A Guide to a Quantum-Safe Organization

Transitioning from today's cybersecurity to a quantum-resilient environment

December 2021 - Updated July 2022

QED-C

Executive Summary

- A large-scale quantum computer, if developed, will **render all commonly used public key cryptography** protocols, which are widely used in key exchange, digital signatures, and authentication, **no longer secure.** Broken digital signatures could enable bad actors to forge documents that cannot be distinguished from the genuine article. Symmetric keys may also be weakened.

- While quantum computers may be many years in the future, **the timelines for cybersecurity transitions can be just as long;** furthermore, some applications (i.e., key exchange) are **vulnerable today** (via "harvest now and decrypt later" attacks).

- Solutions to transition to quantum-safe infrastructure are coming – government, academic, and industry teams are most notably developing post-quantum cryptography (PQC) and quantum key distribution (QKD). **The most common quantum-safe solution** worldwide for organizations and individuals **will be PQC,** although **there are significant opportunities for QKD** and both solutions can be deployed together.

- IT teams should proactively start by creating an **inventory of all cryptographic systems** that are used; this will be one of the most critical and time-consuming steps of the transition but is fortunately traditional IT work (no quantum physicists required!) and may not require a significant amount of investment.

- Creating a cryptography inventory and adopting "**crypto agility" will be a critical part of the transition** but their benefits extend beyond just protecting against the quantum threat; teams will identify poor legacy cryptography implementations and can replace them to **bolster security against both quantum *and* classical threats,** present and future.

- Quantum-safe solutions **will not be a drop-in replacement,** so testing is required in advance of deployment to understand if hardware needs to be replaced and to ensure interoperability; **hybrid mechanisms** combining classical and post-quantum cryptography schemes are also becoming available and can be deployed now.

- IT and procurement teams must **ask current and prospective vendors for their quantum readiness plans** to clarify who will handle which part of the transition and to ensure that investments that are being made today will position organizations towards quantum resilience.

- It is expected that **transitioning to quantum-safe infrastructure may not be optional** at some point for many organizations who need to remain compliant with FIPS certification and other industry standards. Cryptographic transitions are always difficult and this one will be no exception.

Acknowledgements

Many individuals contributed their perspective and expertise to the development of this report. We extend special acknowledgement to the members of the QED-C Use Cases Technical Advisory Committee (TAC), who were instrumental in scoping our effort and reviewing and refining the final document:

- Santanu Basu, Corning
- JW Bray, GE Research
- Dr. William Clark, General Dynamics Missions Systems
- Dr. Jonathan Felbinger, QED-C / SRI International
- Will Finigan, Aliro Quantum
- Jim Gable, Anametric
- Dr. Noel Goddard, Qunnect
- K Karunaratne, Qubitekk
- Denis Mandich, Qrypt
- Elliott Mason, Young Basile
- Corey McClelland, Qubitekk
- Dr. Celia Merzbacher, QED-C / SRI International
- David Ott, VMware
- Rima Oueid, U.S. Department of Energy
- Dr. William Oxford, Anametric
- John Prisco, Safe Quantum
- William R. Trost, AT&T
- Katherine Ward, General Dynamics Missions Systems
- Damian Watkins, Aperio Global

Several other experts also graciously contributed hours of their time to review and edit the final draft. We thank and acknowledge our review panel for their contributions:

- Nicholas Genise, SRI International
- Brian LaMacchia, Microsoft
- Rafael Misoczki, Google
- Dustin Moody, National Institute of Standards and Technology
- Nicholas Peters, Oak Ridge National Laboratory

This work was conducted on an unclassified basis. All assessments of technology-related progress and feasibility are based on one-on-one conversations with experts and public data. Journal articles and websites are cited where relevant, but much of the insight was gathered through expert interviews. The report was researched and written in collaboration with Newry Corp. and with particular thanks to Kasey O'Malley of Newry Corp.

This publication of the Quantum Economic Development Consortium, which is managed by

SRI International, does not necessarily represent the views of SRI International, any individual member of QED-C or any government agency.

About the Quantum Economic Development Consortium

The Quantum Economic Development Consortium (QED- C) is an industry-driven consortium managed by SRI International. With a diverse membership representing industry, academia, government and other stakeholders, the consortium seeks to enable and grow the quantum industry and associated supply chain. For more about QED C, visit our website at quantumconsortium.org.

The Nature and Timeline of The Quantum Threat

Why should I care?

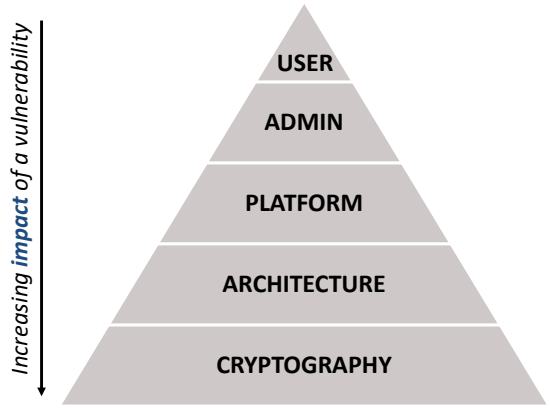
News of quantum computing developments and public and private investment has hit the mainstream media and conference tracks within the last several years at an increasing rate. While many information technology (IT) professionals and chief information security officers (CISOs) are generally aware that quantum computers may threaten the public key infrastructure (PKI) and other cybersecurity protocols, the situation is complex, so the Quantum Economic Development Consortium (QED-C) developed this guide as an overview to make it easier to plan ways to address these new vulnerabilities.

The "blast radius" of a cryptographically relevant quantum computer would be significant, as public key protocols are used across the public and private sector to secure website connections, banking transactions, email exchanges, virtual private networks (VPN), e-commerce, digital signatures, and more. Boston Consulting Group (BCG) estimates that PKI enables more than 4.5 billion internet users to securely access 200 million websites and engage in $3 trillion of retail e-commerce annually [1]. The World Economic Forum similarly predicts that over 20 billion digital devices will need to be upgraded or replaced globally in the next 10-20 years to use quantum-safe cryptography [2].

