Managing Cryptographic and Quantum Risk

A non-technical and hype-free explanation of what's at risk, what you can do, and why you should act now.

isara.com | quantumsafe@isara.com | +1 877 319 8576
560 Westmount Road North, Waterloo, Ontario, Canada N2L 0A9

CONTENTS

EXECUTIVE SUMMARY

Today's organizations rely on cryptography to an extent that few people realize. Even CIOs and CISOs typically don't give much thought to cryptography, and when they do it's usually because their security teams have escalated a serious issue.

Nevertheless, cryptography is essential to every organization's operation and continuity. Regardless of the size of your organization, the cryptographic foundation is ubiquitous and complex; within larger organizations—especially those which have grown through mergers and acquisitions—it's likely that no one in the organization has a firm grasp of all of the cryptographic systems in use.

Like other critical building blocks of information technology, cryptographic systems require management and maintenance. Most of the time, these needs are addressed invisibly, with updates included within the regular cadence of software patches and system upgrades.

Over the past 25 years, cryptographic algorithms have experienced only a few significant vulnerabilities and upgrades; as a result, enterprises have become accustomed to relying on their IT suppliers to manage the cryptography as part of their product life cycle.

Occasionally, though, cryptographic management demands a large-scale migration to a new cryptographic standard.

History teaches us important lessons in this regard: as just one example, the transition from SHA-1 to SHA-2 has made clear that organizations struggle to complete cryptographic migrations in a timely manner, increasing risk. For example, SHA-1 was effectively deprecated in 2011 due to security vulnerabilities—yet many organizations are still working to complete the transition to SHA-2 almost a decade later.

Organizations have struggled with this update because SHA is embedded in a vast number of protocols, systems, and solutions. Simply gaining visibility into the posture of any single algorithm has proven to be a daunting manual task that rarely gets accomplished—so it's no wonder that migrating all the affected systems and software libraries is such a challenge.

Experience also shows us that these transitions are costly, disruptive, and take much longer than we anticipate—realistically requiring a decade or more to complete.

And there is no greater cryptographic migration than the one which is just now beginning: from classical public-key cryptography to quantum-safe cryptography.

With the proliferation of IoT devices and other systems that rely on public-key cryptography to transact digitally in some form, the scale of this approaching migration is larger than anything the industry has previously undertaken.

The necessity for, and scope of, this migration is unlike anything industry has yet encountered. Perhaps the most appropriate analogy is the Y2K bug, but even this comparison is flawed:

- With Y2K, no one could be certain of the precise impact of failing to patch vulnerabilities, whether on isolated devices or on connected systems, although experts were in agreement that the consequences would be unwelcome
- With Y2Q, while the date itself lacks precision we know the impact—the foundations of public-key infrastructure are breakable, and everything which depends upon public-key cryptography (which is more than you think) can no longer be trusted

Google's 2019 achievement of quantum supremacy served as a reminder that Y2Q is closer than many observers like to imagine. In fact, certain organizations—particularly those involved with critical infrastructure, connected vehicles, long-lived IoT devices and communication platforms—should already be investigating, testing, and engaging in proof-of-concept work with quantum-safe candidate algorithms available today.

But even setting aside the quantum threat, and focusing instead purely on classical threats against modern cryptography, organizations and their leaders must sit up and pay attention because the challenge of building, managing, and maintaining cryptographic systems creates gaps that skilled threat actors can exploit. Successful exploitation of these systems can be devastating—severely disrupting an organization's operation or even threatening its very continuity.

A critical first step for managing this risk is to increase cryptographic agility, by improving cryptographic visibility (identifying where and how cryptography is used) and by making architectural and deployment decisions with upgradeability and migrations—including to quantum-safe cryptography—in mind to decrease the costs and risks associated with such changes.

Cryptographic and quantum risks, while undoubtedly complex and even exotic, should be considered as categories of the broader class of cyber risk. Accordingly, an organization's cyber risk strategy or governance program is not complete without crypto-risk and quantum risk management plans in place.

INTRODUCTION

cryptography

> *the practice and study of techniques for secure communication in the presence of third parties*

Cryptography is a vital element in today's information economy: it encodes our secrets, protects our information, enables secure communication, and authenticates our digital identities.

Symmetric cryptography employs a single secret key both to encrypt and decrypt information. Provided a secure algorithm and sufficiently long key length are used, symmetric cryptography is a reliable means of protecting information and is especially useful for encrypting your own data.

Asymmetric cryptography, in contrast, relies on pairs of public and private keys. This ***public-key cryptography*** creates two keys which are related mathematically in such a way that it is impractical to determine one from the other using a classical computer. The public key is shared with the world and anyone with this public key can use it:

- to verify that a message purported to come from the sharer actually does come from the sharer (digital signature)
- to encrypt a message such that only the sharer can decrypt it

Enabling the vast public-key systems in use today is ***public-key infrastructure (PKI)***: the set of solution used by an enterprise to manage the lifecycle of digital certificates, which bind identities and their corresponding public keys.

