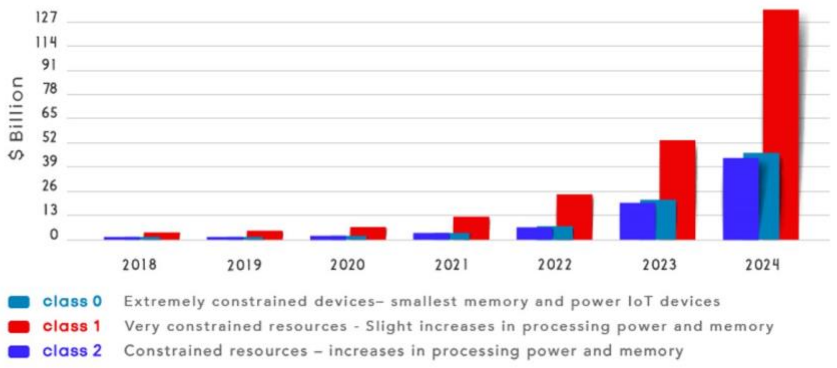


Figure 5. Projection of the number of IoT devices through 2024

IoT Challenges

The transition to quantum-safe security will require a longer upgrade cycle for certain manufacturers and device designers; primarily those that implement classical cryptography in hardware. This includes the uplink connection to modern vehicles, cellular SIM cards, credit card chips, two-factor authentication tokens, and constrained Internet of Things devices.

The existing cryptography suites, such as TLS, were designed for traditional computing devices and servers, and their code size and processing requirements are far too great for constrained devices. Existing security standards such as RSA and ECC require relatively expensive mathematical operations, and AES requires much more battery power and computations than more efficient ciphers.

None of the existing standards were designed with constrained devices in mind; however, due to the requirement of using standards, it is all that is available. This creates a situation that leaves designers without options and without security. Commercial lightweight cryptography options face resistance of adoption because there is no standard, and this creates an unnecessary barrier for the industry to move forward.

Furthermore, the lack of “freely available” lightweight cryptography protocols, combined with the lack of cryptography expertise of device designers, means that existing protocols cannot be adapted to these devices. Thus, they are left unprotected.

A major challenge is that many devices have already been deployed – brownfield deployments – and are already in use today with no security. Greenfield deployments – those devices being deployed into service today – often lack security for the aforementioned reasons as well. The challenge does not only rest in securing greenfield devices; there must be a way to secure existing brownfield devices in the field via firmware updates.

The adoption of these devices, and the speed of innovation, far outpaces the ability of standards bodies to offer suitable lightweight quantum-resistant encryption standards in time for deployment. The challenge is how to incentivize and empower private companies who specialize in cryptography to adopt new and innovative techniques at the speed of the market.

One major challenge that must be solved is how to make companies responsible and willing to spend the money on the security of their devices and networks. Today, entities are unwilling to invest in cybersecurity because of the lack of Return on Investment, and the low visibility that cybersecurity has in day-to-day operations, until an attack happens. Legislative and legal bodies are beginning to pass laws and regulations to incentivize secure designs, and this must continue and gain support throughout the industry.

Towards Quantum-Safe Security

> *"The quantum-safe security industry is also likely to be worth hundreds of millions of dollars per year in the 2020s ... Enterprises and governments should start protecting against the threat of powerful QCs today, not when it happens, since by then it will be too late."*
>
> *-Deloitte*[20]

The emphasis on the post-quantum migration has solely focused on key exchange methods and digital signatures[21], and has overlooked the need to migrate to post-quantum symmetric ciphers. In January 2016, NSA issued a notice to stop using AES-128 and to switch immediately to AES-256[22]. AES-128 is a de facto standard in use by millions of devices, and it is the basis of Bluetooth security[23] and many other protocols. Hardware manufacturers also offer on-chip implementations of AES-128 to increase efficiency of devices. In order to migrate to post-quantum security, new hardware designs of devices must begin to enter the market today.