Introduction

Security vulnerabilities can take a variety of forms. They may stem from something as localized as user errors – including poor passwords and opening phishing emails – or from farther-reaching administrative, platform, or architecture flaws arising from missed software upgrades or misconfigured implementations. Recent attacks such as the T-Mobile, Colonial Pipeline, and Solar Winds incidents have exposed the vulnerability of existing cybersecurity infrastructure to bad actors and have illustrated that even a single breach from a localized user error can cause significant supply chain disruption and cost billions of dollars.

DATA BREACH CAUSES



- The IBM Cost of a Data Breach Report estimates the average cost of a data breach in 2020 was $3.86 million
- User-level attacks – e.g., compromised credentials (19% of all attacks), phishing (14%), business email compromise (5%) – account for most breaches today
- Other common data breach targets, including cloud misconfiguration (19%) and vulnerability in third-party software (16%), are further reaching than user-level attacks, but none threaten public key cryptography

Future threat: quantum computer attack

Public key cryptography underpins the security of a significant share of data and transactions. While most data breaches are caused by more localized errors today, a quantum computer could break the foundational cryptography layer and therefore have an even greater impact.

Source: QED-C, figure adapted from Hudson Institute, data from IBM Cost of a Data Breach Report 2020

Given the volume and diversity of threats that CISOs face today, it is easy to dismiss the threat posed by quantum computing simply because it is longer term. Many articles on the topic diminish concerns by stating that we are a decade away from a large-scale quantum computer capable of cracking current cryptographic algorithms. However, given the potentially massive consequences of a cryptographically relevant quantum computer (general purpose or special purpose) emerging sooner than anticipated, it is clear that this is an issue that we cannot ignore. Experts predict the advent of the quantum age could represent an "extinction event" for today's public key cryptography, so CISOs need to proactively think about preparing for this once-in-a-generation transformation of cybersecurity. Furthermore, the possibility of adversaries storing communications today so that they can decrypt them in the future is another motivation for acting now. Other cryptographically relevant computers (e.g., optical or neuromorphic computing) are also being developed, but the focus of this paper is on quantum computing.

Fortunately, there are many actions that IT professionals can take today to proactively evaluate the quantum threat, identify potential vulnerabilities in their systems, and prepare. Preparation does not require a quantum physicist – IT professionals can plan for and execute transition plans as they have before for other obsolete cryptographic protocols, including Secure Hash Algorithm (SHA-1), SHA-2, Rivest, Shamir, and Adleman (RSA) -1024, RSA-2048, etc. The lifetime of cryptographic algorithms is finite, necessitating adjustments as computers and hackers become more sophisticated. The quantum threat is just another evolution and transition that IT professionals will need to manage.

Overview of Threat Posed by Quantum Computing

Quantum computers exploit quantum properties, which allow them to solve certain types of problems much more quickly than classical computers; these problems include integer factorization, simulation, optimization, database searching, and others. They will not replace classical computers but will be specialized machines or used as co-processors. While this computing power is expected to create positive outcomes via discovery of new materials and drugs, supply chain optimization, disease diagnosis, and more, it can also enable bad actors to crack most of the world's existing cybersecurity protocols.

Current encryption protocols, including Transport Layer Security (TLS), rely on both public key and symmetric key algorithms to secure communications. They depend on problems that are practically intractable for classical computers, including finding the factors of the product of large prime numbers. Where it might take a current supercomputer many thousands of years to crack these problems, a cryptographically relevant quantum computer, if developed, may only take hours to accomplish the same task.

The degree of impact will vary by type of encryption protocol:

- ***Asymmetric public key (e.g., RSA-2048, ECC-P256)*** – A large-scale quantum computer capable of running Shor's algorithm will see exponential speed-ups compared to classical computers. As a result, public keys based on common algorithms like RSA and ECC, which are widely used for digital signatures and key establishment, will no longer be secure. Many key exchanges are vulnerable to "harvest now and decrypt later" attacks, meaning adversaries can infiltrate networks and databases now and store the encrypted data, knowing that they will be able to rapidly decrypt it once a cryptographically relevant quantum computer is developed. Digital signatures will also be vulnerable to Shor's algorithm, and there is added risk of bad actors releasing fraudulently signed documents that cannot be distinguished from the genuine article. It is thus critical to prepare early because the post-quantum-based validation technology must be deployed in advance. Asymmetric public key decryption is considered the greatest threat posed by future quantum computers.
- ***Symmetric key (e.g., AES-256)*** – A large-scale quantum computer capable of running Grover's algorithm will see quadratic speed-up compared to classical computers. Some forms of symmetric cryptography are more vulnerable than others [3]. In general, doubling key sizes would provide comparable security

to protect against a quantum attack; however, not all applications can move to larger key sizes due to memory limitations. Many legacy systems and even new, smaller Internet of Things (IoT) devices will need to turn to new alternatives.

- Authentication, which is used to verify the identity of a user or device prior to information exchange, is also at risk. Authentication schemes use the same public key signature protocols described above and are therefore susceptible to a quantum-based attack. Message authentication code (MAC) and authenticated encryption with associated data (AEAD) modes in these schemes are at risk of an attack by Grover's algorithm.

QUANTUM IMPACT BY TYPE OF CRYPTO PROTOCOL

Crypto Protocols	Use Case	Quantum Impact	Urgency
Asymmetric (public key) – RSA, DH, ECC	Key Exchange	No longer secure – Shor's algorithm	**Highest** – vulnerable to "store now and decrypt later" attack today
	Digital Signatures, Authentication	No longer secure – Shor's algorithm	**High** – will not be secure as soon as an adversary has a powerful enough quantum computer
Symmetric – AES	Encryption	Weakened – Grover's algorithm	**Moderate** – would require much larger quantum computer (Grover's algorithm is less efficient vs. Shor's); can move to larger key sizes to preserve security
MAC, AEAD	Authentication	Weakened – Grover's algorithm	**Moderate** – risk of attack

Source: QED-C
Abbreviations: Rivest, Shamir, and Adleman (RSA), Diffie-Hellman (DH), Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), Message Authentication Code (MAC), Authenticated Encryption and Associated Data (AEAD)

If caught unprepared, the impact could extend into the past and future. Many critical financial documents and legal agreements (e.g., wills, real estate agreements) are digitally signed, and if a bad actor cracks the key, they could effectively rewrite the past, which could have severe financial consequences.