This document examines two significant risks facing today's organizations—***cryptographic risk*** and ***quantum risk***—and two concepts which relate to both.

It makes no assumptions about technical foreknowledge or domain expertise—the intention is to offer solutions for CEOs, CIOs, CISOs, and other executives so that managing these risks is not disruptive, but merely part of their organization's normal cybersecurity and governance plans.

Part I—Managing Cryptographic Risk explains how the ubiquity and complexity of cryptographic systems introduces risks that pose major—and perhaps surprising—threats to today's organizations. It introduces ***cryptographic agility*** as a means to manage this risk.

Part II—Managing Quantum Risk explains how ***quantum computing***'s ability to break public-key cryptography threatens to cause enormous disruption to many of today's information systems. This part concludes by presenting ***quantum-safe cryptography*** as the most viable solution to this coming calamity.

Either part can stand alone, but the two broad classes of risk are linked: cryptographic agility better prepares an organization to cost-effectively and reliably introduce the quantum-safe cryptography which will be vital to avoiding disruptions and for ensuring continuity in the post-quantum age.

And just how far away is that age? As you will see from *The Quantum Timeline*, a two-page feature slotted between the document's two main parts, it's closer than you might think—and there are compelling reasons to take action immediately.

PART I—MANAGING CRYPTOGRAPHIC RISK

Today's organizations rely on an expansive and growing technology base, including:

- computers, mobile devices, and the Internet of Things;
- operating systems, application software, and communications protocols;
- networks spanning public, private, and hybrid clouds, public networks, and on-premises equipment.

Cryptography allows organizations to protect sensitive information by verifying identities and encrypting information as it moves throughout this rich fabric and as it is exchanged with third parties.

However, cryptography is often taken for granted because it is so deeply embedded into existing systems. Most organizations have become accustomed to cryptography working transparently in the background, only giving these critical systems attention when something significant changes—whether with the cryptographic algorithms themselves or with the systems they are protecting.

Few organizations have an understanding of their cryptographic risk: how well their data is protected by cryptographic means and the gaps and vulnerabilities which exist. Fewer still have the agility to update their cryptosystems safely, securely, and without disruption—whether as part of a large-scale generational migration or simply to manage risks in the shorter term.

Cryptography is ubiquitous and complex

Key takeaways:

- Cryptography is a foundation of today's information-powered organizations
- Cryptography is ubiquitous, but it is typically relegated to the background
- Cryptographic systems are complex, having been developed and extended over decades

Cryptography plays an enormous role in today's organizations and within our wider information-powered economy. But with occasional exceptions—say, an expired certificate warning in a browser—like the foundations of a grand building, cryptography is rarely noticed except by those who specifically seek it out.

Over many years—and for some organizations, even many decades—the cryptographic layer has become tremendously complex. Even organizations who do recognize that there is complexity are almost certainly underestimating the degree. For example, every merger or acquisition, every OEM component, every piece of third-party software—and the list goes on—has potentially introduced cryptographic elements and assets.

In particular, the last decade has seen public-key infrastructure integrated into many business applications through digital certificates which provide the foundations for digital trust. These certificates are the core component for strong authentication between entities and for secure communication through public and private networks.

Certificates, private keys, and the algorithms they employ ensure confidentiality, integrity and availability, often using many different cryptographic libraries spread across many applications.

To briefly explore just one example, people and organizations rely upon digital signatures every day—often without realizing it—to verify the integrity of financial transactions and to ensure both the authenticity (i.e., it came from the real vendor) and integrity (i.e., it has not been modified) of software updates. An attacker with the ability to forge digital signatures can wreak financial havoc and, likely worse, can trick devices into installing malicious software updates to practically any effect.

Few organizations have a complete or accurate knowledge of all the locations where cryptographic keys are being stored and used across applications, browsers, platforms, files, modules and other systems and components. Fewer still can extend that knowledge into their third-party relationships including vendors, contractors, and OEMs.

This complexity comes at a cost: ever-increasing risk.

Cryptographic risks threaten operations and continuity

Key takeaways:

- The consequences of a successful attack against an organization's cryptographic foundation are devastating
- Large-scale cryptographic migrations are complex and can take many years to complete
- Serious cryptographic risks exist today which can have unexpected and immediate impact to an organization's operations and continuity

Because of the foundational role cryptography plays in information security, cryptographic risks are risks to the entire organization. Unfortunately, awareness of these risks often takes a back-seat to more publicized cybersecurity threats like phishing, ransomware, cyberespionage, and hands-on-keyboard attacks. However, organizations ignore cryptographic risk at their own peril, as the consequences of a successful attack—for instance, the Logjam attack against a Diffie-Hellman key exchange[1]—are potentially devastating.

One reason why cryptographic systems are frequently overlooked by organizations is because most companies don't directly implement, manage, or deploy cryptography. Instead, they deploy solutions—and the solutions include embedded cryptography.

There's also truth in the old adage, "out of sight, out of mind"—dealing with crypto-related issues including migrations and expired certificates requires administrator action which is not part of the routine patch cycle.

