Preparing Communications Networks for the Quantum Future

ATIS-I-0000089
February 2022

ABSTRACT

Computational problems that would take a classical computer tens of thousands of years to complete can be solved in seconds by a quantum computer — making quantum computers' power exponentially greater than computers in use today for certain classes of problems. There are concerns, however, that quantum's computational power will eventually compromise current encryption algorithms widely used by network operators. New cryptography algorithms and technologies will be required to secure communications and data against the threat of quantum computers.

Although quantum computing is still in the early stages of development, network operators should begin to understand its implications on current communications and data management. Organizations will need to implement a new approach to assessing crypto agility and risk to the business to be quantum resistant in the future.

FOREWORD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cybersecurity, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

COPYRIGHT INFORMATION

ATIS-I-0000089

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [https://www.atis.org/policy/patent-assurances/] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

TABLE OF CONTENTS

1
INTRODUCTION

The huge leap forward in computational ability to solve certain problems that quantum computing delivers comes from leveraging the quantum properties of entanglement and superposition. While classical bits are independent (i.e., operation on one bit does not impact another bit), operations on quantum bits (qubits) may be made to be correlated using quantum entanglement. Furthermore, unlike the binary bits in classical computing, qubits can exist in a superposition of 0 and 1. This makes it possible to speed up solving specific problems using quantum computers rather than classical computers.

One example of such a problem is factoring the product of two very large primes, which forms the foundation of RSA — a commonly used public key encryption algorithm. While classical computers may require hundreds of years to factor a 2048-bit RSA key, a future quantum computer may be able to do so in a day [1][2]. As a result, future quantum computers using Grover's search algorithm may have the potential to weaken private key cryptography, which uses symmetric key encryption [3].

All digital infrastructure that permeates every sector and part of society uses cryptography to secure and protect them, including – communications, remote connections, computing, IoT devices, etc. Cryptographically Relevant Quantum Computers (CRQC), ones able to break the encryption used for information and secure communication, do not yet exist. However, information encrypted with current cryptographic techniques can be intercepted, stored, and decrypted once such computing capabilities materialize. The retrospective decryption of encrypted data is a genuine threat; thus, any critical data requiring long-term security should be identified and protected now if necessary.

To advance operators' and users' needs in this area, the ATIS Quantum-Safe Communications and Information Initiative (QSCII) brought together industry experts to develop a roadmap of work items, aligned with industry best practices and other quantum standards initiatives. In addition, the initiative is also addressing key regulatory, governance, and interoperability implications to enable quantum-safe security.

This white paper provides a high-level overview of the current activities to ensure communications and information will be resistant to quantum threats in the future. It discusses the potential risk areas for communications infrastructure and the potential timelines for when those risks will emerge, identifying indicators for organizations to assess crypto agility and business risk so that they can plan for this eventuality. These key indicators include:

- Creating awareness of the quantum threat and risk to security.
- Implementing a new approach to managing security.
- Assessing the enterprise's readiness to become crypto-agile and resistant to future classical or quantum threats.
- Monitoring the development of postquantum cryptography standards and solutions.
- Getting started by acting today to set their organization on a path to be quantum resistant.

2
THREAT TIMEFRAME

Quantum computers are information processing devices that implement mathematical computations using quantum mechanical physical phenomena. Quantum computers can theoretically solve specific types of math problems that are intractable on classical computers.

Quantum computing was first proposed in the 1980s, with interest growing in the 1990s by the introduction of Shor's algorithm. This algorithm exponentially speeds up a class of cryptoanalysis, which potentially threatens some cryptographic methods currently used to protect government, enterprise, and civilian stored data and communications.

Since the early 2000s, significant progress has been made in the development of quantum computers. Trapped ions and superconducting qubits are the leading technologies for quantum computing today. Although trapped ion and superconducting quantum computers are now available for experimentation, these systems are limited due to the modest number of qubits with limited coherence time and connectivity. Furthermore, quantum gate operations currently have poor fidelity.

A quantum computer design that can scale to the appropriate size and achieve good-enough fidelity to break current cryptography doesn't exist today, nor is it clear that it can be achieved by straightforward scaling of any of the current implementations. The key properties that determine a quantum computer's capabilities are the qubit coherence time, the inter-qubit connectivity, the number of qubits, and the single-qubit and two-qubit error rates. It is generally accepted that error rates in quantum computers will never be as good as in classical computers. Therefore, significant research is in progress to incorporate error correction during the computation process.

