The Engineer Who Cried Quantum

EMERGING TECHNOLOGIES COMMITTEE IMPACT REPORT ON POST QUANTUM CRYPTOGRAPHY

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

EXECUTIVE SUMMARY

The advent of quantum computing has been 40 years in the making. This long timeline has led many to put the cybersecurity impacts of cryptanalytically relevant quantum computers[1] (CRQCs) on the backburner. However, as we approach the realization of this revolutionary technology, we cannot ignore the fact that CRQCs will inevitably render all currently deployed public key cryptography obsolete and weaken other fundamental cryptographic techniques such as symmetric key cryptography and hashing algorithms. Thus, it is imperative that we proactively plan and prepare for the transition to quantum-resistant cryptography. This report outlines the impact of this impending transition for the Communications Sector, focusing on the inherent challenges posed by the scale of deployments, the performance requirements of key protocols, and the international coordination required for any changes to protocol standards.

While the exact timeline for realizing CRQCs is uncertain, a substantial number of experts suggest that there is a high likelihood of constructing a functional CRQC within the next 20 years. Despite the uncertainty, it is possible that adversaries may already be recording encrypted traffic for harvest now and decrypt later attacks. Notably, the NSA and the updated CNSA 2.0 are already driving a transition to quantum safe solutions for national security systems. However, given the magnitude of the transition, a one-size-fits-all approach is not viable, necessitating a Quantum Risk Assessment (QRA). Based on that QRA analysis, migration options may include:

- **One-time migration** to the NIST PQC algorithms (once standardized). This option may include a software patch or replacing a hardware module.
- Designing products to be **crypto agile**. Crypto Agility (CA) is the ability to rapidly swap out encryption algorithms, such as PQC algorithms without long downtimes or extensive changes to the associated infrastructure. CA also allows for risk mitigation against other algorithmic breakthroughs, potential future flaws, and other threats.
- Composite or **hybrid solutions**, such as hybrid digital certificates, that combine classical cryptography along with quantum safe solutions. Such solutions may be needed for comprehensive security as well as for backwards compatibility.
- Cost of implementation or performance issues due to the increased computation, memory, storage, and communication requirements associated with PQC may prohibit the migration. In this case, there will be **risk acceptance and planning for obsolescence**.
- **Exploration of alternatives** like QKD, QRNG, and redesigning of protocols and architecture are potential solutions that may offer quantum resistance and should be considered alongside PQC.

As the migration to quantum resistance cryptography begins, there are going to be numerous common challenges that will impact the entire ecosystem. First, there is a lack of standardized algorithms. Second, is a lack of mature open-source libraries in multiple languages based on standardized algorithms that can be used in production ready systems. Third, and perhaps most significantly, there is a dearth of quantum resistant cryptography capable infrastructure that is needed to use any cryptography in practice. These include, but are not limited to, key management systems, hardware accelerators, hardware security modules (HSMs), and broader Public Key Infrastructure (PKI) solutions. Many of these are IT sector dependencies that must be addressed before the Communications Sector can implement its transition.

In addition, there are challenges unique to the Communication Sector that also need resolution. First, we must research, integrate, and test quantum resistant cryptography algorithms in key protocols, such as DNSSec, IPSec, and RPKI, to identify the best candidates. Second, where currently approved quantum resistant algorithms cannot be simply integrated, these protocols must be modified through appropriate standards setting bodies like IETF and 3GPP; such modification will likely be required for hybrid deployments where quantum resistant cryptography may be used in combination with classical cryptography. Finally, and critically, the chosen solutions will have to be analyzed to ensure that they can be used under the current IP rights available for the relevant quantum safe algorithm.

The federal government assumes a pivotal role in the migration to quantum resistance. Establishing the creation of test beds, such as through National Cybersecurity Center of Excellence (NCCoE), can assist in the examination of the performance of NIST PQC candidates within key Internet protocols. Research funding, such as grants from the National Science Foundation, can be allocated to drive research into quantum resistant cryptography, hybrid solutions, and PQC alternatives. To foster collaboration and knowledge exchange, the federal government should also work towards reducing the barriers that US researchers and practitioners face when engaging with international counterparts. Given that many PQC experts reside outside the US, making it easier to bring them stateside to work at US companies will be helpful. Furthermore, providing financial incentives and tax benefits for providers who invest in quantum safe technologies will help remove systems that are unable to migrate.

1 NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems > National Security Agency/Central Security Service > Press Release View

CONTENTS

"Can you do it with a new kind of computer — a quantum computer? Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements."