Within industry, we have not prepared well for cryptographic migrations. For example, dependencies between vendors require coordination and forward/backward compatibility. This general lack of planning, combined with the volume of infrastructure and dependence on interoperability between systems from different vendors, means that it is not uncommon for mistakes to be made and for vulnerabilities to be introduced.

Even setting aside the quantum risk, other cryptographic risks exist including the ongoing danger of relying upon obsolete encryption algorithms, using encryption keys which are too short, and the relatively common challenge of certificate management.

A failure by the teams responsible to manage cryptographic assets—including certificates, keys, algorithms, and libraries—can have unexpected and immediate impact, threatening an organization's operations and continuity. We don't need to look far for examples:

- In February 2020, Microsoft Teams was unavailable for several hours due to the expiry of an SSL certificate[2]
- Also in February 2020, Apple announced that their Safari browser will no longer accept new HTTPS certificates that expire more than 13 months from their creation date; Google's Chrome will no doubt follow suit[3]
- In March 2020, Let's Encrypt revoked 3 million TLS certificates that were issued without a check of the Certificate Authority Authorization (CAA); users had only a few days to renew and replace certificates, with many customers and clients struggling to meet the deadline[4]

Fortunately, certificate management is well-understood and the examples above result from human error, policy decisions, and implementation mistakes. Far more devastating is the potential impact of relying on outdated and compromised cryptographic algorithms.

For example, in January 2020 researchers published a practical collision attack against Secure Hash Algorithm 1 (SHA-1).[5] While the National Institute of Standards and Technology (NIST) formally deprecated use of SHA-1 in 2011 and disallowed its use for digital signatures in 2013, it remains in fairly widespread and significant use. In an article examining the announcement, Ars Technica explains that:[6]

> *The new attack is significant. While SHA1 has been slowly phased out over the past five years, it remains far from being fully deprecated. It's still the default hash function for certifying PGP keys in the legacy 1.4 version branch of GnuPG, the open-source successor to PGP application for encrypting*

email and files. Those SHA1-generated signatures were accepted by the modern GnuPG branch until recently, and were only rejected after the researchers behind the new collision privately reported their results.

Git, the world's most widely used system for managing software development among multiple people, still relies on SHA1 to ensure data integrity. And many non-Web applications that rely on HTTPS encryption still accept SHA1 certificates. SHA1 is also still allowed for in-protocol signatures in the Transport Layer Security and Secure Shell protocols

Most IT managers are familiar with the importance of maintaining up-to-date software inventories as a way to manage broader cyber risk and to contribute to efficient operations. These inventories capture which software versions are in use, which assets have public exposure, and which systems are considered business-critical, and IT and security teams rely on these inventories as an important component of their update and patching process.

Managing ***crypto-risk*** requires applying a similar mindset to cryptographic assets.

Manage crypto-risk by improving crypto-visibility

Key takeaways:

- The first step towards managing cryptographic risk is to improve cryptographic visibility by creating a full inventory of where, how, and what cryptography is used by the organization
- An organization's crypto-visibility should extend into vendors, contractors, OEMs, third parties, partners, etc.

Whether an organization is preparing for a major cryptographic migration or simply aiming to increase understanding of their crypto-risk by better managing cryptographic assets, the success of the initiative depends on the organization's cryptographic visibility.

While crypto-risk represents how well information is protected by cryptographic means, ***crypto-visibility*** represents the degree to which an organization is aware of their cryptographic assets.

Cryptographic infrastructure is widespread and often hidden behind many other technology layers; to lay the foundation for improving crypto-agility and to meaningfully manage crypto-risk, organizations need to create a comprehensive inventory of cryptographic assets including:

- where cryptography is used
- how cryptography is implemented
- what cryptographic systems are employed

As noted previously, most IT managers already understand the value of maintaining hardware and software inventories; moreover, cybersecurity and information security in general are increasingly seen as elements of governance. Therefore, an inventory of cryptographic assets is simply a continuation of these initiatives.

Closely linked to this inventory, organizations must also identify all business-critical systems, applications, and information, and their dependence upon the cryptographic assets. Again, many organizations will have already conducted at least part of this exercise as part of the security governance.

Additionally—and again with obvious parallels in broader cybersecurity—an organization must extend their crypto-visibility into vendors, contractors, OEMs, third parties, and partners.

Manage crypto-risk by improving crypto-agility

Key takeaways:

- Cryptographically agile organizations are able to adopt and integrate new cryptographic systems without making significant changes to infrastructure and without suffering from unnecessary disruptions
- Gartner predicts that by 2021, crypto-agile organizations will suffer 60% fewer cryptographically related security breaches and application failures than organizations without a plan
- An organization's crypto-agility is also impacted by vendors, contractors, OEMs, third parties, partners, etc.

In a 2017 report, *Better Safe Than Sorry: Preparing for Crypto-Agility*, Gartner stated that, "*Sudden and unpredictable algorithmic and cryptographic compromises can leave application security at risk. Security and risk management leaders must prepare for these events by crafting agile response plans.*"[7]

The report predicts that by 2021, organizations with crypto-agility plans in place will suffer 60% fewer cryptographically related security breaches and application failures than organizations without a plan.