Assessing the Risk and Timing of the Threat

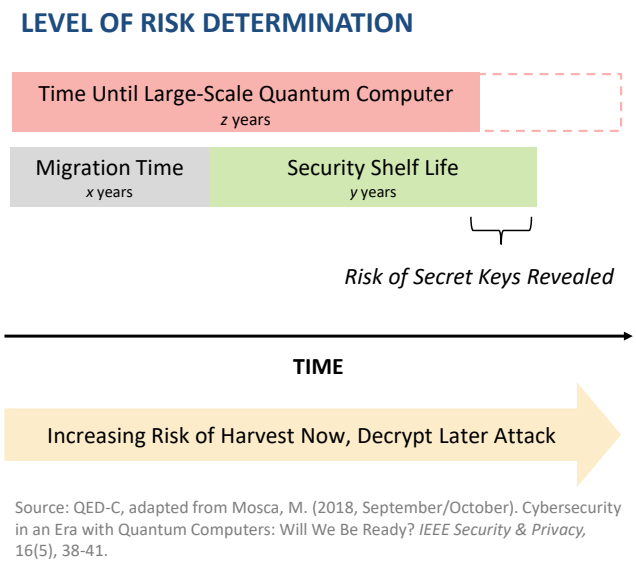
Companies have different risk profiles and may need to prepare differently for the quantum threat. The framework below, developed by Michele Mosca of the University of Waterloo, a quantum cryptography authority, provides a mental model for how organizations can start to assess their risk.

The first variable to consider is the migration time – i.e., how long it will take to transition to a quantum-secure environment. Migration time will vary between organizations based on the volume and diversity of assets and applications. Experts estimate that it will take 10+ years to transition to quantum-safe cryptographic protocols, which may be optimistic given that it took 20 years for AES to replace DES and 3DES [1]. Organizations should not underestimate the time to transition – quantum-safe protocols will not be simple drop-in replacements because:

- Post-quantum cryptography (PQC) protocols are new solutions that still need to be tested in real-world applications. Thorough testing and experimentation will be critical to ensure interoperability.
- PQC-enabled protocols are larger than current PKI protocols, so organizations need to test and reconcile implications for network performance and hardware upgrades. Embedded systems may be constrained by memory size, compute resources, and power availability. Thus, IoT devices may be severely affected.
- The magnitude of the changes required is also massive given that PKI underpins so much of the public internet, which has many cascading dependencies.

Security shelf life – i.e., how long data needs to remain secure – is the second variable that will also vary among applications, organizations, and industries. Because encryption relying on the current PKI is vulnerable to "harvest now and decrypt later" attacks, any data that needs to remain secret 10-20 years from now is already at risk. "Harvest now and decrypt later" attacks refer to the possibility that eavesdroppers may already be tapping communications networks today and storing encrypted data, knowing that they will be able to rapidly decrypt it in the future once a cryptographically-relevant quantum computer is developed. The most stringent requirements for security shelf life may be industry-specific – e.g., government, financial, and healthcare – to protect information such as national intelligence, intellectual property and trade secrets, and personally identifiable information.

Long-lasting hardware that uses over-the-air authentication for updates may still be in the field when a cryptographically relevant quantum computer is developed and could therefore also be at risk. For example, vehicles are often on the road for 10-15 years, and a sufficiently capable quantum computer might be developed in that time. If that happens, adversaries could potentially use a quantum computer to crack the authentication protocol and hijack the system by sending malicious software updates. Many industrial IoT devices are also present in the field for long periods of time and, due to performance constraints, they may remain vulnerable. Critical infrastructure, which uses operational technology (OT) networks, is one of the most extreme examples given the long expected lifetime of infrastructure assets.



Source: QED-C, adapted from Mosca, M. (2018, September/October). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy,* 16(5), 38-41.

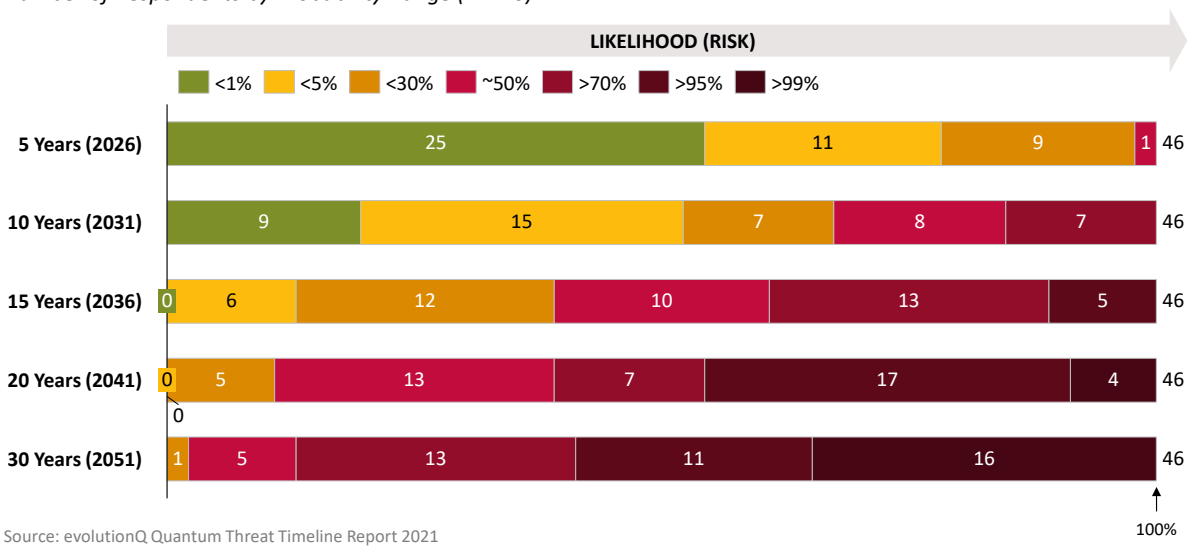
In the Mosca model, shown to the left, the first two variables (x and y) need to be added together to estimate how much time an organization needs to transition. The model assumes that data is being exposed to potential harvesting just before the migration is fully completed (i.e., at time x) and that the data is vulnerable for the full shelf life (i.e., y) after that migration completion time. Data exposed before the completion time is also vulnerable for the full shelf life, but its utility will expire before the data that was exposed just before the migration is completed. Thus, the sum of the first two variables (x and y) provides an estimate of how much time organizations need to transition to quantum-safe security protocols. One can compare this figure to z, which is the estimated time until the successful development of a large-scale quantum computer capable of cracking PKI. Informed by a survey of industry experts, Michele Mosca estimates that there is a 50-50 chance of cracking RSA-2048 by 2031 [4].