Today's quantum computers are referred to as Noisy Intermediate Scale Quantum (NISQ). They lack the ability to perform Shor's and Grover's algorithm at the magnitude needed to currently impact cybersecurity. Full-scale, fault-tolerant (largely superconducting) quantum computers — the kind that can solve BIG problems — are still a long way off. Regardless of the type of quantum technology, we are concerned with CRQCs because those are the systems that will start breaking modern encryption algorithms. Building a quantum computer that delivers the key properties at a sufficient level to break current cryptography is a formidable task due to scientific and engineering obstacles. We do not know when fault-tolerant quantum computers will have sufficient scale and quality to threaten cryptography. However, we can track progress made towards achieving key milestones to help us gain insight into when the quantum computer threat will become real.

The National Academies of Sciences, Engineering and Medicine report on Quantum Computing [4] proposes several milestones and metrics to track progress in Quantum Computing. Their report finds that RSA 2048 cryptography will be safe for the next decade.

The Global Risk Institute in their Quantum Threat Timeline report 2021 [5] surveyed 47 thought leaders in key relevant areas of quantum science and technology. These experts were asked to provide estimates about the development timeline for quantum computers, specifically for quantum computers powerful enough to pose a threat to cybersecurity. 46 out of the 47 experts contributing overall— suggest that the quantum threat is becoming more and more concrete.

Specifically, within the next 15 years, more than half (28/46) of the respondents indicated the threat would be likely or more likely. This time frame appears as a tipping point, as the number of respondents estimating a likelihood of "about 50%" or larger, become the majority. This opinion study suggests the quantum threat has a more than even chance of being realized in 15 years. Figure 1 reproduces the summary of opinions of 47 experts surveyed on the likelihood of a significant quantum threat to public-key cybersecurity as a function of time.

Quantum computer technologies have a very limited track record due to it being a young field. Because of the small amount of experience with quantum technologies, predictions about quantum computing are based on educated guesses. As the technology matures and data is accumulated, predictions will be driven by extrapolation of past trends. We plan to periodically revisit the progress made toward key quantum computing technology milestones to provide updates to the threat timeline.

The takeaway message is that quantum computing differs from classical computing and, in principle has computational advantages in cryptographic problems that are intractable for classical computers. Thus, it has the potential to undermine the current communication and information security. However, due to overwhelming science and technology challenges, it is not clear when a quantum computer will be developed that will be powerful enough to threaten current cryptography.

