Planning for Cryptographic Readiness in an Era of Quantum Computing Advancement

David Ott, Dennis Moreau and Manish Gaur
VMware, U.S.A.

Keywords: Post-quantum Cryptography, PQC, Public Key Cryptography, Cryptographic.

Abstract: As the prospects for scaled quantum computing steadily improve, there is an important disruption emerging in response within the world of security: post-quantum cryptography, or PQC. In the 1990s, Peter Shor showed that if scaled quantum computers were to exist, they could be used to efficiently break trap door functions underlying our widely used public key cryptography algorithms (RSA, DSA, ECDSA, ECDH). Various US government agencies have issued reports on this concern, including NIST which embarked on a standardization effort to select new algorithms with the help of the cryptography community as of 2016. But while NIST will address the problem of new algorithms, many organizations feel puzzled at the uncertain timeline for PQC and the lack of guidance on the path forward with migration. In this paper, we discuss the problem of PQC readiness from an organization's point of view, providing recommendations on how to understand the landscape and guidance on what can and should be done in a phased manner. While scaled quantum computing may seem a distant concern, we believe there are good reasons for an organization to start now in developing its understanding of the situation and creating a phased action plan toward PQC readiness.

1 INTRODUCTION

Quantum computing, or the controlled use of quantum physical phenomena (e.g. superposition, entanglement) to represent and manipulate information, has made significant strides in recent years. Notably, quantum "supremacy" was recently demonstrated experimentally by Google using their 53-qubit Sycamore processor (Arute et al., 2019). Prototypes by companies like IonQ, IBM, Intel, Honeywell, Rigetti, and Google have propelled quantum computing state-of-the-art to 50-100 qubits, at the cusp of what is now referred to as NISQ, or Noisy Intermediate-Scale Quantum technology (Preskill, 2017). Both government and private investment have increased dramatically; for example, the US Congress passed the National Quantum Initiative Act in December of 2018 calling for $1.2B to quantum information science initiatives over a 5-year period (H.R.6227, 2018). The European Commission has funded the Quantum Technologies Flagship initiative with €1B for research and technology innovations over the next 10 years (EU, 2021).

While research advancements make quantum computing look increasingly promising, many people are not aware of the security implications. In January of 2016, the NSA/CSS Information Assurance Directorate released a FAQ stating that sufficiently large quantum computers "would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures" (NSA/CSS, 2016). This was further underscored by NIST who, in a subsequent April 2016 report (Chen et al., 2016), described well-known public key cryptography algorithms such as RSA, ECDSA, ECDH, and DSA as "no longer secure".

In December of 2016, NIST kicked off a new cryptographic standards initiative by publishing an open call for Post-Quantum Cryptography (PQC) algorithms to replace our existing public key cryptography, citing "noticeable progress" in quantum computing (QC) development and the complexity of transition to new algorithms as key drivers for what would seem an early effort. 69 proposals were received by the November 2017 deadline, and the number has since been vetted to seven finalist and eight alternate candidates which are currently under consideration at time of this writing. PQC standards are intended to provide quantum safe alternatives to our current public key cryptography standards.

Ott, D., Moreau, D. and Gaur, M.
Planning for Cryptographic Readiness in an Era of Quantum Computing Advancement.
DOI: 10.5220/0010886000003120
In *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, pages 491-498
ISBN: 978-989-758-553-1; ISSN: 2184-4356

While NIST is well-positioned to lead the international community in developing PQC standards, we note that the initiative does not address the complex problem of cryptographic migration for millions of organizations across the industry. Today, 4.1 billion Internet users and 2 billion web sites (Hosting Facts, 2021) rely on public key cryptography for secure communication. Millions of organizations worldwide furthermore use cryptography for identity verification and authentication, secure software updates, trusted infrastructure management, secure email, key management systems, transport security, confidential data protection, and more. Public key cryptography solutions are embedded into our compute infrastructures at many layers, from hardware features and operating system software stacks to application-level data handling and user interfaces. The extensiveness and pervasiveness of cryptography usage means that a transition to new PQC standards will be a complex undertaking on a massive scale.

Our interest in this paper, is providing early guidance to organizations who may be just learning about the challenge of PQC migration for the first time and struggle to understand what they can and should do as the march toward scaled quantum computing continues to advance. While PQC standards and industry migration might appear years away, we believe there are some good reasons for an organization to take stock of its risks and begin structured preparation at this early date, and generally be ready for the transition as the timeline for quantum computing continues to change in a volatile manner.