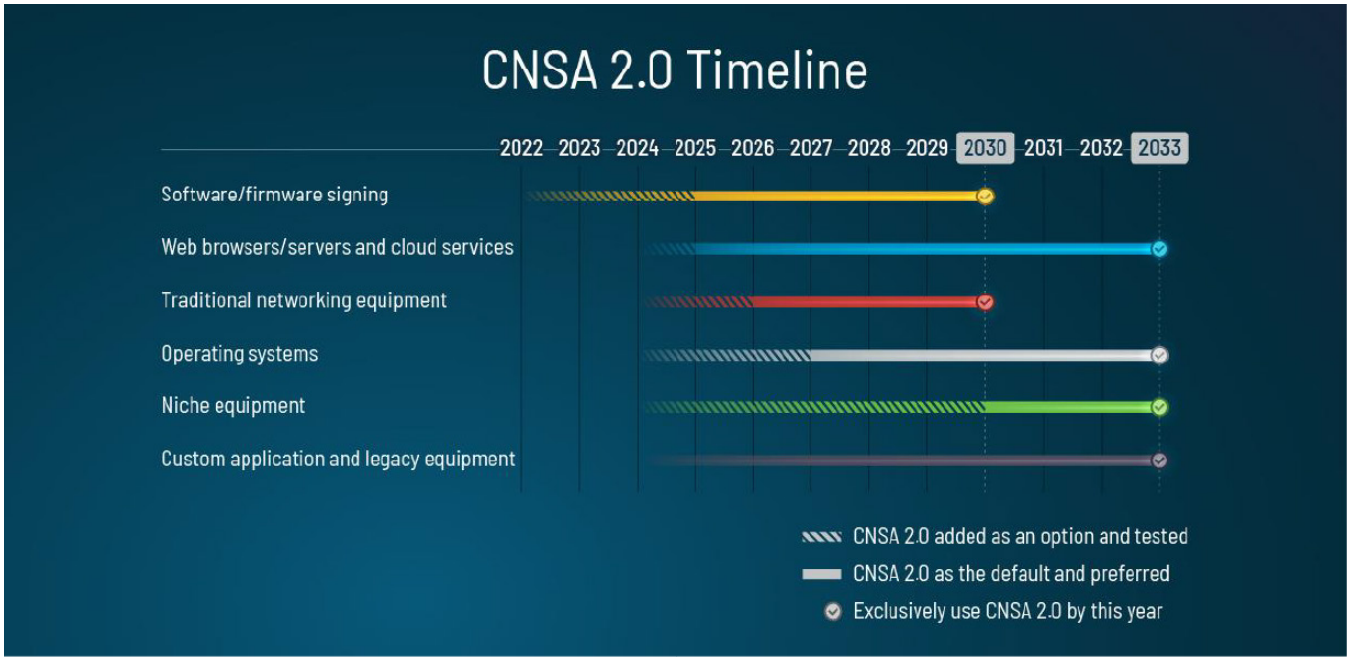
- RICHARD FEYNMAN

INTRODUCTION

Since Feynman's famous talk "Stimulating Physics with Computers" in 1981, the world has seemingly been on the edge of a quantum computing breakthrough. This was further advanced by Peter Shor's research in the 1990s advanced the utility of quantum computers for real world problems, as well as addressing the challenges of decoherence in building quantum computers with quantum error correcting codes[2]. Despite these advances and corresponding investments, the first quantum computer would not arrive until 2010[3]. The resulting excitement led to a quantum gold rush, with governments and companies around the world making quantum an R&D priority. As of 2023, IBM has a 433 qubits quantum computer[4].

Throughout this timeline cybersecurity experts have worried about the impact of quantum computers on cryptography. It is estimated that a cryptanalytically relevant quantum computer (CRQC), that is a quantum computer designed to break or create cryptography, with 6,000 stable qubits is needed to start cracking our current asymmetric algorithms[5]. According to the 2022 Quantum Threat Timeline Report published by the Global Risk Institute, 90% of quantum computing experts surveyed expressed a more than a 50% probability of a CRQC being constructed in the next 20 years[6].

While no known CRQCs currently exist, it is reasonable to speculate that adversaries could be actively recording encrypted traffic today with the intention of decrypting it when a CRQC becomes a reality. This is referred to as a harvest now, decrypt later attack. For many classes of data - such as national secrets, commercial IP, personal health and financial information - the need for secrecy lasts more than 20 years. With a greater than 50/50 probability of CRQC development in the next 20 years, there is a need to begin a risk informed migration to post-quantum cryptography (PQC) or quantum resistant algorithms.



Announcing the Commercial National Security Algorithm Suite 2.0 CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov)

2 Available at https://link.springer.com/chapter/10.1007/978-3-030-83274-2_2
3 Available at https://www.forbes.com/sites/gilpress/2021/05/18/27-milestones-in-the-history-of-quantum-computing/?sh=274c73427b23
4 Available at IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two
5 Available at Post-Quantum Cryptography FAQ (dhs.gov)
6 Available at 2022 Quantum Threat Timeline Report - Global Risk Institute

Despite this, driving stakeholder engagement and creating a sense of urgency has been difficult. Cybersecurity experts are engaged in a perpetual battle, constantly addressing the dynamic and evolving landscape of cyberattacks. With concepts that even puzzle quantum physicists coupled with the fact that quantum computers and associated threats appear distant, engineers advocating for investments for a quantum resistant world are often perceived to be crying wolf.