The estimates in the chart below are based on when we may have a quantum computer capable of running Shor's algorithm, but different protocols will be broken at different rates. For example, ECC may be more vulnerable to attack than RSA for key sizes of comparable classical resistance [5]. Factors that could accelerate the timeline to cracking RSA or similar protocols include:

- Faster-than-expected scaling of quantum computing capability via increased number of qubits (quantum bits) available and decreased error rates
- Specialized quantum computers purpose-built to run specific algorithms developed in advance of general-purpose quantum computers
- Developers optimizing Shor's and other quantum algorithms to work more efficiently – i.e., with fewer qubits
- Development of a new algorithm capable of breaking public key algorithms like RSA and ECC more efficiently than Shor's

EXPERT ESTIMATES ON THE LIKELIHOOD OF A QUANTUM COMPUTER BEING ABLE TO BREAK RSA-2048 IN 24 HOURS AS A FUNCTION OF TIME

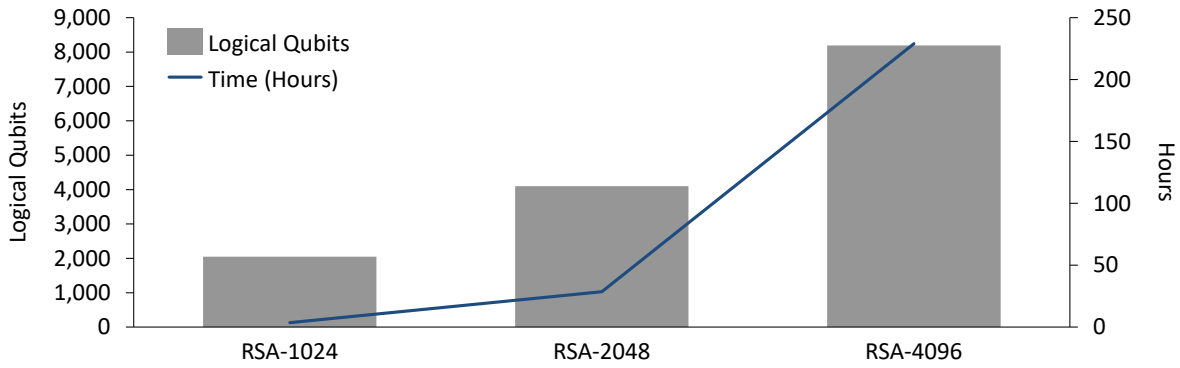
Number of Respondents by Probability Range (n = 46)



Source: evolutionQ Quantum Threat Timeline Report 2021

Tracking quantum computing progress is proactive, though it can be challenging as different developers report progress using different units (e.g., physical qubits, logical or algorithmic qubits, quantum volume, etc.), so making an apples-to-apples comparison is not always possible. IT teams should be aware of this nuance as they interpret the implications of quantum computing advancements. Multiple variables (e.g., number of qubits, error rates, circuit depth, and qubit connectivity) are relevant to assess whether a quantum computer is cryptographically relevant, and it will vary by the type of quantum computer. Defining all of these variables is beyond the scope of this paper but there are recommended references at the end. One example metric to monitor is logical qubits, considered by many to be a fundamental unit of a scalable quantum computer. A logical qubit comprises multiple underlying physical qubits that together act as a single qubit with lower error rates. At this time, a significant number of physical qubits would be required to produce one logical qubit, and no system has produced a single logical qubit yet. About four thousand logical qubits are expected to be needed to crack RSA-2048, and teams can accordingly track progress toward this goal [5].

LITERATURE-REPORTED ESTIMATES OF RSA QUANTUM RESILIENCE BY KEY LENGTH



Source: QED-C, data from National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects.* Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

Preparing a Quantum-Secure Environment

What solutions are available?

Several quantum-secure solutions are in various stages of development at standards development organizations and private companies. The leading approach to building quantum-safe solutions for information security purposes is post-quantum cryptography (PQC). PQC consists of various algorithms designed to be resilient to quantum computing attacks and is intended to replace today's key establishment and digital signature algorithms (e.g., RSA). The second major approach to quantum security employs quantum science directly within networks to exchange encryption keys in a more secure way – a technique called quantum key distribution (QKD). The most common quantum-safe solution worldwide for organizations and individuals will be PQC, although there will be applications for QKD and both solutions can be deployed together.

Post-Quantum Cryptography (PQC)

Post-quantum cryptography is a class of asymmetric crypto-based methods designed to be quantum-resistant – i.e., they are based on math that gives no advantage to a quantum computer (and that a classical computer cannot solve efficiently either). These protocols are being developed to replace quantum-vulnerable algorithms (e.g., RSA, Diffie-Hellman, and ECC).

Most applications will adopt PQC in some form because it is designed to work on today's distributed infrastructure and internet. As a software-based approach, it can work across the existing public internet and theoretically can be implemented in existing hardware, which reduces the overall transition cost. However, because PQC algorithms can be up to 10 or even 1,000x more computationally intensive than classical algorithms, they do come with higher processing overhead [6]. In reality, a software-upgradable "drop-in" replacement (e.g., via a simple application programming interface [API] call) will not be possible in many instances [7]. For example, some IoT devices do not have the computational horsepower nor the memory required to execute PQC-based key establishment mechanisms. Hardware upgrades may thus be required to ensure that memory, speed, and / or entropy requirements are met without sacrificing secure functionality. The average lifetime of many IoT devices may make this impractical. Industrial control systems or other devices in the field which may be more challenging to upgrade could be a more natural fit for QKD [8].