This paper is organized as follows: In section 2, we discuss the broader picture of timelines and the state-of-the-art in both QC and PQC. In section 3, we point out several issues that motivate early awareness and planning for PQC readiness. In section 4, we provide organization guidance in several areas: goal development, phased migration planning, identifying long-lived information assets at risk, and industry and standards involvement. In section 5, we discuss some addition gaps that will need to be addressed collectively by the industry. In section 6, we summarize the contents of this paper and mention future work.

2 Y2Q: THE CRYPTOGRAPHIC READINESS RACE

The problem of cryptographic readiness for an organization and the industry can, at its core, be viewed as a race between two competing timelines. On the one hand, QC technology advancements over time will bring the technology closer and closer to a scaled form that represents a threat to today's widely deployed public key cryptography algorithms. On the other hand, PQC standards and subsequent deployment initiatives will bring the industry closer and closer to a state of cryptographic readiness (i.e., quantum safety). The situation is depicted in Figure 1.

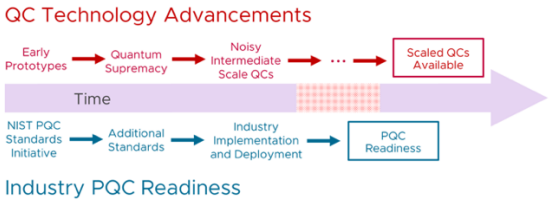

Figure 1: Y2Q and the race between QC Technology Advancement and PQC Readiness.

The term "Y2Q" is meant to denote that point at which scaled QC is available and quantum safe algorithms must be in place as a defense. The term borrows from "Y2K" in which the industry, as a whole, faced a readiness challenge associated with concern over data formatting implications of the transition from year 1999 to 2000. Note that Y2Q is unlike Y2K in that the timeline for QC computing advancement and eventual realization in scaled form is uncertain. Nonetheless, we believe the broader industry readiness implications make it a useful analogy and tool for building awareness of the situation.

2.1 QC Technology Advancement

The Central to QC technology advancement is the *qubit*. A quantum bit, or qubit, is a unit of information represented by a quantum-mechanical system and leveraging quantum *superposition*. That is, while a "bit" in classical computing stores either a 0 or 1 but not both, a "qubit" in QC uses quantum superposition to store both 0 and 1 probabilistically. Through quantum *entanglement*, multiple qubits interact to support an exponential number of states, for example, a 3-qubit register representing the probability space of all 23 or 8 possible states simultaneously. Quantum algorithms essentially manipulate probability distributions through controlled "gate" operations on physical qubits. Note that the results of a QC computation, however, are measured using classical devices which cause the quantum state to collapse to a classical value.

Advancements in quantum computing technology are along many dimensions. A variety of approaches are being explored for realizing qubits (e.g., photon polarization encoding, Josephson junctions in superconducting circuits, electron position in quantum dots, etc.), each of which offer various advantages and disadvantages. A major challenge is that of quantum *decoherence*, or the loss of correct phase relation between states. Sophisticated vacuum chambers and cryogenic systems are used to lessen the impact of interaction with the surrounding environment and improve the longevity of quantum coherence.

Key metrics in assessing quantum computing advancement include number of qubits, gate type and fidelity, physical error rate, qubit coherence time, number of gate operations before decoherence, and connectivity (NAS, 2019; Bishop et al., 2017). At the time of this writing, industry leaders in quantum computing arguably include IonQ who announced a 79-qubit processor based on trapped ions in December of 2018 (IonQ, 2018), and Google who, as mentioned in the Introduction, announced *quantum supremacy* in October 2019 with its 53-qubit Sycamore processor (Arute et al., 2019). The term "quantum supremacy" was coined by John Preskill (Preskill, 2011) and refers to QC computations that "go beyond what can be achieved with ordinary digital computers."

2.2 Industry PQC Readiness

The power of quantum computing lies in its ability to represent and manipulate an exponential state space using quantum superposition and entanglement. In 1994, before substantial QC prototypes had been built, Peter Shor showed that a sufficiently large QC, if it existed, could be used to solve the problem of integer factorization in polynomial time using O(log N)2 number of operations/gates (Shor, 1997). This surprising result can, furthermore, be generalized to solve the discrete logarithm and elliptic curve problems.