Crypto-agility captures the ability of an information security system to adopt and integrate new cryptographic algorithms without making significant changes to the system's infrastructure. Cryptographically agile organizations can upgrade and evolve their cryptographic systems safely, securely, and without disruptions, giving them important advantages and significantly lowering their crypto-risk.

Large-scale cryptographic migrations are enormous undertakings which often take years—or even decades—to complete. For example, SHA-1 was considered insecure as early as 2005 and was formally deprecated by NIST in 2011, yet remains in widespread use despite practical (i.e., affordable) exploits.

Additionally, the gradual shift from Rivest-Shamir-Adelman (RSA) to elliptic-curve cryptography (ECC) has already been underway for more than 10 years and is still ongoing.

Becoming crypto-agile begins with improving crypto-visibility but extends much farther. While crypto-visibility requires organizations to build and maintain an inventory of cryptographic assets, maximizing crypto-agility requires organizations to make architectural and deployment decisions with upgradeability and outright replacement in mind.

Similar to crypto-visibility, crypto-agility also incorporates awareness of business-critical systems, as maximizing the effectiveness and efficiency of updates and migrations depends on proper prioritization.

Finally, an organization's crypto-agility—and, ultimately, its crypto-risk—are both impacted by vendors, contractors, OEMs, third parties, partners, and (in some cases) customers. When an organization understands their own crypto-agility and crypto-risk, it is in a much stronger position to impose expectations and requirements upon these other entities.

Now, consider that:

- The cryptographic footprint is larger than at any point in history
- Information systems and vendor ecosystems are more integrated than ever before
- The switch to quantum-safe cryptography is a wholescale migration, rather than 'merely' an incremental change
- The migration will take years—likely even decades—to complete, so it requires forward/backward compatibility such that systems can operate during the migration period

Add it all up, and it's clear that the migration to quantum-safe cryptography poses new and unique challenges and—at the least—rivals in scope and complexity any previous transition.

THE QUANTUM TIMELINE

Since their 1981 inception in the mind of brilliant physicist Richard Feynman, quantum computers have come a long way thanks to academic focus and the compounding effects of engineering advances.

At first, progress was restricted to thought exercises and chalkboards. Perhaps most notably:

- In 1994, MIT mathematician Peter Shor presented an algorithm to efficiently find the factors of large numbers, in theory significantly outperforming the best-known classical algorithm
- In 1996, Bell Labs mathematician Lov Grover presented an algorithm offering significant ***quantum advantage*** in inverting functions, which also has applications for searching unstructured databases

But by the late 1990s, researchers were building and running the first quantum computers.

> "We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten.
>
> —Bill Gates

Quantum clouds

It's important to note that quantum computing will not be limited to those governments, research institutions, and companies which design and build the quantum computers themselves. Just like enormous classical computing power and resources are now available to anyone and everyone as a service from the cloud, so too will quantum computing be available.

In fact, it's been available on the cloud since 2016, when IBM offered researchers access to a 5-***qubit*** quantum computer. Since then, other companies have followed suit, either by making their own computing resources available directly (Xanadu, QC Ware) or by partnering with the world's largest cloud providers; in late 2019, both Microsoft and Amazon unveiled quantum cloud computing platforms, providing access to quantum computers from vendors including D-Wave, IonQ, and Rigetti.

The takeaway? Anyone with sufficient financial resources—whether friend or foe—will have access to quantum computing.

May 1981 — Caltech physicist Richard Feynman gives a lecture outlining the potential advantages of computing with quantum systems[10]

November 1994 — MIT mathematician Peter Shor presents an algorithm (***Shor's algorithm***) that can efficiently find the prime factors of large numbers and calculate discrete logarithms, in theory significantly outperforming the best classical algorithm[12]

May 1996 — Bell Labs' mathematician Lov Grover presents an algorithm (***Grover's algorithm***) that offers significant performance advantage in identifying inputs to black-box functions when the output is known[13]

July 1985 — British physicist David Deutsch publishes the idea of a "universal quantum computer" that would operate beyond the limits of any classical machine[11]

December 2001 — A collaboration between IBM and Stanford University publishes the first implementation of Shor's algorithm, using a 7-qubit quantum processor to factor 15[14]

Approaching Y2Q

In recent years, advances in quantum computing have accelerated. In March 2018, Google unveiled a 72-qubit quantum processor. Late in the same year, IBM announced it had passed the 50-qubit threshold, while Intel reached 49 qubits.[8]

That said, experts agree it would take a 2,000-qubit, fully fault-tolerant system to be at least theoretically capable of breaking some public-key cryptography algorithms, such as 1,024-bit RSA or 256-bit ECC. That may seem a long way off, but the rate of recent milestones and the continued compounding effects of advancements strongly indicate that Y2Q—the date when a quantum computer can crack public-key cryptography—is on, or only just over, the horizon.