Yet, it may not be possible to put off the transition much longer. In the United States, the NSA made its first major update to Commercial National Security Algorithm (CNSA) with version 2.0[7], by including multiple quantum resistant algorithms. NSA's recommended transition timeline began immediately on the publication of CNSA version 2.0 and concludes in 2033 (in line with NSM-10[8]). Industries may start expecting customer demands for quantum resistant cryptography in products as early as 2024, especially for any technologies with a shelf life of over 10 years.

This report outlines the impact of this impending transition for the Communications Sector. Some of the challenges, from the lack of standardized algorithms to absence of production ready libraries, will be impactful across sectors. However, the scale of the Communications Sector's infrastructure, the above timeline, and the processes for upgrading key protocols will offer unique roadblocks requiring a coordinated effort from the sector.

HOUSTON, WE HAVE A QUANTUM PROBLEM!

The core technology that underlies all cybersecurity controls is cryptography. Modern cryptosystems often rely on the assumption that certain mathematical problems are hard to solve in reasonable time frames using classical computers. For example, there are currently no known algorithms that can be used to factor the product of two very large primes in a reasonable time using classical computers; this mathematical problem forms the foundation of a ubiquitously used public key cryptosystem called Rivest-Shamir-Adelman (RSA)[9]. That said, the advent of CRQC will break this assumption. For instance, Shor's algorithm implemented on a CRQC will break RSA. This can be addressed by migrating to cryptography based on quantum resistant mathematical problems, e.g., lattices and learning with errors[10].

In the United States the National Institute of Standards and Technology (NIST) has been running a multi-year effort to standardize PQC[11]. In July 2022, NIST announced the round 3 candidates[12]. NIST chose CRYSTALS-Kyber for public key encryption and key establishment as well as CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures. All Round 3 finalists – apart from SPHINCS+ – are lattice based; SPHINCS+ is a hash-based encryption system.

Separately, NIST also announced Round 4 candidates for potential standardization, specifically BIKE, Classic McEliece, and HQC, as well as SIKE. Notably, NIST currently does not have any candidates for digital signatures in Round 4[13]. All but one of the Round 4 candidates are code-based encryption systems, while SIKE, Supersingular Isogeny Key Encapsulation, has been broken.[14] There are two other classes of quantum safe mathematical problems, i.e., non-commutative and multivariate; however, algorithms for these classes were either broken in earlier rounds or not considered due to performance or lack thereof.

In contrast to public key cryptography, symmetric key cryptography and hashing algorithms are currently considered to be quantum resistant. However, quantum computers may utilize Grover's algorithm to provide a speedup to conduct a brute force search for keys[15]. This may be addressed by doubling the size of the symmetric keys or hashing outputs. While this appears less challenging, it hides the assumption that doubling key sizes does not impact the entropy of key generation[16].

Both public key cryptography and symmetric key cryptography are used in combination to secure websites,

7 Available at https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

8 Available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

9 Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. Available at https://dl.acm.org/doi/pdf/10.1145/359340.359342

10 Bernstein, D., Lange, T. Post-quantum cryptography. Nature 549, 188–194 (2017). https://doi.org/10.1038/nature23461

11 https://csrc.nist.gov/projects/post-quantum-cryptography

12 https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022

13 https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdfs

14 Castryck, W. and Decru, T., 2023, April. An efficient key recovery attack on SIDH. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 423-447). Cham: Springer Nature Switzerland. Available at https://eprint.iacr.org/2022/975.pdf?trk=public_post_comment-text

15 Ma, C. , Garg, V. (2021). Navigating the Transition to a Post-Quantum World. SCTE Cable-Tech Expo. Available at: https://www.nctatechnicalpapers.com/Paper/2021/2021-navigating-the-transition-to-a-post-quantum-world.

16 ATIS White Paper (2023). Implications of Entropy on Symmetric Key Encryption Resilience to Quantum. Available at: https://www.atis.org/resources/implications-of-entropy-on-symmetric-key-encryption-resilience-to-quantum/

email, and other cyber based technologies. Encryption using public keys is computationally expensive; thus, they are used to set up a shared symmetric key which is then used to encrypt traffic data. However, this requires binding a public key to an entity. This is done through Public Key Infrastructure, which uses a Certificate Authority to issue a Certificate that associates an entity name with the corresponding public key. Most modern systems use X.509 standard for certificates. These certificates are designed to associate one unique key of a certain size with one entity. Thus, transition to a quantum resistant world will require an update to the X.509 standard. Unfortunately, many quantum-resistant public key algorithms have key sizes that are significantly larger than those of classical public key algorithms and could present issues.

The impact of PQC algorithms will not be limited to X.509 standards. Communications Sector uses encryption in a range of core communications protocols like DNSSec, IPSec, RPKI. These protocols are critical to securing routing. Consider the impact of transitioning DNSSec to PQC. DNS is used to resolve a domain name to the appropriate associated IP. DNSSec adds authenticity and integrity to a DNS response by requiring the operator to cryptographically sign the IP information related to their domain. It is critical for these signatures to be small while also preventing DDoS attacks, packet fragmentation, and other security issues[17]. Additionally, the key sizes need to be small enough to fit in a single packet. Finally, the signature schemes should be fast enough to allow for the same number of signatures that are generated for classical public key based DNSSec. Based on this, researchers note that only FALCON may satisfy the current structure of the DNSSec; alternatives may require redesigning the DNSSec protocol entirely[18].