The implications for public key cryptography are significant. Public key cryptography relies on one-way functions which are easy to compute in one direction and intractably hard to compute in the inverse direction. Shor's algorithm implies that an adversary could reverse engineer the private key for a 2048-bit RSA public key in polynomial time using a QC with approximately 4000 qubits (QC Report, 2020). Even worse, a 256-bit modulus elliptic curve public key could be broken (i.e., the private key derived) in polynomial time using a QC with approximately 2300 qubits (NAS, 2019). This leap in computational efficiency has led NIST to proclaim in a 2016 report (Chen et al., 2016) that widely deployed public key cryptography algorithms RSA, ECDSA, ECDH, and DSA are "no longer secure" if and when QC becomes sufficiently scaled.

Fortunately, the research community has done significant work over the last decade (and borrowing from earlier decades) (pqcrypto.org, 2021; PQCrypto, 2008-Present) looking at public key cryptography solutions based on an alternative set of trap door functions with no known mapping to QC. While sometimes referred to as "quantum resistant" or "quantum safe" cryptography, algorithms are collectively known as post-quantum cryptography and center around the following five approaches to trap door functions:

- *Hash-based cryptography*. Easy to compute a cryptographic hash but difficult to find an input value from a hash value.
- *Code-based cryptography*. Easy to do matrix multiplication with error correcting codes, but hard to reconstruct.
- *Lattice-based cryptography*. Easy to compute vectors in n-dimensional Euclidean space but difficult to reconstruct.
- *Multivariate cryptography*. Easy to compute transform-ations in multivariate equations, but hard to reconstruct.
- *Supersingular elliptic curve isogeny*. Easy to create isogeny mappings between elliptic curves but hard to reconstruct.

As mentioned in the Introduction, NIST kicked off a PQC standards initiative in December of 2016 by publishing an open call for PQC algorithms. From the 69 complete proposals that were received in late 2017, seven primary and eight alternates candidates are now under consideration at the time of this writing (NIST PQC, 2021). There are shown in Table 1. Draft standards are expected to be available sometime between 2022, although a 2-year period of public commentary will be observed before standards become official, perhaps sometime in 2024 (NIST PQC, 2021).

How PQC will be deployed once the NIST standards are published is a major challenge, and the subject of this paper. We believe the migration picture has started to emerge but is arguably in its infancy and in need of industry attention. TLS and other protocols (Dierks et al., 2008; Rescorla, 2018; Housley, 2015) that perform cipher suite negotiation could potentially add PQC as new cipher suite alternatives. But Hybrid modes of key exchange have been proposed for TLS

Table 1: PQC algorithm proposals under consideration by NIST at the time of this writing.

	Finalists	Alternates
Hash-based		SPHINCS+ Picnic (ZNP)
Lattice-based	CRYSTALS-DILITHIUM KYBER NTRU SABER Falcon	FrodoKEM NTRU Prime
Code-based	Classic McEliece	BIKE HQC
Multivariate	Rainbow	GeMSS
Elliptic Curve Isogeny		SIKE

1.3 (Stebila et al., 2019) in which multiple algorithms are used in combination, thus addressing the problem of introducing new standards and implementations while maintaining compliance with current standards. Hybrid X.509v3 certificates already support extensions which could be used to embed a PQC signature into another signature using a conventional algorithm. Standards and open source implementations are needed.

3 ESTABLISHING NEAR-TERM PRIORITY

It is not uncommon for organizational leaders to view scaled quantum computing as many years away. As such, attention to PQC is assigned a low priority in yearly planning cycles, especially relative to other seemingly more pressing needs. In this section, we review key arguments motivating the need for prioritizing PQC in the near-term and addressing the problem of long-term readiness before the threat of QC escalates.

3.1 Near-term Concerns

One key problem to consider in the PQC readiness challenge is that of QC timeline uncertainty. While experts agree that QC has made considerable advancements (Chen et al., 2016; Shankland, 2019) and that the level of VC and government investment has gone up dramatically (Temkin, 2021; Qureca, 2021), the timeline of scaled quantum computing is at best uncertain and at worst an elusive goal that may not be realized at all (Dyakonov, 2018).