Organizations will also need to invest in crypto agility, which is the ability of a security system to be able to quickly switch between algorithms and cryptographic primitives. Crypto agility will be critical for adopting new PQC algorithms now and updating them in the future as new ones become available. Like today's current public-key algorithms, PQC algorithms may still be susceptible to future classical or quantum computing attacks. In addition to replacing algorithms, organizations may need to adapt their cryptography to include multiple cascaded schemes (known as "defense in depth") to combine classical cryptography and PQC in a hybrid scheme.

The National Institute of Standards and Technology (NIST) is actively working to standardize PQC algorithms. They began a competition-like process in 2016 and have worked through three prioritization rounds to date with the announcement of the first selections in 2022. Each option presents tradeoffs, and NIST evaluated the different options to compare security (against both classical and quantum attacks), performance, and other factors (e.g., open intellectual property (IP) due to a preference for patent-free

NIST STANDARDIZATION PROCESS ROUND 3 SELECTIONS

Application	Selections	4th Round Candidates	Not Selected
Key Exchange Mechanisms (KEMs) / Encryption	CRYSTALS-KYBER	BIKE Classic McEliece HQC SIKE	NTRU NTRUprime SABER FrodoKEM
Signatures	CRYSTALS-Dilithium Falcon SPHINCS+	none	Rainbow GeMSS Picnic

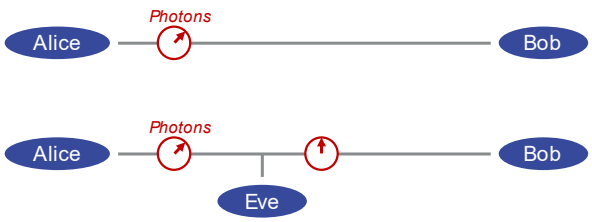
schemes, drop-in replacements, resistance to side-channel attacks, simplicity and flexibility, misuse resistance, etc.). The final selections were announced on July 5, 2022, and draft standards will be released for public comment either later this year or in 2023, with the goal of releasing the first set of standards by 2024. One algorithm, CRYSTALS-KYBER, was selected for key encapsulation mechanisms (KEMs), while three others - CRYSTALS-Dilithium, Falcon and SPHINCS+ - were selected for signatures. Further revisions will come after this initial selection, so organizations must prepare for a continual wave of updates and transitions.

Various companies and academic groups have already developed libraries, such as the Open Quantum Safe project, that include the final selections and fourth round candidates [9]. They are available to collaborate today for pilot projects and to help teams anticipate how new schemes could impact network performance so they can prepare for the transition accordingly. Some major cloud providers are preparing to support hybrid post-quantum TLS. Additionally, NIST has revised an existing standard to allow for piloting a NIST-approved classical algorithm with a post-quantum one so that security levels are not reduced, but a hybrid approach is employed.

Quantum Key Distribution (QKD)

QKD is a hardware-based approach that leverages the principles of quantum physics to facilitate more secure key exchange between two parties. It involves sending photonic qubits (quantum information) either over fiber or in free space (line-of-sight, for example, satellite communications links) to one or both of the parties. When a bad actor attempts to 'eavesdrop,' it perturbs the photons in a detectable way due to quantum effects. Secrecy is ensured because the communicating parties will know if their connection has been compromised. Information leakage can then be mitigated through known techniques such as privacy amplification. While commonly framed as a solution to the quantum threat to RSA and other encryption methods, the concept of QKD pre-dates Shor's algorithm. QKD is a more general solution that may increase security for exchanging secret keys, or otherwise establishing shared secret information that can be used for other protocols.

ILLUSTRATIVE SCHEMATIC OF QKD



Source: OIDA Quantum Photonics Roadmap 2020

PROTOCOLS ADDRESSED BY QUANTUM SOLUTIONS

Use Case	Addressed by PQC	Addressed by QKD
Authentication	Yes	No
Key Exchange	Yes	Yes

Source: QED-C

For the task of key exchange, QKD is theoretically secure, meaning that, regarding the algorithms and computing resources used by a potential attacker, it is algorithm-independent and does not rely on any computational complexity assumptions. It also exhibits perfect forward secrecy[1], which is not the case for all key exchange mechanisms. Despite these advantages, there are some limitations that limit the utility of QKD to specific applications. Limitations of current technology include:

- Only suitable for shorter distances (typically a maximum of ~125 km, though 600 km has been demonstrated in the lab with twin-field QKD) and in point-to-point fiber links (unless trusted nodes are used, which can violate the information theoretic security) [10]. Quantum repeaters will extend this distance, obviating the need for trusted nodes, but their development and deployment will likely be on a similar schedule as that of a large-scale quantum computer. Free space approaches, including satellite, have been demonstrated to overcome optical fiber distance limitations.
- Key exchange rates of early QKD technology were limited historically, though they have recently increased to greater than 1 Mbps, thereby not limiting for many applications.
- Requires new, specialized end-point hardware (increasing cost) but in many cases can use existing fiber installations if the appropriate capacity is available.
- Can be used for key exchange and key agreement cryptographic protocols but cannot be used for authentication. While one can authenticate a QKD link manually when installing the network, it is not feasible for non-secure end-point installations and would require additional authentication techniques for regularly reconfigured information networks.
- Presents some risk of hardware vulnerabilities / side-channel attacks; however, many of the side channel attacks associated with QKD (e.g., beam splitting, detector control, laser damage) have been addressed by new protocols.

QKD will not be adopted everywhere (e.g., to secure standard information networks like the public internet) but there are specific applications where the short distance, key exchange rates, and manual authentication process are not practically limiting and where it can bring meaningful advantages. For example, QKD is already being adopted in time-sensitive industrial control systems at electrical utilities to improve grid security. As operators look to protect their utility networks, they sometimes find that traditional PKI infrastructure can be too complex, difficult to maintain, and can present latency and outage risks. By comparison, QKD can in many cases offer reduced complexity over PKI-based security mechanisms and can be installed on existing dedicated point-to-point fiber lines. Up to 90% of substations in the United States are within 20 km of the communication node and most are within 5 km, so the transmission distance limit of QKD, which is limiting in other applications, is not a constraint. QKD is finding additional utility in campus-like installations, 5G (for backhaul or encryption hopping), satellite communications, and data center applications.