THE GREAT MIGRATION

Given NSA's update to CNSA and the potential for harvest now, decrypt later attacks, the need to migrate to quantum resistant cryptography is paramount. However, a full migration to quantum resistance cryptography could take up to 20 years[19]. The key industries that must begin the migration now are the Defense and National Security, Critical National Infrastructure (including the Communications Sector), and banking and financial service providers. Given that this is one of the biggest cryptography migrations in history, it cannot be approached in an ad hoc manner and requires a risk-informed strategy. This section details some of the critical considerations to planning this migration strategy.

What to Migrate:

A risk-informed strategy must begin with a risk assessment. Thus, a quantum risk assessment (QRA) should be conducted to inventory assets that will be affected. These should then be prioritized based on sensitivity and shelf life. A QRA, such as A Methodology for Quantum Risk Assessment may be integrated into broader risk assessments (RA).[20] Alternatively, a dedicated QRA, like CARAF, will focus solely on the issues that emerge from CRQC.[21] Regardless of the approach, it should include an inventory of assets and their cryptographic protections, a shelf-life comparison to the probability and time to attack, cost to migrate, strategy and documentation of migration, and continuous monitoring.

Although the highest risk assets are those protected by public key algorithms, all assets and cryptographic protection methods should be inventoried. Even though symmetric algorithms are seemingly quantum resistant, they should still be inventoried. Without fully understanding the capabilities of CRQCs, having a full inventory will lead to better preparedness for any future cryptographic breakthroughs.

How to Migrate:

There are several options to take systems from quantum vulnerable to quantum resistant, as well as different methods of implementing PQC. The migration pathways to consider are a one-time migration, crypto agility by design, or using a hybrid solution. All hardware and software currently being developed, should be look for options to integrate quantum resistance. For technology that is currently deployed (and those that are already developed and currently going into production), a hybrid solution might be the only option until the affected encryption can be replaced.

One-time Migration

After conducting a risk analysis and prioritizing what to migrate, the current technologies that must migrate can undergo a singular migration to one of the standardized PQC algorithms. However, the NIST PQC algorithms cannot be integrated until they are fully standardized. The migration may range from hardware replacement to a software patch. After the implementation of PQC, interoperability, security, and functionality testing should occur. Continuous monitoring must be conducted on the quantum landscape,

17 Müller, M., de Jong, J., van Heesch, M., Overeinder, B. and van Rijswijk-Deij, R., 2020. Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. ACM SIGCOMM Computer Communication Review, 50(4), pp.49-57. Available at: https://ris.utwente.nl/ws/files/241156422/Muller2020retrofitting.pdf

18 Jafarli, S., 2022. Providing DNS Security in Post-Quantum Era with Hash-Based Signatures (Master's thesis, University of Twente). Available at: http://essay.utwente.nl/89552/1/Jafarli_MS_EEMCS.pdf

19 Available at Quantum Threat Timeline Report 2020 - Global Risk Institute

20 https://www.evolutionq.com/publications/quantum-risk-assessment

21 Ma, C., Colon, L., Dera, J., Rashidi, B. and Garg, V., 2021. CARAF: Crypto Agility Risk Assessment Framework. Journal of Cybersecurity, 7(1), p.tyab013. Available at: https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827

to ensure the selected method continues to deliver quantum resistance.

Crypto Agility by Design

Crypto Agility (CA) is the ability to rapidly swap out encryption algorithms and does not require long downtimes or extensive code revisions. Thus, products should be able to swap in different cryptographic algorithms, including PQC. Building in CA simplifies the PQC migration, by allowing for a rapid migration to NIST's PQC algorithms, once they become available. CA is ideal during this transitory period prior to the standardization of PQC algorithms and protocols. The benefits of CA go beyond PQC and add to overall security. CA allows for risk mitigation against other algorithmic breakthroughs, potential future flaws, and other threats.[22]

Nonetheless, CA can be limited by using hardware solutions. For example, many devices use hardware crypto accelerators to speed up crypto related functions, e.g., encryption and decryption. In many cases these are application specific integrated circuits, i.e., they cannot be upgraded as the logic is burnt on the chip. Even when upgrading or patching is possible, these may lead to compatibility issues.[23] Although some hardware can be crypto agile, there may be performance barriers or limits to the agility. As a result, manufacturers should carefully consider the hardware design and performance of their products when designing for CA while making sure they have a plan for upgrading or patching equipment with new cipher suites.