But while the uncertainty of the QC timeline leaves open the possibility of late or no arrival, it also includes the possibility of early arrival. In fact, events like product announcements (IonQ, 2018; Kelly, 2019; IBM, 2019), milestone achievements (e.g., quantum supremacy) (Arute et al., 2019), government announcements (H.R.6227, 2018), entrepreneurship activity (Gibney, 2019), and worldwide investment (Katwala, 2019; Castelvecchi, 2019) have had the effect of pulling in predictions (Wallden et al., 2019). As such, we argue that the risk stemming from timeline uncertainty is a good reason for any organization to actively monitor and make preliminary preparations as a form of risk mitigation.

Another key concern is that of PQC migration complexity. NIST, in its PQC call for proposals, notes that, “a transition to PQC will not be simple as there is unlikely to be a simple ‘drop-in’ replacement for our current public key algorithms” (NIST CFP, 2017). In fact, PQC algorithms differ significantly in performance, compute, memory, and other resource requirements, and sometimes present new requirements compared to our current standards (e.g., entropy) (Chen, 2017). Meanwhile, technical bodies overseeing many public key cryptography usage domains have done little to take stock of these implications, or to consider the details of PQC migration more closely.

From an organization point of view, considerable lead time will be needed to work through the complexities of cryptographic migration. For example, an IT organization will need to interact with its myriad software and service providers, each of whom will have their own roadmap complexities in implementing PQC. Planning for quantum safety in an organization’s software and service offerings often implies lengthy design-implementation-testing-release pipelines. Interactions between standards bodies, open source communities, third party solution providers, certification agencies, and company planners can be iterative and take considerable time to work though. Perhaps it is no surprise, then, that prior cryptographic migrations (3DES to AES, MD5 to SHA1, SHA1 to SHA2, RSA to ECC) have often taken a decade or more to establish broad adoption (Cloud Security Alliance, 2019).

A third problem for any organization is that of customer and regulatory demands. As QC advancements make headlines, more and more organizations, and perhaps whole industries (e.g., financial), will ask questions about the quantum safety of an organization’s software and services. We argue that almost any organization must consider their plans for readiness in order to address emerging customer concern over the issue. Note that these demands may significantly precede the arrival of scaled QC and may be associated with activity in the press as technology advancements and new prototypes are given high profile.

3.2 The Problem of Harvest Now, Decrypt Later

Another notable problem in the uncertain timeline of scaled QC is that of harvest now, decrypt later (a.k.a., capture now, attack or exploit later). In this security threat, an adversary captures ("harvests") encrypted information assets as they traverse the production Internet or are exposed in other forms. The captured data is then archived until scaled quantum computers become available in the future. Given sufficient longevity to the information under attack (e.g., trade secrets, social security numbers), the attack is worth waiting for. For example, a TLS connection using the current ECDH standard could be copied and stored as it traverses the public network and then attacked by an adversary 10 years from now when scaled QC is widely available in the public cloud or a nation state computing lab.

The threat implies the need for an organization to consider the lifetime of their information assets, their level of exposure, and whether they should implement protections before scaled QC becomes available. (Protection options are discussed in section 4.3 below.

4 ORGANIZATIONAL ROADMAP

What can and should an organization be doing to plan for PQC readiness during this early period of quantum computing technology advancement? After all, aren't PQC standards still years away? In this section, we propose ideas for how an organization can create and structure its path to readiness in a phased manner that avoids premature or overly reactive readiness actions.

4.1 Establishing Goals

An important objective for any organization developing a PQC action plan should be establishing goals that can help to guide long term planning. The notion of "readiness" may vary from organization to organization, depending on the nature of its business or service (e.g., educational services vs investment management), the industry sector (e.g., automotive vs finance), and associated information assets (e.g., customer preferences vs health care data).

One broad distinction is that between IT operations readiness and product/service readiness. Goals associated with the former may include identifying cryptography usage and key information assets across the organization and understanding exposure points that could be exploited by a future adversary with access to scaled QC. Goals might also comprehend software and services supplier relationships, and exposure points that call into question their level of readiness and roadmap for PQC.

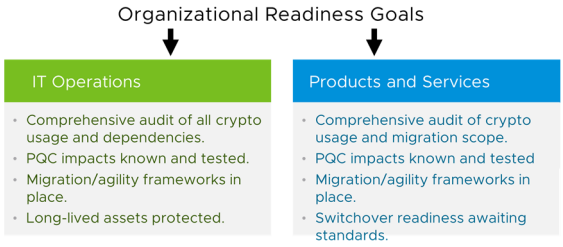

Figure 2: Illustrating and organization's PQC readiness goals.