To take just one vendor as an example, IBM has doubled the power of its quantum computers annually since 2017—and if this trend continues, then the 2000-qubit threshold will be reached within the 2020s.[9]

> "This ramping up of industrial activity has happened sooner and more suddenly than most of us expected.
>
> —John Preskill, Quantum Information Theorist at CalTech

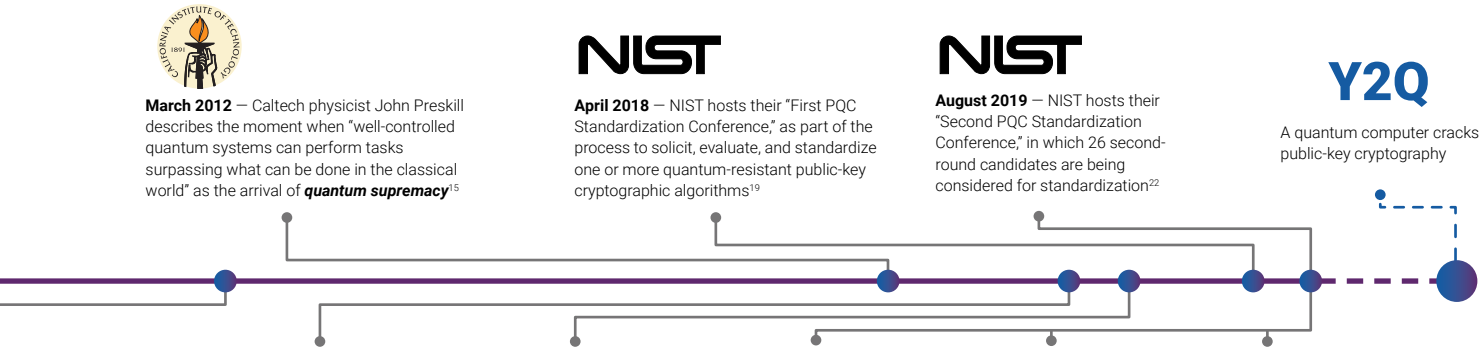
Act today to protect tomorrow

NIST is still in the process of standardizing quantum-safe cryptographic algorithms, but that doesn't mean you have to wait to start managing the quantum risk.

There are already solutions available to bridge the gap between classical and quantum-safe encryption—and there are real reasons to take action today:

- Systems, products and platforms being designed today that will still be in use a decade or more from now need to be quantum-safe
- Motivated threat actors are already harvesting communications protected by today's classical cryptography—to decrypt with quantum computers in the future
- The shift to quantum-safe algorithms will be the largest and most complex cryptographic migration in history—and getting started now offers significant advantages

> "In a five- to ten-year time frame, quantum computing will break encryption as we know it today.
>
> —Sundar Pichai, CEO, Alphabet



March 2012 — Caltech physicist John Preskill describes the moment when "well-controlled quantum systems can perform tasks surpassing what can be done in the classical world" as the arrival of ***quantum supremacy***[15]

April 2018 — NIST hosts their "First PQC Standardization Conference," as part of the process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms[19]

August 2019 — NIST hosts their "Second PQC Standardization Conference," in which 26 second-round candidates are being considered for standardization[22]

Y2Q

A quantum computer cracks public-key cryptography

April 2015 — NIST hosts their first "Workshop on Cybersecurity in a Post-Quantum World," to engage academic, industry, and government stakeholders[16]

August 2015 — The NSA announces that it plans to replace Suite B (specified by NIST) with a new cipher suite due to concerns about quantum computing attacks on ECC[17]

May 2016 — IBM makes a quantum computer with 5 qubits available to researchers via the cloud[18]

January 2019 — IBM unveils their first standalone quantum computer, which is housed in a 3m glass cube[20]

March 2019 — IBM unveils their IBM Q System One quantum computer, with a fourth-generation 20-qubit processor producing a quantum volume of 16[21]

October 2019 — ITU includes ISARA-developed hybrid certificate technology in its certificate standard "Recommendation ITU-T X.509 | ISO/IEC 9594-8"

October 2019 — Google claims the achievement of quantum supremacy (the precise details are disputed, but the claim is ultimately accepted as valid)[23]

December 2019 — Amazon announces their Braket service, providing access to quantum computers from D-Wave, IonQ, and Rigetti[25]

November 2019 — Microsoft announces Azure Quantum cloud service[24]

PART II—MANAGING QUANTUM RISK

Despite the exotic physics at its foundation, quantum computing is merely the next step in a historical progression of harnessing natural phenomena to perform useful tasks:

- In the 19th century, steam engines powered the industrial revolution
- In the 20th century, electrons enabled electronics and computing
- In the 21st century, quantum properties are being applied to information processing

While quantum computers are often described in terms of a revolutionary speedup of familiar computing capabilities, this characterization is both misleading and incomplete. A more accurate representation is that for some problems—but not every problem—a quantum computer is potentially exponentially faster than a classical computer.