Hybrid

With most crypto transitions there is a one-for-one swap between the old and the new algorithms. While SHA2 simply replaced SHA1, CRYSTALS-Kyber will not replace RSA in a simply one-for-one swap. As quantum resistant cryptography has, in most cases, not undergone decades of cryptoanalysis, it is possible that vulnerabilities may be discovered later. For example, SIKE was in the NIST competition for many years before it was broken using a standard classical computer. Thus, for comprehensive security PQC and classical algorithms will be deployed together as a hybrid solution. This means that regardless of the algorithms chosen the overhead from cryptography will increase. For instance, in the case of certificates, there will be a requirement to either include two sets of keys within a single certificate or bind two separate certificates to the same entity. This will introduce novel challenges related to certificate revocation, key management, and PKI; this may require providers to rearchitect solutions.

Risk Acceptance

After a thorough risk analysis is conducted, the implementation of quantum resistant solution may not be financially or operationally feasible. Research and testing are necessary to understand the effects of performance due to the increased computation, memory, storage, and communication requirements associated with PQC algorithms, such as larger key sizes, more complex algorithms, or both. There will undoubtedly be a large amount of risk acceptance and obsolescent equipment.

Alternatives to PQC

There is no way to know that the PQC algorithms that will be standardized by NIST will be completely quantum resistant. Alternatives to PQC that create quantum resistant technology are being researched. Several of the most widely researched are Quantum Key Distribution, Quantum Random Number Generator, and symmetric key encryption.

Quantum Key Distribution or QKD is an alternative to post-quantum cryptography. QKD relies on the fundamental physics of not cloning, observing, or measuring a quantum state. This results in the collapse of the quantum function. Preventing any attacker from simply copying a quantum bit sent by Alice to Bob. The promise of QKD is that as it relies on physics, rather than mathematical assumptions, it is theoretically secure against a computationally unbounded adversary. Yet QKD has limitations in practice. QKD can only be used to exchange keys between two parties, is limited to a few hundred kilometers over fiber, and QKD Over Air is limited by line of sight. The NSA does not consider QKD to be a relevant solution to address the threats from CRQC.

Cryptographic algorithms rely on randomly generated values. A Quantum Random Number Generator (QRNG) is a Random Number Generator (RNG) that uses quantum mechanics for entropy. Classical RNG uses a pseudo random number algorithm. QRNG research should continue as is can be used to generate the strongest possible cryptographic keys.[24]

Another viable option for achieving quantum resistance is through the redesigning of protocols and architecture. As stated previously, NIST states symmetric cryptography offers quantum resistance and increasing the key size increases the strength.[25] Some technology could be redesigned to use symmetric encryption instead of asymmetric encryption. Other redesign options, including completely remodeling the architecture behind identification and verification, should be researched.

22 Available at [1909.07353] Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility (arxiv.org)
23 Available at ha536vg.pdf (iiis.org)
24 Available at Quantum security technologies - NCSC.GOV.UK
25 Available at Post-Quantum Cryptography | CSRC (nist.gov)

Cost, implementation, interoperability, and remaining risk will be the drivers to determine the best migration path or quantum resistant method for each use case. PQC, CA, hybrid, QKD, QRNG, redesign, and other potential solutions should continue to be researched, tested, and monitored.

BARRIERS TO ADOPTION

Algorithms and Standards

By far the biggest hinderance in the advancement to quantum safe measures is the lack of standardized algorithms. NIST has been leading the effort to standardize these algorithms in US. In Europe ETSI has chosen to simply complement the NIST process rather than run its own competition[26]. Internationally, IETF has stated that it is not scoped to define new cryptography; instead it will focus on incorporating PQC in protocols[27,28]. Most IETF efforts in this space are based on NIST PQC candidates; for example, the PQC being considered for integration with the Cryptographic Message Syntax (CMS) is SPHINCS+, a NIST PQC candidate[29]. At the time of writing this report, NIST has chosen CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ as candidates for standardization; however, these are yet to be standardized.

Furthermore, post-quantum cryptography is less mature than classical cryptography. Few PQCs, such as NTRU and McEliece, have been around as long as RSA or Diffie Hellman. Most PQCs have been around for less than 20 years. This means that even if some PQCs are currently considered secure, such as those chosen by NIST for standardization, it is not unlikely that new attacks using classical computers may be discovered in time. This was, for example, a case with SIKE, one of the fourth-round finalists, which was broken five years after being entered in the NIST standardization process.

It is crucial to highlight that the NIST standardization process received a significant number of 69 submissions. However, out of these submissions, only seven have successfully met the criteria of being both secure and operationally useful, leading them to be selected for standardization or advanced to round four. This reiterates the long-standing understanding among cryptographers that constructing new algorithms that possess both practical utility and security is an exceptionally challenging task. Therefore, the scarcity of new, secure, and practically viable algorithms remains one of the most substantial threats within this domain.

Even if NIST's current set of algorithms are standardized and found to be secure, they will have to go through a process to be incorporated into broader standards. For example, NIST will need to update the Federal Information Processing Standard to incorporate post-quantum algorithms. Similarly, NSA's updated CNSA 2.0 does include some quantum resistant algorithms. However, the choice is limited; NSA may want to add at least the other Round 3 candidates from NIST such as FALCON.