Product/service readiness must consider the PQC challenge from a customer's point of view. Goals may be set that anticipate customer questions about product roadmap readiness and the quantum safety of customer information assets. Similar to IT operations, goals may include a comprehensive understanding of cryptography usage, long-lived information assets, and key areas for prototyping PQC usage and migration. Technical goals in both domains might include an understanding of PQC performance and platform resource impacts, for example, an understanding of PQC impact on network communications in customer-facing products and services. Anticipating migration complexities, PQC testing requirements, and auditing frameworks might be considered among many other issues.

4.2 Building a Phased Migration Plan

We recommend that organizations consider developing a phased approach to PQC readiness as seen, for example, in Table 2. Phases can be constructed to synchronize with the timelines discussed in section 2, and to gradually increase the level of resourcing and investment as PQC solutions become more available and QC scaling increases.

Table 2: A phased approach to organizational PQC readiness.

Phase	*Objectives*
1. Organization	• Establish PQC Working Group • Preliminary impact assessment (IT, products/services)
2. Assessment and Planning	• Risk assessment (information assets) • Crypto usage inventory and migration requirements analysis • Dependency analysis (suppliers, open source, standards)
3. Experimentation and Prototyping	• Understand PQC algorithm impacts • Develop migration and agility frameworks
4. Scaled Integration and Testing	• Deployment of migration and agility frameworks • Testing and verification
5. Switchover Readiness	• Configurable, auditable readiness frameworks in place • Ongoing maintenance and updates • Early protection for long-lived info assets / devices

The example provided in Table 2 is intended as a starting point for organization discussion.

Organization Phase. A working group (WG) should be created comprised of representatives from business units around the organization, each of whom have a stake in the longer term PQC readiness picture. The WG should establish two timelines that will be closely monitored in on ongoing way per Table 3, and identify the broader scope of impacts of PQC to the organization. Impacts should include both internal operations and external-facing products and services.

Table 3: Key Y2Q timelines and tracking areas.

QC Technology Advancement	State-of-the-art Prototypes/Products • Qubit number, error rates, coherence time Technology milestones • Quantum supremacy, quantum error correction • NISC (100-200 qubits), medium scale (200-1000 qubits)
PQC Standards and Industry Readiness	NIST PQC standards development • Pre-standards, draft, comment period, published • Reference implementations, open source libraries Other key standards (IETF, ETSI, ITU, etc.) • e.g., Hybrid TLS 1.3 Migration and agility frameworks and tools availability • Inventory, hybrid X.509 certificates, OS tools

Assessment and Planning Phase. In this phase, the WG should work toward a comprehensive inventory of cryptography usage and long-lived information assets and establish a set of longer term goals that help to define quantum safety given the nature of the organization, its core business and products, its operations, and its customer base. A discussion of goals must also consider key dependencies (e.g., PQC standards and implementations) and the manner in which PQC deployment should proceed across IT infrastructure and customer products.

Experimentation and Prototyping Phase. The WG should identify areas of key impact and risk for the organization and begin experimenting directly with PQC prototypes. Goals of exploration should include understanding the performance and resource requirements (e.g., memory, CPU, I/O, communications, entropy) of PQC, developing reusable frameworks for PQC migration, and ensuring that PQC deployment schemes are cryptographically agile (see section 5.1).

Scaled Integration and Testing Phase. The understanding and frameworks developed in the prior phase should be scaled across IT infrastructure and company products and services. The goal, perhaps counterintuitively, is not comprehensive migration to PQC, but comprehensive readiness for migration. That is, the machinery or instrumentation needed for migration is integrated, tested, and ready to be enabled. This step likely includes automation for key migration tasks, and considerable work on verification schemes. The latter is needed for auditing and certification when NIST standards are explicitly adopted across the industry.

Switchover Readiness Phase. In this phase, an organization is in a readiness state for PQC migration, with configurable and auditable frameworks in place. Changes in NIST algorithm standards can be readily deployed, as can changes by other standards organizations (e.g., ITU, ETSI, IETF) for specific cryptography usage domains. Testing infrastructure is in place to verify updates and a global switchover to PQC standards if and when the time has arrived.

4.3 Addressing Long-lived Information Assets

Evaluating future QC risk to long-lived information assets and whether or not to take action in the near term is a difficult decision that every organization will need to navigate. Mosca (2018) has proposed a widely cited risk assessment framework shown in Figure 3.