In particular, quantum computers are very adept at problems where it's easy to verify the correctness of an answer but also very difficult to determine the answer in the first place. At the present time, there are three types of problem where researchers are confident quantum computers will outperform classical computers:

- Factoring: finding the two numbers that multiply together to make a larger number provided as input
- Inverting: finding an input to a function that produces a particular output
- Simulating quantum systems

Crucially, these three types of problem have sufficiently valuable applications that governments, education institutes, and private organizations worldwide are devoting significant resources towards researching quantum computing and preparing for its consequences—both planned and unintentional.

As we will see, a quantum computer's superior ability to factor and invert undermine the very foundation of public-key cryptography.

Public-key cryptography and the quantum threat

Key takeaways:

- Public-key cryptography is widely employed to encrypt communications and to authenticate identities and content integrity; it is the foundational layer of information security and the consequences of a successful attack are catastrophic
- The security of public-key cryptography depends on the fact that the mathematical problems underlying schemes such as RSA and ECC are difficult to solve on classical computers
- Quantum computers are uniquely capable of breaking current, classical public-key cryptography because of their ability solve the mathematical problems at its heart

Public-key cryptography uses pairs of keys to ensure only authorized entities can read information:

- Public keys, which may be widely shared and are typically certified by a Certification Authority (CA)
- Private keys, which are known only to the owner

Since the mid-1970s, public-key cryptography has been widely employed to encrypt communications and to authenticate endpoints (and sources). For example, a message encrypted by a sender using a recipient's public key can be decrypted only by the recipient's corresponding private key.

Building upon communication and authentication, other common applications of public-key cryptography include digital cash and currencies, password-authenticated key agreement, time-stamping services, non-repudiation protocols, and blockchain.

The security of current, classical public-key cryptography relies upon the mathematical property that while it is easy for a classical computer to multiple two prime numbers together to create a semi-prime product, it is very computationally intensive for a classical computer to start with that product and determine its prime factors.[26]

Even when using extraordinarily powerful classical computers, if sufficiently large keys are used then it is simply impractical to calculate private keys. However, because of their unique capabilities, quantum computers will provide a practical means of overcoming this barrier, essentially breaking the cryptography underlying current ***public-key infrastructure (PKI)***.

To understand the seriousness of this threat, imagine the security systems that protect an organization's information as a pyramid, going from the least- to the most-securely protected (Figure 1):

- At the top are the most common challenges to system security: ***user errors*** like poor passwords, opening phishing emails and malicious documents, and similar risks
- Next come ***administrator errors***, such as failing to patch vulnerabilities as quickly as possible and unnecessarily exposing a larger-than-necessary threat surface
- Then there are ***platform issues***, which include implementation flaws and glitches flowing from poor installation of security systems
- Next up are ***architecture flaws***—the result of poorly designed systems—which generate other vulnerabilities that threat actors can leverage into a major security breach
- At the bottom stands ***cryptography***, the most important means by which companies and agencies normally protect and authenticate data and transactions; more specifically, the cornerstones of this foundation are the digital signatures that allow secure updates of applications and infrastructure and which permit authentication of operations within information systems

As we move down the pyramid, the vulnerabilities become harder to exploit, but the potential impact of a successful exploitation grows enormously. In fact, the last element in the pyramid, cryptography—and more specifically, public-key cryptography—is where the quantum computing threat is greatest.

The unpleasant—but very real—fact is that quantum computing has the potential to catastrophically disrupt an organization's IT norms, to impose huge new workloads on IT staff, and even to threaten the existence of the organization itself.

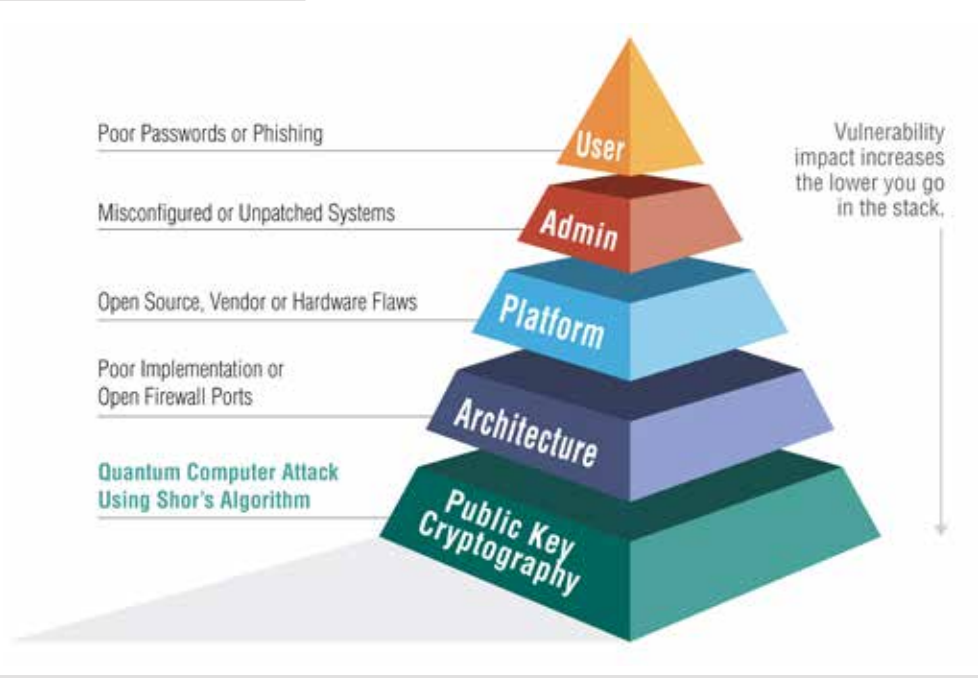


Figure 1—Pyramid representation of security systems protecting an organization's information; as we move down through the layers, vulnerabilities become more difficult to exploit but impact disproportionately grows