Aside from the government, these algorithms will also need to be added in industry standards such as those from 3GPP, IETF, and others. For example, the Transport Layer Security (TLS) protocol standard from IETF will need to be upgraded to allow for post-quantum cryptography-based handshakes. Simultaneously, the public key infrastructure, such as x.509 certificates, that makes TLS possible will also need to be updated. Each individual organization from 3GPP to IETF will have a distinct process and timelines for making these changes.

IT Sector Dependencies

In addition to the lack of standardized algorithms and protocols, another challenge is the lack of standardized libraries that can be deployed in production ready systems. While the algorithms in the NIST process have corresponding optimized libraries, these are essentially research code. Another key source for post-quantum cryptographic libraries is Open Quantum Safe, a collaborative research project between industry and academia[30]. The operative word being research. These libraries are yet to attain enough maturity to be considered for production ready systems. Furthermore, even the available libraries are primarily written in C or Assembly Instruction and often only support Intel Processors. This means that there are few or no options for other languages like Rust or other processors like ARM[31].

The lack of mature production capable libraries then flows downstream into the lack of mature integrations into protocols and applications. For example, Open Quantum Safe offers prototype integrations for TLS, SSH, X.509, CMS and S/MIME. However, the project explicitly states, *"we do not currently recommend relying on liboqs or our application integrations in a production environment or to protect any sensitive data."*

The next missing piece is the availability of PQC capable hardware and software that allows the deployment of these technologies. For example, we need chip vendors to provide

26 https://www.etsi.org/newsroom/news/1981-2021-10-etsi-releases-two-technical-reports-to-support-us-nist-standards-for-post-quantum-cryptography

27 https://wiki.ietf.org/group/sec/PQCAgility

28 https://datatracker.ietf.org/wg/pquip/about/

29 https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-sphincs-plus/

30 https://openquantumsafe.org/

31 There is ongoing work at IETF to build wrappers for Rust and Python. However, at the time of writing this work is in its infancy. Here is an example for a Go wrapper - https://github.com/thales-e-security/goliboqs

PQC capable crypto accelerators, security elements, and Trusted Platform Modules (TPM). Additionally, we need PQC capable Hardware Security Modules (HSM) and key management solutions. These solutions often burn crypto capabilities into the chipset; thus, the Communications Sector technologies that rely on these solutions may not be able to undergo a simple software update to transition to PQC; instead, they will require truck rolls and physical rip and replacement.

IT Sector's efforts to provision PQC capable solutions (both software and hardware), much like the standards efforts, are still not mature enough to use in production, let alone at the scale of the Communications Sector.

IP Challenges

As a technology field, cryptography is subject to heavy intellectual property enforcement and presents significant liability risk to industry participants.[32] The intellectual property risks inherent in NIST's efforts to standardize PQC algorithms thus presents a significant barrier to the adoption of any future standard. These risks will need to be carefully addressed before encouraging adoption and implementation of particular PQC algorithms.

As described above, NIST is currently in the process of standardizing PQC encryption algorithms. Thus far, NIST has since 2016 held four rounds of standardization that include solicitation for candidate algorithms and analysis of the candidates' suitability for standardization. In July 2022, NIST announced four algorithms would be standardized—one public-key and key-establishment algorithm, and three digital signature algorithms. At this juncture, the algorithms have not yet been standardized, and NIST is continuing to assess other key-establishment algorithms from the fourth round of the standardization process.

As part of these efforts, NIST has taken steps to address some IP risks. For example, NIST has (1) required all algorithm submissions to include an intellectual property statement disclosing any patents protecting the algorithm[33] and (2) negotiated a nonexclusive license to two patent portfolios to allow companies to adopt and use the selected CRYSTALS-Kyber encryption algorithm.[34]

While NIST's steps are important, they do not fully guarantee that a company using a NIST-selected algorithm can do so without the risk of IP infringement liability. *First,* even extensive due diligence cannot identify all patent risks. *Second,* with respect to the license agreement that NIST negotiated, stakeholders should be aware that such licenses do not guarantee that a company can use the CRYSTALS-Kyber encryption algorithm without subjecting itself to the risk of infringement liability. Somewhat counterintuitively, a patent license does not grant any rights to implement a particular technology; it is simply an agreement that the owner of the licensed patents will not enforce those specific patents as long as the terms of the license are adhered to. To the extent that other individuals and companies hold patents that cover the chosen algorithm, those companies remain free to sue companies who adopt and implement the algorithm.

Third, the owners of the licensed patents can still bring infringement lawsuits against companies if they stray outside the somewhat ambiguous terms of the license. Importantly, at this juncture while NIST is still in the standardization process, the license agreements only cover use of the CRYSTALS-Kyber algorithm as part of an adopted standard. Thus, until NIST issues a final standard, any use of the algorithms would be outside the scope of the license and therefore unprotected. Additionally, the license excludes any "modification, extension, or derivation of the parameters of the PQC ALGORITHM."[35] Companies may inadvertently increase their liability exposure by operating under the NIST license if any of their work can be characterized as an extension or derivation of the licensed algorithm.