Commercial QKD solutions are available from several vendors and development is ongoing to reduce the drawbacks so the solution can be more widely adopted. Security agencies such as the National Security Agency (NSA) advise against the use of QKD for securing the transmission of data in national security systems due to current limitations [11]. However, many installations in Europe, Japan, and, to a lesser extent, the United States, are actively testing and deploying the technology to further validate and refine protocols. In parallel, there are nascent QKD certification efforts underway.

[1]Perfect forward secrecy refers to a feature that guarantees that no key material is ever used more than once between messages and across clients, and compromising any one session key only affects that session. This term says nothing about the strength of the protocol used.

Future Quantum Networks

Future quantum networks will distribute entanglement and use quantum teleportation to transmit quantum information – not just keys. Alternative concepts encode quantum information in error correcting codes composed of many photons to transmit quantum information directly between repeater nodes that do not share entanglement. There are longer-term solutions that extend beyond QKD and are sometimes colloquially referred to as the "quantum internet" because they will extend to more complex network topologies (not only point-to-point) and enable new capabilities. While QKD will be an early application for distributed quantum repeater networks, others include distributed quantum computing and quantum sensor networks.

Future quantum networks are expected to be a critical solution for quantum-safe communications but are not yet ready for commercial deployment because fundamental building blocks (photon sources, quantum memories, error correction, etc.) are still in development. Optimistically, commercial implementation of a basic quantum repeater may be available in the next 2-3 years, so it may be 5 or more years before a basic repeater network with a handful of nodes is available. The Department of Energy recently kicked off multiple test bed projects in October 2021, and while perhaps premature, many experts draw parallels between today and the Advanced Research Projects Agency Network (ARPANET) in the 1970s [12]. As with the classical internet, broader deployment is expected to follow. Given the timeline, end users should adopt other solutions to prepare for the quantum computer threat while being aware that these networks are coming.

Quantum Random Number Generators (QRNG)

Random number generators are at the foundation of nearly all cybersecurity. Pseudo random number generators (PRNGs) are most commonly used today but they use deterministic algorithms to produce deterministic, "statistically random" numbers. Thus, most "random numbers" used today are not truly random. The quality of the randomness can vary, which weakens cryptographic systems as they rely on the unpredictability of the keys. A different class of random number generators, true random number generators (TRNGs), can use classical physical processes to create entropy, but they are typically slow. Quantum random number generators (QRNGs), in contrast, leverage the inherent, provable randomness of quantum mechanics to efficiently create truly entropic keys.

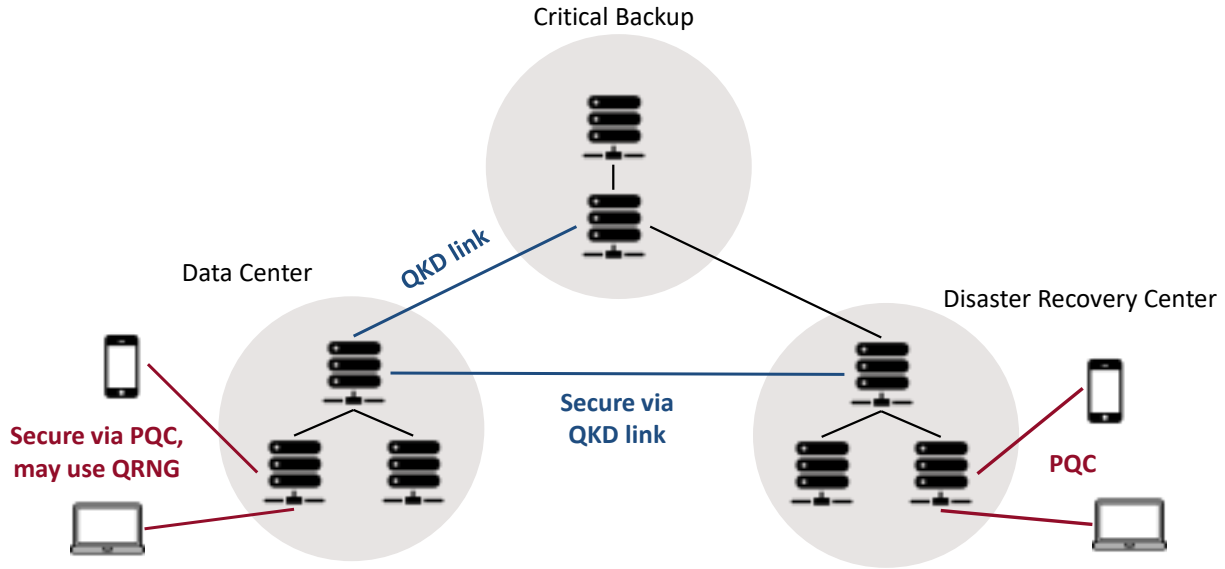
Random numbers are a critical supporting technology because they are used in two-factor authentication and underpin all encryption keys used in classical, PQC, and QKD protocols. Independent of the quantum threat, QRNGs address existing cybersecurity vulnerabilities that result from weak random numbers [13]. For example, machine learning techniques can also attack weak random numbers, which has already put cryptocurrency at risk [14]. QRNGs can be combined with other quantum-safe solutions like PQC to further enhance security. Many PQC protocols need both more random numbers (100 to 1,000x) as well as a different statistical distribution for these random numbers, which has motivated the development of QRNGs to replace PRNGs and TRNGs [6]. QRNGs are also being used in electronic gaming and applications that require simulation of complex systems.

Many QRNG solutions are commercially available today – the hardware has been embedded in hardware security modules (HSMs), other network appliances, and cellphones. Vendors also offer cloud-based solutions. While these solutions are available, organizations are considering certification processes and how to address the supply chain concerns of customers with the most stringent security requirements. QRNGs can potentially demonstrate provably quantum operation, and by implication true randomness, but certification of both the quantum sources and the supporting electronics (e.g., extractors) is needed.

Hybrid Solutions

As the discussion above has highlighted, there are multiple potential solutions available. These technologies are often complementary and can and should be combined in a hybrid manner to maximize effectiveness. In the short term, organizations may consider layering PQC on top of existing classical cryptography to add additional layers of defense, and investments in crypto agility will enable organizations to swap in or layer different algorithms to manage the different stages of the transition in the future.