The scope of quantum risk

Key takeaways:

- Governments, defense contractors, and certain enterprises have been preparing for the quantum threat for years
- Three areas face particularly high risk: authentic software updates, confidential communications, and digital identities
- Taken together, these three areas are enough to threaten critical infrastructure, connected vehicles, long-lived IoT devices, communication platforms, and other important systems

Governments, defense contractors, and some enterprises take the ***quantum threat*** very seriously and began preparations years ago—but now the rest of the business world is taking notice, thanks to leading analysts, consulting firms and government agencies.

But even with all the attention given to quantum computing, it can be difficult for businesses and other organizations to gain a clear picture of the concrete impact of breaking PKI and undermining roots of trust.

Leaders and executives need to recognize three areas which face particularly high risk:

- Authentic software updates
- Confidential communications
- Digital identities

Many systems, products, and platforms being designed today will still be in use a decade or more from now. Some of these—particularly IoT and connected devices with long in-field service lives—will need to receive software updates throughout their functional lifetime. Today, digital signatures built upon PKI are used to authenticate software updates to ensure only trusted parties can provide them. In the future, quantum computers will allow adversaries to masquerade as trusted parties and effectively trick devices into installing inauthentic, forged updates.

PKI is also at the heart of much of today's confidential communications: a sender uses the recipient's public key to encrypt a message such that only the recipient, using their private key,

Gartner

"If a sufficiently powerful quantum computer becomes available within 10 or so years, any data that has been published or intercepted is subject to cryptanalysis by a future quantum computer."

—Gartner, in The CIO's Guide to Quantum Computing

Deloitte.

"Enterprises and governments should start protecting against the threat of powerful quantum computers today, not when it happens, since by then it will be too late."

—Deloitte, in Technology, Media, and Telecommunications Predictions 2019

NATIONAL ACADEMY OF SCIENCES

"Prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

—National Academy of Sciences, in Quantum Computing Progress and Prospects

can decrypt. However, quantum computers will allow a third party who intercepts the communication to determine the recipient's private key from the corresponding public key, which then allows the third party to decrypt the message.

Finally, PKI is the foundation of today's digital identities, because an identity signed with an entity's private key can be verified by anyone who has access to the sender's public key. To understand how this system functions in practice, consider a familiar analog: how governments use passports to manage identities. A passport serves as an individual's credential, while the passport office is the trusted authority which confirms the individual's identity so others can trust the passport. The infrastructure layer of PKI is analogous to the passport office that other entities trust.

The quantum risk is that anybody equipped with a quantum computer and an entity's public key can calculate the corresponding private key and impersonate the entity. Extending the passport example, both the passport user and the issuer need to protect from quantum threats for trust to be maintained.

Taken together, just these three areas are enough to threaten:

- ***Critical infrastructure***: smart grids, power stations, terrestrial telecommunications networks, satellites
- ***Connected vehicles***: consumer vehicles, public transportation, military assets
- ***IoT devices***: smart meters, industrial control systems, pipeline monitors
- ***Communication and information platforms***: private communications, blockchain-based systems

Plus, it isn't enough for leaders to concern themselves with the direct risks facing, and impact to, their own organization, but also the risks and impact which come from third party suppliers, OEMs, vendors, contractors, etc.

Becoming quantum-safe

Key takeaways:

- There are two accepted approaches to mitigating the threat to classic cryptography from quantum computing: quantum key distribution (QKD) and quantum-safe cryptography
- Of the two, quantum-safe cryptography is the most practical and readily available alternative
- "Hybrid" solutions which integrate quantum-safe cryptographic algorithms into existing infrastructure are available today

There are two accepted approaches to mitigating the threat to classic cryptography posed by powerful quantum computers: quantum key distribution (QKD) and quantum-safe cryptography.

QKD is a means by which two parties agree upon encryption keys and which relies on the properties of quantum mechanics to guarantee security. Quantum physics has the peculiar behavior that simply observing something changes its state. Leveraging QKD, it is possible to create a communication network that shares this quantum property, meaning that two parties will know if a message was observed by a third party because the simple act of observation would change the state of the message in a detectable manner.

While math-based cryptography can be made impractically difficult to compromise, communication built upon QKD (assuming no implementation errors) is provably secure. Because of this promise of being 'unhackable', QKD is an active area of research and is seen by some as the 'Holy Grail' of cryptography.