More generally, any standardization process raises concerns regarding intellectual property protection and liability exposure, and PQC standardization is no exception. Once a standard has been selected and gains adoption, industry participants become subject to network and lock-in effects, making it difficult to avoid infringement once industry becomes aware of a relevant patent. The risk here is substantial. As just one example, after the widespread adoption of Hypertext Transfer Protocol Secure (HTTPS) encryption protocol, patent trolls launched hundreds of opportunistic lawsuits against companies that had adopted HTTPS,[36] resulting in over $40 million in settlements from

32 *See* CNET, RSA Sues Novell Over Cryptography Patent (Feb. 6, 2002), *available at* https://www.cnet.com/tech/tech-industry/rsa-sues-novell-over-cryptography-patent/; *See* V. Goel, NYT, *Apple Pay Violates Patents Held by Security Technology Inventor, Lawsuit Alleges* (May 21, 2017), *available at* https://www.nytimes.com/2017/05/21/technology/apple-pay-patent-lawsuit.html; G. Gross , ComputerWorld, *Internet Transaction Patent Case Goes to Trial* (Feb. 27, 2003), *available at* https://www.computerworld.com/article/2581733/internet-transaction-patent-case-goes-to-trial.html; Wired, *Encryption Copyright Battle* (May 21, 1998), *available at* https://www.wired.com/1998/05/encryption-copyright-battle/.

33 NIST, Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process at § 2.D.

34 Available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

35 License Agreement § 2.9 (U.S. Portfolio Only).

36 See S. Nichols, The Register, Sued for Using HTTPS: Big Brands Told to Cough Up in Crypto Patent Fight (Dec. 1, 2015), available at https://www.theregister.com/2015/12/01/cryptopeak_sues_/.

companies for just one of the asserted patents.[37] These considerations all counsel in favor of proceeding with caution here.

FEDERAL INCENTIVES AND BROADER CONSIDERATIONS

The federal government can play an influential role in helping the Communications Sector address the barriers to PQC adoption identified in the previous section. For instance, while the IT Sector's PQC offerings mature, the federal government can drive the creation of test beds to examine the performance of NIST PQC candidates within key Internet protocols. This work, for example, can be advanced through the National Cybersecurity Center of Excellence (NCCoE) workstream on Migration to Post Quantum Cryptography[38]. Prior to the standardization of the NIST PQC algorithms, industry can begin testing crypto agility or algorithm exchange, especially algorithms with much larger key sizes. Backwards compatibility of systems will present a challenge and should be tested. Testbeds will be an integral part in the mapping of the migration, determining challenges, and creating an accurate timeline.

Additionally, the federal government can use research funding, such as through the National Science Foundation, to drive research into quantum resistant cryptography, hybrid solutions, and PQC alternatives. For example, the current research on integrating PQC into DNSSec is largely conducted at University at Twente in Netherlands[39]. The US government can incentivize similar work at US universities, especially through the creation of a new Industry-University Research Partnerships dedicated to the advancement of PQC within key internet protocols.

The federal government can reduce the barriers that US researchers and practitioners face when engaging with international counterparts. First, cryptography continues to be regulated under export controls by the Bureau of Industry and Security (BIS). This may create a chilling effect for US researchers who may wish to make their libraries and other PQC related work more widely available to receive feedback from international cohorts. Second, as many PQC experts reside outside of the US, making it easier to bring them stateside to work at US companies will be helpful. This can be done by making it easier for PQC researchers to get an O-1 visa or adding PQC related work as part of the National Interest Waiver program.

Transition to quantum resistant cryptography is going to be an expensive exercise. This will be particularly true when the transition requires a hardware upgrade, such as replacing crypto accelerators that support classical algorithms with those that support post quantum algorithms. In some cases, such upgrades may be prohibitively expensive. For some smaller providers even testing new solutions may impose significant financial hardship. The federal government can address these by providing financial incentives and tax benefits for providers who invest in quantum resistant technologies.

As noted in the previous section, adoption of PQC relies on the creation of new standards including those for quantum resistant integrations and upgrade to key protocols such as DNSSec. Much of this standard's effort requires international coordination, through participation in cross national standards bodies like 3GPP and IETF. The federal government can advance the participation of US companies in these standards setting bodies by creating financial incentives, which will align with the National Standards Strategy for Critical and Emerging Technology[40].

CONCLUSION

The journey to quantum resistance is a long one. The migration to quantum resistant cryptography will be a significant effort, requiring new technical solutions, cross ecosystem collaboration, and in some cases extensive financial investments. The technical complexities of such a transition pose unique challenges for the Communications Sector, given the scale of communications infrastructure and the performance requirements of underlying protocols that were historically not designed to address security.

To address these challenges as well as mitigate the impact of harvest now, decrypt later attacks, the Communications Sector needs to plan for a migration to a quantum resistant world now. Specifically, individual actors in the sector need to define and adopt a migration strategy informed by a risk analysis of all impacted assets, including hardware assets, software assets, protocols, and other supporting infrastructure. While certain assets may necessitate a one-time migration, such as to the existing set of NIST PQC candidates, others with an extended lifespan in the field should consider implementing crypto agility to prepare for multiple transitions.