EXAMPLE HYBRID IMPLEMENTATION



Source: QED-C, adapted from ID Quantique

Hybrid installations could include a combination of post-quantum solutions (i.e., PQC + QRNG). While most end users will adopt software solutions (PQC) to secure their information networks, specific applications may also use QKD (illustrative example shown in the figure below). Organizations must evaluate their requirements and can layer various risk mitigation strategies to suit their assets and applications.

Transition Requirements

What will it take?

It is difficult to predict precisely the total investment that will be required to transition to quantum-safe cryptographic protocols. However, we can look to historical transitions as proxies to provide a frame of reference. For example, symmetric key cryptographic protocols have been replaced several times to increase security in a similar manner to how PQC will replace current PKI algorithms like RSA. DES was approved as a standard in 1976 but was broken in the late 1990s and subsequently retired in 2005. 3DES was then adopted but in 2018 NIST provided guidance for retiring 3DES – replacing it with AES – by 2023. BCG estimates that it took 20 years for the entire ecosystem to replace DES and 3DES with AES [1]. Within a single enterprise it took Blackberry about 5 years to transition from 3DES to AES [15]. Other historical transitions point to similar timelines and levels of investment, as it took 10-20 years to transition from SHA-1 to SHA-2 [15].

Estimates from PQC experts span a similar timescale of 5-20 years. NIST expects it will take 5-15 years after the development of standards [16]. Other consultants have a more conservative estimate of 10-20 years [17]. Timescales will vary depending on whether an organization's assets are enterprise-owned or owned by third parties and whether quantum support services are used.

For investment, Inside Quantum Technology estimates that the market for PQC software and chips will ramp up to $9.5 billion by 2029 [18]. The investment for an individual company will vary significantly based on their scale and the nature of their assets (number, use of the cloud, and compatibility of existing hardware with PQC) and information (criticality and security shelf-life). Simple web-based applications may have an easier transition with simple upgrades to TLS whereas more specialized systems will be more complicated and may require hardware upgrades.

While the investment and time could be significant, organizations should build the quantum-safe transition into their regular lifecycle planning. Procurement should ensure that any new software or hardware will be compatible with PQC to futureproof new infrastructure. The cost of an attack relative to the investment that is required often clearly justifies the upgrades. IBM Security estimates that the average cost of a single data breach is $8.6 million in the US ($3.8 million global average), with energy, healthcare, and retail sectors experiencing the greatest increase in breach costs [19].

Furthermore, as was the case for some historical transitions, transitioning to quantum-safe cybersecurity protocols will be recommended by standards and regulatory agencies for many organizations. Historically, when a new, more secure encryption protocol became available, security policies followed to require them. Certain sectors, such as transportation or critical infrastructure, may be subject to regulatory requirements. Given the international nature of IT technologies, changes may be driven by non-US compliance requirements (such as affected privacy). While this has not happened yet, organizations will likely eventually be required to transition to PQC to remain compliant with Federal Information Processing Standards (FIPS) certification. The IT industry will sunset old, insecure algorithms as with SHA-1, etc.

Practicalities

How can I get started?

There are several steps that organizations can and should be taking today to prepare.

1. *Assign resources* – Designate which person or team will be responsible for developing a quantum-readiness roadmap to manage the transition. Note that a lot of the activity will require traditional IT work that will help general IT modernization efforts. A team of quantum physics PhDs is definitely not needed. Starting early can prevent a rush to implementation, which can ensure quality remains high and costs remain predictable and manageable.
2. *Build awareness* – Engage the community and develop an understanding of PQC and technology readiness levels. Build awareness in procurement teams so they incorporate quantum-safe requirements into requests for proposal (RFPs) for regular lifecycle management. Ask vendors for their quantum-safe plans starting now.
3. *Define responsibilities* – Determine who is responsible for each part of the network. Even if an organization does not do their own software development, it is important to understand what cryptography is used and to ask current and prospective vendors for their quantum readiness plans.
4. *Develop an inventory and priority list* – Review every device, system, code, platform, and vendor that

is used in the organization, and understand what cryptography is used and how encryption keys are generated, stored, and applied. Developing the cryptography inventory may be the hardest part of the transition, but the good news is that building this awareness may help organizations become more secure even before a quantum threat materializes, as any archaic or obsolete systems will be identified. Once the inventory is developed, organizations can prioritize which transitions need to occur first based on:

- Inventory and nature of the data – how critical it is and how long it needs to remain secure.
- Asset lifetime – acknowledging that authentication protocols need to be upgraded.
- Susceptibility to an attack – e.g., key exchange is the highest risk today, as it is vulnerable to a "harvest now and decrypt later" attack.

Organizations also need to estimate the potential future loss related to quantum events and compare that to the capital value of equipment at risk.

5. *Evaluate solutions and implementation options* – Assess how PQC, QKD, and other actions could mitigate vulnerabilities. For each priority, assess what upgrade is possible as a protection mechanism. Companies should prepare to adopt a hybrid security approach, layering PQC in addition to current classical cryptographic algorithms like RSA to further enhance security. Invest in crypto agility to improve flexibility and nimbleness. If a cryptographic primitive of a system is discovered to be vulnerable due to a quantum threat or other attack vector, crypto agility will allow organizations to adapt and replace those algorithms more easily to maintain resilience.
6. *Experiment and test* – While standardization is still in progress, IT teams can test examples in the meantime to prepare for implementation. Experimentation will build awareness and clarify uncertainties about how challenging the transition will be – e.g., whether new hardware will be required to run PQC algorithms. Many cryptography libraries that include the final candidates from the NIST competition are already available.
7. *Continually monitor progress* – Develop relationships with and access to experts to monitor progress and advancements in both quantum-safe solutions and quantum computing developments to continually reassess the timeline and risk level.

There are numerous resources that can help organizations get started on their transition to a quantum-safe cybersecurity architecture. IT teams should engage with vendors and ask them for their plans to identify ways they can support the transition. Large service providers are already developing solutions that implement PQC (e.g., integrating into key management systems, VPN) and several suppliers offer PQC libraries, QKD hardware, and QRNG hardware or services. Participation in industry groups like the QED-C and standards bodies will also help the team remain engaged and informed to enhance understanding of the risk and potential solutions.