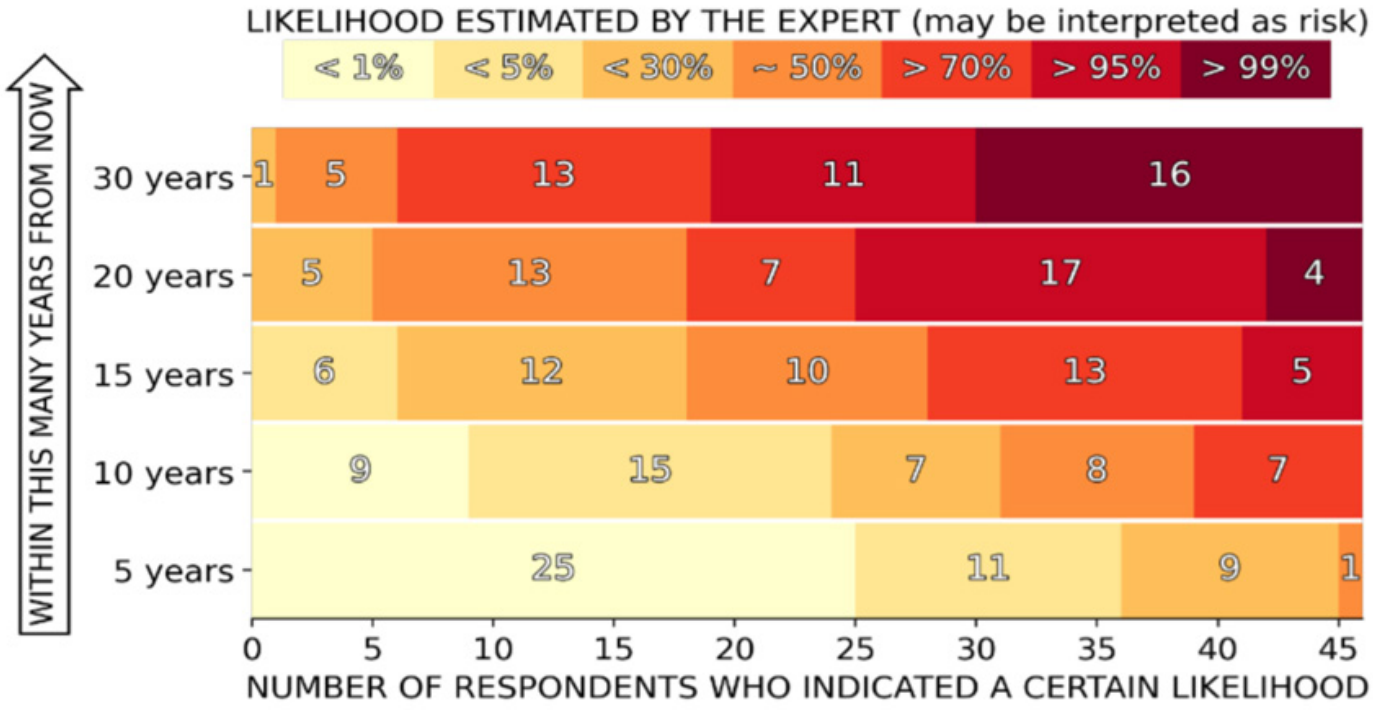

Figure 1: Expert Opinions on the Technical Realization of Quantum Computers. [5]

3
IMPACTS TO CURRENT CRYPTOGRAPHY

Quantum computer technologies have a very limited track record due to it being a young field. Because of the small amount of experience with quantum technologies, predictions about quantum computing are based on educated guesses. As the technology matures and data is accumulated, predictions will be driven by extrapolation of past trends. We plan to periodically revisit the progress made toward key quantum computing technology milestones to provide updates to the threat timeline.

The takeaway message is that quantum computing differs from classical computing and, in principle has computational advantages in cryptographic problems that are intractable for classical computers. Thus, it has the potential to undermine the current communication and information security. However, due to overwhelming science and technology challenges, it is not clear when a quantum computer will be developed that will be powerful enough to threaten current cryptography.

Quantum computers exploit two properties of quantum mechanics. This makes them superior to classical computers, namely in terms of superposition and entanglement. This will allow quantum computers to solve certain types of problems more quickly than classical computers. Two such problems are factorization (and the discrete logarithm problem) and the ability to search unstructured data more quickly. Current public encryption algorithms such as RSA and Elliptic Curves, commonly used in Transport Layer Security (TLS) and Secure Socket Layer (SSL), are based on the intractability of factorization and computing discrete logarithms.

Figure 2 summarizes the algorithm types, purposes, impacts and quantum attack vectors. Symmetric key encipherment is based on unstructured algorithms, which could be attacked by using a quantum computer to search through large amounts of unstructured data. On the other hand, PKI is at much greater risk once a CRQC becomes available.

Encryption Algorithm	Type	Purpose	Impacts	Quantum Attack
AES, DES	Symmetric Key	Encryption	Larger Key sizes needed	Grover's Algorithm
RSA, Elliptic Curve (ECC), Diffie-Hellmann (DH)	Public Key	Encryption Digital Signatures	No longer secure	Shor's Algorithm
SHA-2, SHA-3	Hash	No longer secure	Use larger digests	Grover's Algorithm

Figure 2: NIST Overview of Algorithm Types and Quantum Attack Vectors

Quantum computing, in principle, has the potential to disrupt both public and private key encryption schemes, which are ubiquitous in securing communications, including web traffic, especially when it comes to accessing medical records or financial transactions such as banking and online shopping. The bottom line is if and when a CRQC is available in the future:

- **No online system can be trusted anymore** because the current key establishment and key exchanges can be breached.
- **No online presence can be trusted to be authentic** because current digital signatures can be hacked.
- **Transaction non-repudiation becomes invalid** because current signature algorithms can be forged.

4
MITIGATING TECHNOLOGIES AND RELATED RESEARCH

This section provides an overview of some of the technologies being developed that could be used to improve security toward being quantum resistant.

Post-Quantum Cryptography (PQC)

There is a clear need for new public key encryption algorithms that will be resistant to quantum computing to replace the popular RSA and Elliptic Curves, which are currently prolific in most secure transactions. Since 2016, the National Institute of Science and Technology (NIST) has been working publicly on this very problem, with the goal of identifying a new class of asymmetric key encryption algorithms that are quantum resilient. By using different mathematical foundations than classical public key algorithms, the new algorithms are believed to be more difficult to solve by quantum computers.

After the original call for algorithms in 2016, NIST has gone through several rounds of reviews, with the third-round candidates announced and ratified in July 2020 [4]. Figure 3 depicts the current timeline. At the time of this report's publication, NIST was on track to announce the finalist sometime in 2022, with the finalized standard being published in 2024.