37 B. Chappell, NPR, *Jury Orders Newegg To Pay $2.3 Million In 'Patent Troll' Case* (November 26, 2013), *available at* https://www.npr.org/sections/thetwo-way/2013/11/26/247350084/jury-orders-newegg-to-pay-2-3-million-in-patent-troll-case; A. Greenberg. Forbes, *Meet The Texas Lawyer Suing Hundreds Of Companies For Using Basic Web Encryption* (Nov. 9, 2021), *available at* https://www.forbes.com/sites/andygreenberg/2012/11/09/meet-the-texas-lawyer-suing-hundreds-of-companies-for-using-basic-web-encryption/.

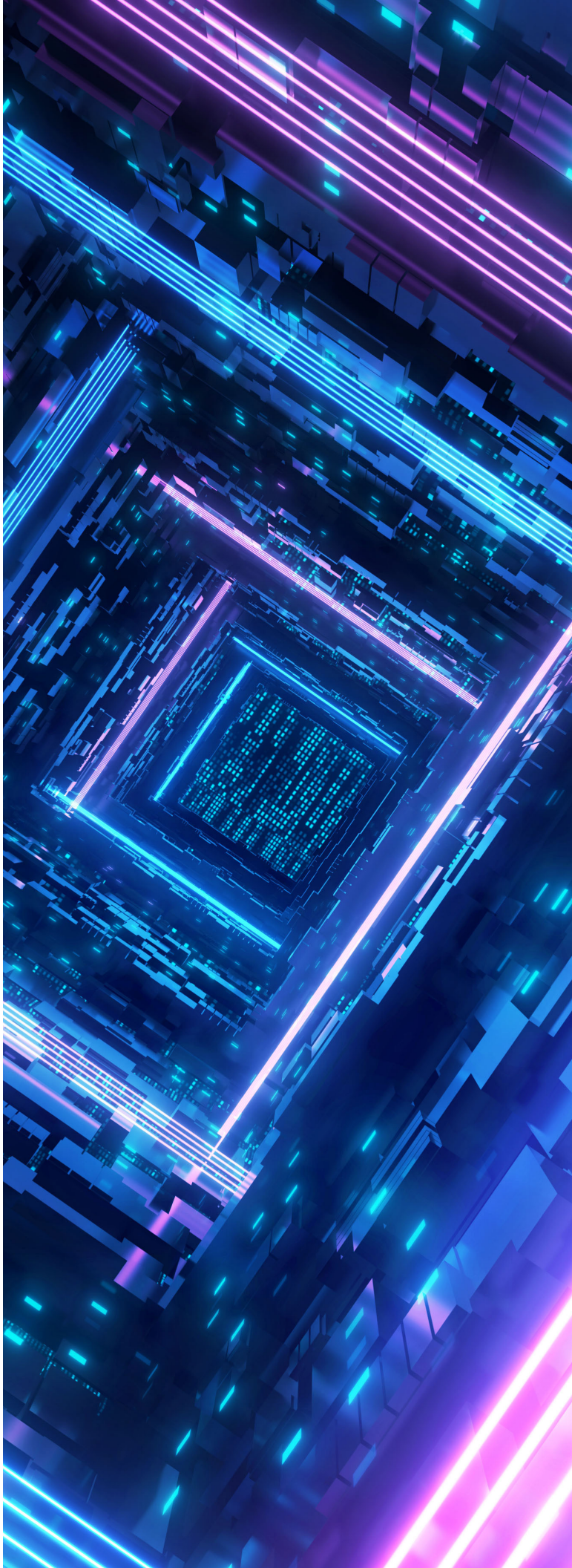
38 https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

39 https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf

40 Available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/

Any effort to migrate the Communications Sector providers to PQC will need to address its dependencies on the IT Sector. This includes the availability of production ready PQC libraries and PQC capable solutions, such as crypto accelerators, TPMs, HSMs, key management software, and more. The absence of production ready libraries and standardized algorithms will impinge downstream integrations into core protocols like DNSSec. Simultaneously, the lack of PQC capable crypto accelerators will delay the migration of long-lived devices like gateways and SIM cards to quantum resistant cryptography.

The engineering community has long been aware of the cybersecurity threats that emerge from large scale quantum computers. Yet the immediate and often overwhelming nature of other cyberthreats have pushed their cries of quantum to the backburner. However, the quantum wolf will no longer be kept at bay and demands a significant investment to transition to a quantum resistant world. The Communications Sector will not be left untouched by this transition and must address key challenges that are unique to its underlying technical stack. Be prepared. Have a migration strategy. Afterall, the cryptographic concerns are just the beginning of potential quantum computing threats.



CSCC EMERGING TECHNOLOGIES COMMITTEE CO-CHAIRS

Vaibhav Garg, Executive Director, Cybersecurity Research & Public Policy, Comcast Cable

Taylor Hartley, Network Security Solutions Architect, MANA Network Product Solutions, Ericsson

Justin Perkins, Manager, Cybersecurity and Policy, CTIA