There are three key parameters to consider: the security lifetime of a cryptographic key protecting an information asset, the amount of time needed for PQC migration (dependent on both organization factors and industry dependencies), and the time needed for realizing scaled QC as a technology. The problem, of course, is that the latter two factors are not known, making the estimate an exercise in exploring potential scenarios on how the future could play out. We note, however, that security risk assessment is by no means a new field and well-studied methodologies like FAIR (Freund et al., 2014) are available for the analysis.

Define:

x : Security shelf life (i.e., crypto key lifetime requirement)
y : Migration time (i.e., time required for PQC readiness)
z : Collapse time (i.e., time required for scaled QC)

QC security threat:

$x + y > z$: Security shelf life plus migration exceeds scaled QC

Figure 3: Mosca's risk assessment framework for QC.

Organizations that choose to take near term action to counter the threat of harvest now, decrypt later have a number of options. Firstly, they might consider ways to limit or avoid long-lived information asset exposure. For example, they might avoid passing sensitive data over the production Internet, or make exclusive use of private links within organization infrastructure. Another approach is the use of

quantum safe VPNs or communication tunneling mechanisms. The arrangement has the advantage of not requiring PQC migration for the myriad applications and services utilized by an organization. Early adoption is likely to mean that the solution is pre-standards, so decisions will need to be made on PQC algorithm selection and how future changes will be enabled.

4.4 Industry and Standards Involvement

Beyond internal considerations, an organization should consider involvement in industrywide PQC initiatives as key stakeholders. NIST, in its PQC standardization initiative, has repeatedly invited the broader industry to submit benchmark results, application-based considerations, and protocol-based requirements associated with PQC candidate algorithms (Moody, 2019). Such information can help to inform their decisions as they vet alternatives and select parameters for standardization.

Organizations may similarly have a stake in other standards that are emerging on the PQC landscape. PQC hybrids in TLS 1.3, for example, are discussed in a July 2019 Internet Draft from the IETF. Among other issues, the group is considering design alternatives for key share exchange between clients and servers and how keys should be combined. Such issues may have important implications for network appliances and web server performance. As another example, the OASIS open standards group has been actively considering how quantum safety will be integrated into the Key Management Interoperability Protocol (KMIP) that is widely used by key management servers (OASIS, 2019).

Many organizations make extensive use of open source cryptography libraries and have a significant stake in expediting and hardening PQC implementations. The Open Quantum Safe (2021) project has implemented, for example, a branch of the widely used OpenSSL library that includes PQC for TLS 1.3 (Crockett et al., 2019). This early library effort can be used for testing and evaluating PQC in organization prototypes. OQS authors invite open source contributors to join them in implementing PQC algorithms for various operating systems and architectures (OQS, 2021).

4.5 Cryptographic Agility

A 2019 workshop sponsored by the CRA Computing Community Consortium (2019) points out the need for research on cryptographic agility, or the ability to migrate cryptographic algorithms and standards in an ongoing manner. While cryptographic libraries offer modularized selection among algorithms or standards, work is needed to extend the notion of "agility" to include flexible frameworks for adjusting cryptographic usage for different compliance requirements, organizational policy changes, multiple operating points on the security-performance tradeoff spectrum, and more.

5 CONCLUSION

In this paper, we have considered the problem of organizational readiness for new public key cryptography standards (PQC) in response to the threat of scaled quantum computing (QC). The situation can broadly be described as "Y2Q", or the race between QC technology development and PQC readiness (standards and deployment). We argue that many factors (uncertain timeline, migration complexity, the threat of harvest now, decrypt later) imply the need for near term action and planning. Organizations should put themselves on track early for PQC readiness and develop a phased action plan, working through cryptographic migration challenges before threats and regulatory requirements escalate the situation dramatically.

REFERENCES

Arute, F., Arya, K., Babbush, R. et al. (2019, October). Quantum supremacy using a programmable superconducting processor. Nature, vol 574, pp 505–510.

Bishop, L. S., Bravyi, S., Cross, A., Gambetta, J. M., Smolin, J. (2017). Quantum Volume.

Castelvecchi, D. (2019, October 29). Europe shows first cards on €1-billion quantum bet. Nature.

Chen, L. (2017, July/August). Cryptography Standards in Quantum Time: New Wine in an Old Wineskin? IEEE Security and Privacy.