An often-repeated statement is to simply "increase the key size of AES," but the research of how this can be done has only just begun[24]. This upgrade is no more trivial than entirely replacing AES, and any standardization process will take significant time. This is a prime opportunity to rethink how we do encryption. Increasing from 128- and 256-bit keys for AES will further decrease the efficiency of devices, and this will be a major impact to constrained devices. A coherent approach and cooperation across industry and government verticals is required to upgrade software and hardware to meet new encryption demands.

NIST has not moved yet to search for new symmetric ciphers, and the typically multi-year long standardization process for a new version means today's data is at risk for the next number of years. Researchers at universities are investigating ways to create quantum-resistant cryptography; however, they are not the same ones that get paid to integrate algorithms into software and deployments for corporations and governments.

[20] Deloitte. (n.d.). Technology, Media, and Telecommunications Predictions 2019. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/TMT-Predictions_2019/DI_TMT-predictions_2019.pdf

[21] NIST. (n.d.). Post-Quantum Cryptography. Retrieved from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[22] National Security Agency. (n.d.). CNSA Suite and Quantum Computing FAQ, January 2016

[23] NIST. (2012). Special Publication 800-121 Revision 1. NIST.

[24] John Gregory Underhill, S. A. (2019). Towards post-quantum symmetric cryptography. International Association of Cryptologic Research.

Companies and private non-governmental entities have already begun developing and innovating in the space of post-quantum cryptography[25] [26], and patents have been generated around several post-quantum implementations. However, major difficulties arise when attempting to sell these cutting-edge solutions because of the refusal of some corporations and governments to use "non-standard" technology. So, we are at a standoff where we have solutions, but we are unable to deploy them today.

An objection, and one stated at the beginning of any course in cryptography, is "never roll your own crypto." This objection is disingenuous: who, then, is allowed to innovate with cryptography? Great ideas are not restricted to university halls; however, the standardization process exclusively pulls from this body of innovation. The standardization bodies need to leverage the expertise of private entities and facilitate the standardization of intellectual property into standard offerings, while guarding the ability of a company or individual to protect their invention.

Not all nations on the Internet are good willed towards respecting patents or inventions, and the current standardization process requires a full revelation of proprietary information to the entire world. This is a fundamental issue in the current cryptographic standardization process. Furthermore, it can put individuals and corporations at risk of violating the International Traffic in Arms Regulations because of the export classifications by the Commerce Department.

Conclusion

The pace at which our civilization innovates today is unmatched, with information freely available and accessible, and communication across the world happening at near-light speed, advancements in capabilities are happening by the minute – quantum computers, 5G, artificial intelligence, the Internet of Things, ubiquitous connectivity, and blockchains are changing how humanity interacts with the world. The cybersecurity discipline must offer solutions at a similarly fast pace.

The fragmentation of computing into both high-performance clouds down to ultra-constrained devices requires more than a "one size fits all solution" that is standard today. Connecting every thing to the internet increases the exposure and risk of insecurity, and the stakes get higher with every newly deployed IoT device.

The problem is complicated further by the advent of an entirely new form of quantum computer that does not obey rules of the "Turing computers" used ubiquitously today. It is essential to empower and promote fast innovation by private industry, alongside the slower-paced universities, and governments alike, while maintaining intellectual property and rewarding innovation. If we continue down the path of a monolithic security paradigm, it is only a matter of time before it falls to a fast-moving adversary.

There is an obvious and important imperative to migrate to new types of quantum-safe encryption. Additionally, there is a need to migrate to move away from establishing a single technology as a standard, and towards establishing performance standards that post-quantum encryption meet amid a shifting technological landscape.

[25] Cloudflare. (2019). Towards Post-Quantum Cryptography in TLS. Retrieved from https://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/

[26] AgilePQ. (2019). AgilePQ. Retrieved from https://www.agilepq.com/solutions/solutions