Figure 4 shows the round 3 finalists with these algorithms. These algorithms fall into a small class of mathematical properties that include lattice-based, multivariate, code-based, hash-based, and elliptic curves with isogenies. In many cases, the impacts of these new algorithms are not yet well understood, especially in the cases of small handheld devices and IoT. These algorithms all have significantly larger public keys, signatures, and, in some cases, ciphertext, which results in much larger communication overhead. However, in some cases the amount of computation required is actually smaller. One key feature of PQC is that it is based on mathematics, and today there is no proof that these algorithms cannot be broken in the future. The potential to harvest encrypted data now and decrypt later could be a threat that will persist even with PQC.

Figure 3: NIST – PQC Project Timeline

Type	Finalists	Alternates
Public Key Encryption and Key Establishment	Classic McEliece	Bike
	Crystals-Kyber	FrodoKEM
	NTRU	HQC
	SABER	NTRU Prime
		Sike
Digital Signature Algorithm	Crystals-Dilithium	GeMSS
	Falcon	Picnic
	Rainbow	Sphincs+

Figure 4: NIST Round 3 Finalist

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a hardware-based approach that utilizes the quantum property of no cloning (i.e., you cannot measure a quantum state without changing its value [6]), to exchange a symmetric key securely. QKD systems are theoretically secure against a computationally bounded adversary (i.e., keys exchanged using QKD can be used as a one-time pad). In practice, key rates for current QKD systems do not allow such use. Instead, the keys are used in combination with a classical symmetric key encryption algorithm such as AES.

QKD systems may operate over fiber or free space. Over fiber, current commercial systems have a limited transmission distance due to signal attenuation. Unfortunately, classical signal amplification techniques cannot be used with quantum channels due to the no-cloning theorem. To address this limitation, fiber-based QKD systems can be used in combination with trusted repeaters, which violates provable security, or with quantum repeaters, which currently do not exist. There are ongoing efforts to extend the range of fiber-based QKD systems.

Free-space QKD systems are limited by line of sight and atmospheric conditions. Commercial vendors in this space have focused on satellite-based solutions. Additionally, there are academic efforts to implement drone-based free-space QKD. A representative overview of various QKD implementations, as well as their limitations, is **available here** [7].

The practical utility of all QKD systems is also impinged by the need for expensive specialized hardware. Most QKD systems require accurate detection of single photons. These detectors drive the cost of a QKD system. At the time of writing, a pair of QKD nodes are quite expensive.

In 2021, NSA highlighted deficiencies in the QKD system implementation for U.S. government use, but QKD technology has been readily adopted in the U.S., Europe, China, and Japan.

Quantum Random Number Generator (QRNG)

Random number generators (RNGs) have played a big part in nearly all of cybersecurity and are at the kernel of many encryption algorithms. Deterministic classical computers are incapable of generating pure random numbers, so they rely on specialized noise circuits to seed a deterministic algorithm to produce pseudo-random numbers.

There is a new class of RNGs that leverage quantum mechanics. The beauty of these QRNGs is that they provide perfect entropy or randomness (in theory) and thereby eliminate the potential for a bias or pattern to be realized in the underlying cryptography. This means QRNG is promising because randomness is a key aspect of cryptography.

5
COMMUNICATION INFRASTRUCTURE AT RISK

The security and privacy of online communication are currently protected using cryptography, which shields information as it travels around the internet. The same cryptography also ensures the security and integrity of the digital infrastructure on which these secure communications are delivered, including internet infrastructure, mobile communications infrastructures, access control systems, identity systems, secure data stores, and more. Here we highlight some areas that will need to adapt to be quantum resilient.

In general terms, the security aspect of communication infrastructure of all types will be affected if and when a CRQC emerges to break current cryptography. As a result, new security stacks will need to be implemented across the entire communication infrastructure landscape to maintain the current level of security. The following sections highlight the vulnerabilities in some of the application areas.

Internet Infrastructure

Media Access Control Security (MACsec)

MACsec provides security of data between Ethernet-connected devices. IEEE standard 802.1AE defines the MACsec protocol. Initially, MACsec secured the link between two physically connected devices, but in its current form can secure data communications between two devices, regardless of the number of intervening devices or networks.

One of the most compelling cases for MACsec is that it provides Layer 2 (OSI data link layer) security. This enables it to safeguard network communications against a range of attacks, including denial of service, intrusion, man-in-the-middle, and eavesdropping.

With MACsec as the foundational security technology for safeguarding data in motion across Ethernet networks, the use cases are many:

- WAN/MAN routers
- Data center routers and switches
- Server, storage, and top-of-rack switches
- LAN switches
- Secure endpoints such as security cameras and industrial robots

The demand on MACsec in Ethernet is substantially increasing because MACsec is a good fit for industrial applications, which require strong security and efficiency. In addition, MACsec can support secure communication of data with low latency for real-time 5G applications.