Chen, L., Jordan, S., Liu, Y-K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D. (2016, April). NIST Report on Post-Quantum Cryptography (NISTIR 8105).

Cloud Security Alliance (2019, June). Mitigating the Quantum Threat with Hybrid Cryptography.

Computing Community Consortium (2019, January 31-February 1). Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. Workshop report.

Crockett, E., Paquin, C., and Stebila, D. (2019, August). Prototyping post-quantum and hybrid key exchange

and authentication in TLS and SSH. NIST Second PQC Standardization Conference.
Dierks, T. and Rescorla, E. (2008, August). The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC 5246.
Dyakonov, M. (2018, November 15). The Case Against Quantum Computing. IEEE Spectrum.
EU. Quantum Flagship funded by the European Commission. https://qt.eu. Accessed December, 2021.
Freund, J. and Jones, J. (2014, September). Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.
Gibney, E. (2019, October 2). Quantum gold rush: the private funding pouring into quantum start-ups. Nature.
H.R.6227 (2018, December 21). National Quantum Initiative Act. https://www.congress.gov/bill/115th-congress/house-bill/6227.
Hosting Facts. Internet stats and facts for 2021. Retrieved December 2021. https://hostingfacts.com/internet-facts-stats/
Housley, R. (2015, November). Guidelines on Cryptographic Agility and Selecting Mandatory-to-Implement Algorithms. IETF RFC 7696.
IBM (2019, January 8). IBM Unveils World's First Integrated Quantum Computing System for Commercial Use. IBM News Room.
IonQ (2018, December 11). IonQ harnesses single-atom qubits to build the world's most powerful quantum computer. IonQ press release.
Katwala, Amit (2019, November 14). Why China's perfectly placed to be quantum computing's superpower. Wired.
Kelly, J. (2019, March 5). A Preview of Bristlecone, Google's New Quantum Processor. Google AI Blog.
Moody, D. (2019, August 22-24). The 2nd Round of the NIST PQC Standardization Process. Talk delivered at Second PQC Standardization Conference.
Moody, D. (2019, September 4). pqc-forum mailing list announcement.
Mosca, M. (2018, September/October). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security and Privacy.
NAS (2019). Quantum Computing: Progress and Prospects. The National Academies Press.
NIST CFP (2017). Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. NIST Post-Quantum Cryptography Call for Proposals.
NIST Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. Accessed December, 2021.
NSA/CSS Information Assurance Directorate (2016, January). Commercial National Security Algorithm Suite and Quantum Computing FAQ" (MFQ U/OO/815099-15).
OASIS (2019, October). Key Management Interoperability Protocol Specification Version 2.0. OASIS standard.
Open Quantum Safe. https://openquantumsafe.org. Accessed December, 2021.
OQS. Contributing Guide. https://github.com/open-quantum-safe/liboqs/wiki/Contributing-Guide. Accessed December, 2021.
PQCrypto (2008-Present). International Conference on Post-Quantum Cryptography. Springer Link.
pqcrypto.org. Web site founded by D. Bernstein and T. Lange. Accessed December, 2021.
Preskill, J. (2011, October). Quantum computing and the entanglement frontier. Transcribed talk from the 25th Solvay Conference on Physics. arXiv:1203.5813v3.
Preskill, J. (2017, December). Quantum computing in the NISQ era and beyond. Paper based on keynote address at Q2B. https://arxiv.org/pdf/1801.00862.pdf
QC Report. Applying Moore's Law to Quantum Qubits. Retrieved January 2020. Quantumcomputingreport.com.
Qureca (2021, July 2021). Overview on quantum initiatives worldwide - update mid 2021. https://www.qureca.com
Rescorla, E. (2018, August). The Transport Layer Security (TLS) Protocol Version 1.3. IETF RFC 8446.
Shankland, S. (2019, December 12). Quantum computing leaps ahead in 2019 with power and speed. C|Net.
Shor, P. (1997, October). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, vol. 26, no. 5.
Stebila, D., Fluhrer, S., Gueron, S. (2019, July). Design issues for hybrid key exchange in TLS 1.3. IETF Internet Draft.
Temkin, Marina (2021, September 13). Investers bet on the technologically unproven field of quantum computing. Pitchbook. http://pitchbook.com
Wallden, P. and Kashefi, E. (2019, April). Cyber Security in the Quantum Era. Communications of the ACM.