Conclusion

The security implications of a large-scale quantum computer capable of running cryptographically relevant algorithms are significant, for individuals, organizations, and national economic security. It is prudent to start making provisions for cybersecurity now, especially given the existing risk of a "harvest now and decrypt later" attack today. Furthermore, quantum-safe infrastructure is expected to become required by standards and regulatory bodies for many organizations. Emerging solutions like PQC and QKD will not be simple drop-in replacements, and the timeline for the transition to quantum-safe infrastructure will span many years. IT teams should be asking current and prospective vendors for their quantum readiness plans to clarify responsibilities. Teams must proactively evaluate which architecture will be required to secure the various types of information that need to be protected from future quantum threats. These architectures may include a hybrid implementation using a combination of PQC, QKD, and existing cryptography. Taking action to protect sensitive information against the future possibility of a cryptographically relevant quantum computer is a critical and immediate need.

Recommended Further Reading

Getting Ready for Post-Quantum Cryptography, NIST, doi: 10.6028/NIST.CSWP.04282021.

Migration to Post-Quantum Cryptography, NIST and NCCoE, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/pqc-migration-project-description-final.pdf

Post Quantum Cryptography: Readiness Challenges and the Approaching Storm, CCC, https://cra.org/ccc/wp-content/uploads/sites/2/2020/10/Post-Quantum-Cryptography_-Readiness-Challenges-and-the-Approaching-Storm-1.pdf

Quantum Threat Timeline Report, Global Risk Institute, https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

Post Quantum Cryptography, DHS, https://www.dhs.gov/quantum

Practical Preparations for the Post-Quantum World, CSA, https://cloudsecurityalliance.org/artifacts/practical-preparations-for-the-post-quantum-world/

The Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity, Hudson Institute, https://www.hudson.org/research/14930-the-executive-s-guide-to-quantum-computing-and-quantum-secure-cybersecurity

References

[1] L. Comandar, J.-F. Bobier, M. Coden and S. Deutscher, "Ensuring Online Security in a Quantum Future," 30 March 2021. [Online]. Available: https://www.bcg.com/publications/2021/quantum-computing-encryption-security.

[2] C. Foley, J. Gambetta, J. Rao and W. Dixon, "Is your cybersecurity ready to take the quantum leap?," 7 May 2021. [Online]. Available: https://www.weforum.org/agenda/2021/05/cybersecurity-quantum-computing-algorithms/.

[3] M. Kaplan, G. Leurent, A. Leverrier and M. Naya-Plasencia, "Breaking Symmetric Cryptosystems using Quantum Period Finding," 2016, doi: 10.1007/978-3-662-53008-5_8.

[4] M. P. M. Mosca, "Quantum Threat Timeline Report 2020," Global Risk Institute, 2020. [Online]. Available: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/.

[5] M. Roetteler, M. Naehrig, K. M. Svore and K. Lauter, "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms," Advances in Cryptology – ASIACRYPT 2017, pp. 241-270, 30 October 2017.

[6] "pqm4 / benchmarks," GitHub, [Online]. Available: https://github.com/mupq/pqm4/blob/master/benchmarks.md.

[7] W. Barker and M. Souppaya, "Migration to Post-Quantum Cryptography," 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2021/08/04/migration-to-post-quantum-cryptography/final.

[8] P. G. Evans, M. Alshowkan, D. Earl, D. D. Mulkey, R. Newell, G. Peterson, C. Safi, J. L. Tripp and N. A. Peters, "Trusted Node QKD at an Electrical Utility," IEEE Access, vol. 9, pp. 105220-105229, 15 April 2021.

[9] "Open Quantum Safe," [Online]. Available: https://openquantumsafe.org.

[10] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," 2021, doi: 10.1038/s41566-021-00811-0.

[11] National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC.

[12] "Department of Energy Announces $25 Million for Research on Quantum Internet to Accelerate Scientific Discovery," [Online]. Available: https://science.osti.gov/-/media/ascr/pdf/funding/2021/QIS-QuantumInternet-Awar_List.pdf.

[13] J. Kilgalin, "The Irony (and Dangers) of Predictable Randomness," 19 December 2019. [Online]. Available: https://www.keyfactor.com/blog/the-irony-and-dangers-of-predictable-randomness/.

[14] J. Dunn, "Blockchain Bandit stole $54 million of Ethereum by guessing weak keys," 25 April 2019. [Online]. Available: https://nakedsecurity.sophos.com/2019/04/25/blochainbandit-stole-54-million-of-ethereum-by-guessing-weak-keys/.

[15] C. Ma, L. Colon, J. Dera, B. Rashidi and V. Garg, "CARAF: Crypto Agility Risk Assessment Framework," 2021, doi: 10.1093/cybsec/tyab013.

[16] W. Barker, W. Polk and M. Souppaya, "Getting Ready for Post Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," 28 April 2021. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932330.

[17] M. Piani and M. Mosca, "Quantum Threat Timeline Report," January 2021. [Online]. Available: https://evolutionq.com/quantum-threat-timeline-2020.html.

[18] Inside Quantum Technology, "IQT Research Report Projects that Post-Quantum Cryptography will Generate $2.3 Billion in Revenues by 2026," 2021. [Online]. Available: https://www.insidequantumtechnology.com/wp-content/uploads/2021/08/final_-_pqc_press_release-1.pdf.

[19] IBM Security, "Cost of a Data Breach Report," 2020.

[20] National Academies of Sciences, Engineering, and Medicine, "Quantum Computing: Progress and Prospects," 2019, doi: 10.17226/25196.

[21] A. Herman, "The Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity," 3 April 2019. [Online]. Available: https://www.hudson.org/research/14930-the-executive-s-guide-to-quantum-computing-and-quantum-secure-cybersecurity.

[22] A. Herman, "The Executive's Guide to Quantum Cryptography: Security in a Post-Quantum World," 1 May 2020. [Online]. Available: https://www.hudson.org/research/15992-the-executive-s-guide-to-quantum-cryptography-security-in-a-post-quantum-world.