To provide a long-term security, the MACsec protocol should be resistant to future attacks, including quantum ones [8].

DNS Security Extension (DNSSEC)

DNSSEC creates a secure domain name system (DNS) by adding cryptographic signatures to existing DNS records. DNSSEC protects internet users and applications from forged DNS data by using public-key cryptography to digitally sign authoritative zone data when it enters the DNS and then validates it at its destination. These digital signatures are stored in DNS name servers. By checking its associated signature, you can verify that a requested DNS record came from its authoritative name server and was not altered en route, as opposed to a fake record injected in a man-in-the-middle attack.

The characteristics of DNSSEC rely on very low latency of signing and validation, where resolvers need to validate thousands of signatures per second, and signing is time critical. Furthermore, keeping the signed messages within a single

Maximum Transmission Unit (MTU) is critical to ensure performance is not impacted. Replacing the signature algorithm generated by a post-quantum algorithm may result in a signature exceeding a single MTU and cause further delays [9].

5G Infrastructure

5G is used to connect more than just mobile phones, expanding the so-called threat surface. In time, self-driving cars and personal medical technology could both depend on 5G to operate.

The security of the mobile telecommunications infrastructure has relied on cryptography since the advent of the GSM system. 5G mobile network infrastructure is a distributed architecture of microservices, each existing as an app in the cloud and communicating using web service APIs with other components over a 5G signaling protocol. These distributed services are provisioned dynamically within a cloud environment. They rely on the trust, integrity, and security of the hardware, software, and connections in the form of HTTPS, Extensible Authentication Protocol (EAP), Internet Key Exchange Protocol Version 2 (IKEv2), Transport Layer Security (TLS) and OAuth2.0 Authorization Framework to authenticate and authorize interactions among core services. All these protocols that incorporate current symmetric and asymmetric public/private key pair cryptography will need to be updated or replaced to be quantum resistant in the future as identified in [3] and [10]. For instance, the secure link options in the mobile telecommunications infrastructure will need to include quantum-safe methods such as the quantum-resistant algorithms and QKD. This would give mobile operators the flexibility to select the right encryption level based on the traffic type. This approach could help mobile operators optimize the utilization of premium security features such as high-speed, encrypted links and QKD.

Subscriber and Access Network Security

The 5G user and the user equipment (UE) (e.g., the mobile device) is authenticated to the serving network using either the legacy Authenticated Key Agreement (AKA) protocol or the Internet EAP Authentication and Key Agreement (EAP-AKA) protocol. AKA involves an exchange between the UE and the serving network where the two parties are mutually authenticated and a secret session key is established between them. These keys are 128 bits in length, but 3GPP will allow these to be doubled to 256. Though doubling the key size will make it safe, the running time of the algorithm is increased by multiple factors in a classical computer, so there may be implications for constrained IoT devices.

Interconnect/Carrier-to-Carrier Security

When interacting across network domains, and one carrier's core network is communicating with another carrier's, each network domain must mutually authenticate itself. This enables each carrier to trust the other network to maintain the security posture for what will be transported across them. These rely on PKI infrastructures to authenticate and negotiate to ensure the integrity of the communication security across these interconnected domains, which will need to be updated to be quantum resistant.

Work on cryptography in cellular networks technologies, such as 5G, is driven both in 3GPP and IETF. 3GPP 5G R15 standards define security mechanisms such as 256-bit key transmission [11]. Future 5G standards will support 256-bit cryptographic algorithms to ensure that such algorithms used on 5G networks are sufficiently resistant to attacks by quantum computers. The 3GPP has recommended that the ETSI Security Algorithms Group of Experts (SAGE) evaluate 256-bit cryptographic algorithms.

Trusted Telephone Number Service over VoIP (STIR/SHAKEN)

The STIR/SHAKEN framework is an industry-standard caller ID authentication technology that enables subscribers to trust that callers are who they say they are, reducing the effectiveness of fraudulently spoofed calls. The STIR/SHAKEN protocols allow for the authentication and verification of caller ID information for calls carried over IP networks. These authentication protocols rely on asymmetric public private keys (PKI) to sign and verify VoIP calls between carriers, which will need to be updated to be quantum resistant.

SUMMARY

Building cyber-resilience and cryptographic agility into digital communications infrastructure will offer an opportunity to adopt structural improvements in the use of post-quantum cryptography. In addition, new quantum-safe technologies within communication and information systems that could improve the nation's ability to respond to both current and future cyber threats.

6
CRYPTO AGILITY AND RISK ASSESSMENT

Crypto Agility refers to the ability to replace cryptographic primitives, algorithms, or protocols with limited impact on operations and with low overhead. It is of particular importance in the current environment because discovery of vulnerabilities and retirement of algorithms are inevitable. Algorithms were expected to last for decades, but this may no longer be true as the attack surface and speed of innovation increases. Once a particular signature algorithm is used to issue a long-lived certificate, it will be used by many relying parties. None of them can stop supporting it without invalidating all of the subordinate certificates. Switching to agile cryptography will address the difficulties and demands in a much easier, secure and efficient manner. It also will provide a comprehensive platform for cryptographic development for many years to come.

We do not really know when a CRQC will emerge or if a PQC algorithm might become vulnerable in the future. Hence the absolute need for Crypto Agility. Although there are many libraries and solutions available to help with the quantum transition, many systems are not designed to support rapid adaptations of new crypto primitives and algorithms. Crypto algorithms cannot be replaced until all components of a system are prepared to process the replacement. This may require the replacement of cryptographic algorithms and also updates to the protocols, hardware, dependent operating systems, and procedures. In addition to replacing algorithms, other non-security issues — such as adoption rates, backward compatibility, and performance — must also be considered. It is also an iterative process because none of the post-quantum cryptography has been tested with a real quantum computer, so there will likely be many updates before they are truly secure. Incorporating crypto agility into the assets will help facilitate the iterative process.

One of the ways to combine all the factors into a broader crypto agility strategy is to use a Crypto Agility Risk Assessment Framework (CARAF), proposed in [12]. It allows for a smoother transition within a period of time commensurate with an organization's risk tolerance.

- **Phase 1 – Identifying driver.** The goal of crypto agility is to enable an easy tran-sition into new crypto in the future due to compliance, new technology, or new vulnerabilities. In this case, the most immediate driver for crypto agility is the need to prepare ourselves to be quantum resistant and a transition to PQC. As early as 2015, NSA recommended that organizations prepare for the upcoming quantum-resistant algorithm transition. Furthermore, NIST is currently reviewing post-quantum cryptography and quantum-safe standards, which are expected to be out by 2024. Thus, the U.S. government may have an expectation that organizations transition to quantum-safe alternatives in the not-too-distant future, re-gardless of whether quantum computers become practical by 2024.
- **Phase 2 – Inventory of assets.** The PQC evaluated by NIST are meant to replace public key algorithms. Symmetric key and hashing algorithms will simply need larger key sizes and larger outputs to maintain their current security posture. Whereas for public key cryptography, the system will have to migrate from exist-ing algorithms to quantum-safe alternatives. This also means that not all assets will be similarly impacted. In some cases, assets will be phased out before migration is required and are not within scope of consideration. By considering threats first and then inventory, we can eliminate

extra work by focusing only on affected as-sets. This would provide a more optimized and realistic assessment framework, especially for organizations with a wide variety of assets that will be racing against time.

- **Phase 3 – Risk estimation.** We do not really know if it will take a quantum com-puter a day, a week, minutes, or seconds to break encryption. Even if it starts out as a week, the doubly exponential growth rate of quantum compute power will likely reduce that to seconds in a short period of time. So, the typical risk-estimation formula is a combination of probability and impact. In the case of tran-sition for quantum, however, there is a lack of information about the exploits, so the formula for risk will be based on the timeline and cost. The timeline for miti-gation and shelf life can vary widely, depending on the implementation of the as-sets and the type of assets. The cost can also vary widely, depending on the num-ber of assets and the organization.
    - **Timeline:** The estimation for timeline references Mosca's XYZ model [5], where X refers to the asset's shelf life, Y refers to the time needed for mit-igation, and Z refers to the time needed for the threat to realize. If X + Y > Z, then the assets will be at risk for a number of years. NIST theorizes that a practical quantum computer could be built by 2030 for a budget of about a billion dollars [3]. However, the 2030 timeline may not be com-patible with the published roadmaps of quantum computer makers. The first wave of threat actors will probably be nation-states targeting big companies or governments for sensitive information. Once the technology has matured over time, the threat actors will be expanded to include aver-age attackers increasing the risk.
    - **Cost:** The exact value of the migration will differ based on the organization and asset. However, a few trends will likely apply across the board. The cost to migrate will decrease over time as new tools are developed that make integration of quantum-safe algorithms easier. Even existing tools will improve as more entities try to use them in practice. For example, the IoT systems that use TLS implementations that already provide the option to either use a post-quantum or a hybrid solution will be less expensive to migrate compared to those that do not. Based on that, we provide a qualitative cost estimate for quantum-safe TLS migration for IoT assets in this table. Overhead network costs such as latency and bandwidth should also be considered. While increasing key sizes or adopting new algorithms seems easy, both of these could impact network capacity.
- **Phase 4 – Mitigate the risk.** The expected value of risk, determined by timeline and cost, along with the organizational risk tolerance, determines the appropriate risk-mitigation strategy. In terms of mitigation strategies, the organization can choose to accept the risk, phase out the asset, or secure the asset. If the organiza-tion chooses to secure the assets, there are currently multiple options. One can use existing solutions utilizing crypto agility to prepare for future transition or use compensating controls. One can also look at quantum-resistant cryptography, more specifically hybrid cryptography. Hybrid cryptosystems will remain secure as long as at least one underlying crypto scheme remains secure. However, they are slower, have a larger footprint for key storage, and are less efficient. Furthermore, there are no standards in place for hybrid or quantum-safe cryptography, so there is also the risk of implementation flaws.
- **Phase 5 – Organizational roadmap.** The enterprise must determine a tactical roadmap based on the security mitigation strategy. If we choose to accept the risk, the roadmap would be to continue enforcing existing management plans but include an exception process for the assets in question. If the choice is to phase out the asset, then we need to review alternative solutions and include require-ments around post-quantum security in the guidelines. If the choice is to secure the asset, it is important to benchmark test which PQC is appropriate for the asset. The PQC is based on different mathematical

foundations: some work better for encryptions and others work better for signatures. Some have larger key sizes and others work best for small messages. This introduces new constraints such as limited storage, operational overhead, and implementation requirements. Thus, it is important to test on the assets before upgrading.

By taking a risk-assessment approach, we are able to provide clear, actionable guidance for a risk-mitigation strategy, specifically identifying areas that need to be prioritized for protection and where it may be reasonable to accept the risk. Furthermore, converting this strategy into a tactical roadmap provides a better understanding of the solution space and the inherent challenges.

7
PLANNING FOR THE EVENTUALITY

In addition to NIST's work, there are innovations in new quantum-resistant technologies and work at standards development organizations including ATIS. It is recommended that business leaders take several actions to ready their organizations for the security implications of quantum computing.

Why is it so Important Today?

The future threat from quantum computers to current cryptography is real and is estimated to occur within the next 20 years. Although the chances may be slim, it should also be noted that there is a non-zero probability that a CRQC could emerge within next 5 years (Refer to Figure 1). Quantum-resistant cryptography standards are being developed and envisioned to be finalized within the next two years. Only then can infrastructure standards be adapted to incorporate the new PQC algorithms. Change will take time because new security stacks will need to be developed and deployed, and some devices such as IoT devices will not be able to accommodate these new PQC protocols due to constraints.

How Can Businesses Start to Prepare?

1. **Create awareness of the quantum threat and risk to security.**

This paper set out to create awareness and understanding of the risk quantum computing poses to existing cryptographic and encryption systems. Extend this awareness to other business leaders at the board and C-suite level to gain support for investing in a quantum-safe cryptography infrastructure. CIOs and CSOs should increase their engagement with standards development organizations (SDOs) to raise awareness of necessary quantum-resistant protocols and technologies that can be employed to mitigate the risks. Awareness continues to be a significant challenge. Although many are aware that quantum computers pose a cybersecurity threat, most are unaware of how extensively PKI is used in today's online society. Likewise, there seems to be a lack of urgency, but attacks like Store Now Decrypt Later (SNDL) are likely occurring today and should be taken seriously. This can be accomplished via internal posts, lunch-and-learn sessions, and leadership communications, to name a few. It is imperative for companies to appoint resources and start tackling these issues.

The early engagement by an organization in preparing to be "quantum safe" will reflect the prioritization of this issue and position it to be an active topic in security policy and technical discussions, leading to required changes across the organization and system.

2. **Develop a new approach to managing security.**

Next-generation cybersecurity will require new and innovative solutions to be quantum resistant in the future. This starts with awareness as mentioned above, followed by the creation and adoption of entirely new standards from NIST, ATIS, and others. As the industry saw with the retirement of TLS 1.0, it can take a long time to overhaul cryptography and the systems that use it. There are potentially SNDL attacks occurring right now, so it behooves industry to adopt an agile approach to assess the threat and priorities to securing the organization's communication and information.

3. **Assess the enterprise's readiness to become crypto-agile (resistant to future classical or quantum threat).**

Unfortunately, the complexity of the technology makes it difficult to determine an exact timeline for a CRQC to emerge. There are so many different types of quantum technology, and it is not yet unclear

which quantum computing technology will dominate. We are in the middle of a Betamax vs. VHS vs. Laserdisc battle that has yet to play out. Due to the threats posed by a CRQC, and all the surrounding uncertainty, enterprises are shifting towards a crypto-agile methodology for mitigating this very real threat. CARAF is a framework specifically designed for this purpose, and it provides a great starting point.

4. **Monitor the development of postquantum cryptography standards and solutions.**

There is not a one-size-fits-all solution, but rather a complex set of interdependencies when it comes to post-quantum security. An "age-old debate" is emerging about whether to adopt a QKD-centric approach, one using PQC, or maybe even some hybrid combination of the two. Legacy systems will be a particular challenge because it may be difficult or impossible to update the cryptography in those systems due to the limitations of that much older technology. On the other hand, quantum technologies such as QRNG, with their random numbers and perfect entropy, also provide opportunities to enhance security.

5. **Start by acting today to set the organization on a path to be quantum resistant.**

The path to transitioning an organization's current system to be post-quantum resistant will be lengthy and complicated. If an organization has not implemented a plan to ensure that it can be quantum safe for the future, they need to start now. The first steps are to identify a leader within the organization who will be an early adopter of knowledge. That person can take these practical steps outlined within this white paper to make a start. These key steps help enable organizations to be ready for the quantum era because secure data exchange is of paramount importance in today's economy.

The ATIS Quantum-Safe Communication and Information Initiative brings together industry experts on this topic and is developing a roadmap of work items to advance communications service providers' needs to be quantum-safe in the future. The objective of the ATIS Quantum-Safe Communication and Information Initiative is to:

- Represent the North American communication industry on quantum-safe issues.
- Build awareness of quantum's security risks and educate members in quantum technologies.
- Investigate how the telecommunications industry needs to be quantum-safe.
- Influence standards and the communication industry globally on quantum-safe migration strategies.
- Create an evolution path towards quantum-safe communications networks.

To find out more about the ATIS Quantum-Safe Communication and Information Initiative, visit **www.atis.org**.

CONTRIBUTOR ORGANIZATIONS

- AT&T
- Cisco
- Comcast
- Corning
- InterDigital
- Lockheed Martin
- Qualcomm
- Ribbon
- T-Mobile

REFERENCES

[1] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete loga-rithms and factoring. In Proceedings 35th annual symposium on foundations of com-puter science (pp. 124-134). **https://ieeexplore.ieee.org/document/365700**

[2] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Craig Gidney and Martin Ekerå, **https://quantum-journal.org/papers/q-2021-04-15-433/**

[3] NIST Report on Post-Quantum Cryptography, April 2016, **https://csrc.nist.gov/publications/detail/nistir/8105/final**

[4] NIST Post-Quantum Cryptography Project – Road 3 Status, **https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions**

[5] Quantum Threat Timeline Report 2021, Global Risk Institute, **https://globalriskinstitute.org/download/2021-quantum-threat-timeline-report-short-report/**

[6] Wootters, W.K. and Zurek, W.H., 1982. A single quantum cannot be cloned. Nature, 299(5886), pp.802-803. **https://www.nature.com/articles/299802a0**

[7] Amer, O., Garg, V. and Krawec, W.O., 2021. An Introduction to Practical Quantum Key Distribution. IEEE Aerospace and Electronic Systems Magazine, 36(3), pp.30-55. **https://www.walterkrawec.org/papers/qkd-survey.pdf**

[8] Post-quantum MACsec in Ethernet Networks Joo Yeon Cho* and Andrew Sergeev, 2021, **https://journals.riverpublishers.com/index.php/JCSANDM/article/view/5973/5549**

[9] Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNS-SEC, SIDN Labs October 23, 2020, **https://www.sidnlabs.nl/downloads/7qGFW0DiOkov0vWyDK9qaK/de709198ac34477797b381f146639e27/Retrofitting_Post-Quantum_Cryptography_in_Internet_Protocols.pdf**

[10] T. Charles Clancy Robert W. McGwier Lidong Chen, TUTORIAL: Post-Qantum Cryptography and 5G Security, **https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927805**

[11] 3GPP TR 33.841, Study on the support of 256-bit algorithms for 5G (Release 16) **https://www.3gpp.org/ftp//Specs/archive/33_series/33.841/33841-g10.zip**

[12] Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, Vaibhav Garg, CARAF: Crypto Agility Risk Assessment Framework, **https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827**