Unfortunately, QKD requires expensive new infrastructure, including satellites, fiber optics, and quantum repeaters to overcome distance limitations. This hardware dependency and types of network transport also mean that QKD is largely inapplicable to many existing devices (e.g., phones, tablets, IOT devices) and cannot easily be retrofitted into large-scale data centers.

Moreover, QKD does not include the concept of authentication, requiring that another system perform this crucial function.

For these reasons, QKD is a very long way from being a practical solution, with the United Kingdom's National Cyber Security Centre (NCSC) taking the official position that:[27]

> *Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.*
>
> *In addition, we advise that any other organisations considering the use of QKD as a key agreement mechanism ensure that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them.*

Quantum-safe cryptography—also known as ***post-quantum cryptography*** (PQC)—offers a practical and readily-available alternative, because the algorithms at its core can be introduced into existing systems to replace today's RSA and elliptic-curve cryptography. In fact, the NCSC's official advice is that "*the best mitigation against the threat of quantum computers is quantum-safe cryptography.*" [28]

Instead of relying on the difficulty of factoring large numbers or calculating discrete logarithms (employed in ECC), which quantum computers can overcome by employing Shor's algorithm, quantum-resistant algorithms are built upon different fields of mathematics that are believed to be hard for both classical and quantum computers to solve.

To become quantum-safe, an organization needs to catalog its cryptography (i.e., improve crypto-visibility) and be able to manage it and migrate to quantum-safe alternatives as seamlessly as possible (i.e., become crypto-agile).

NIST is helping to develop new global standards for quantum-safe cryptography. In April 2018, NIST held a major standardization conference, and it aims to release new draft standards by 2024.

Importantly, though, organizations do not have to—and in many cases, should not—wait to start managing quantum risk. There are already solutions available to bridge the gap between classical and quantum-safe cryptography.

Plus, starting earlier better equips an organization to confront the very real complexity of the transition and to manage unwelcome surprises which can derail and delay migration efforts—and which can create soaring backend costs.

To prepare for the enormous cryptographic transition, organizations should start by identifying the information and systems that may be at risk in the quantum computing era and by determining where interim solutions are needed to safeguard critical assets.

Plus, while adopting and integrating quantum-safe cryptography is the most practical way to manage quantum risk, all cryptographic upgrades are challenging and time-consuming.

Moreover—to ensure interoperability and sufficient backwards-compatibility—instead of abandoning existing cryptography systems, organizations will need to take advantage of agile cryptography tools and solutions to prepare their infrastructure for eventual implementation of quantum-safe algorithms. Where possible and to mitigate potential harm from harvest-and-decrypt attacks, they should also consider utilizing "hybrid" solutions which maintain the use of NIST-approved algorithms while also future-proofing existing systems.

Regardless of the specific approach and timeline adopted by a particular organization, a prerequisite for a safe, secure, and disruption-free cryptographic migration is for an organization to understand where, how, and what cryptography is being used—which is also the first step to becoming crypto-agile.

CONCLUSIONS AND RECOMMENDATIONS

Today's organizations must confront cryptographic and quantum risks, as both have the potential to create significant disruption.

In the short term, all organizations should take steps to become crypto-agile: doing so is an effective means to manage cryptographic risk and also positions an organization for the migration to quantum-safe cryptography.

To improve crypto-agility, Gartner recommends:[29]

- Building crypto-agility into application development or application procurement workflows
- Creating an inventory of the applications that use cryptography, and identifying and evaluating your dependence on algorithms
- Including cryptographic alternatives and an algorithm swap-out procedure in your existing incident response plans

Beyond those points, organizations should ask their third-party vendors about their cryptographic agility, and should look to replace any products and services that fail to meet crypto-agile expectations.

In addition to improving their crypto-agility, all organizations should endeavor to understand the quantum threat and to stay up-to-date with ongoing developments.

One recommended resource is the NIST Computer Security Resource Center whitepaper, *Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms*, published as a draft in May 2020. [30]

Certain organizations—particularly those involved with critical infrastructure, connected vehicles, long-lived IoT devices and communication platforms—should also investigate and potentially implement quantum-safe algorithms which are available today. These organizations should also ask third-party vendors about their own quantum readiness.

GLOSSARY

asymmetric cryptography
See public-key cryptography.

crypto-agility
The capacity for an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant change to system infrastructure or disruption to dependent systems.

crypto-risk
A quantitative metric or measure, or a qualitative assessment, of the risks to information security (and to systems and processes which depend on information security) faced by an organization due to cryptographic systems and vulnerabilities.

crypto-visibility
The degree to which an organization is aware of where cryptography is used, how cryptography is implemented, and what cryptographic systems are employed.

Grover's algorithm
A quantum algorithm that finds with high probability the unique input to a black box function that produces a particular output value. Due to the quadratic speedup it providers over classical algorithms, Grover's algorithm has the functional impact of halving the key strength of symmetric encryption.

post-quantum cryptography (PQC)
See quantum-safe cryptography.

public-key cryptography
A cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. All public-key schemes are theoretically susceptible to a "brute-force key search attack," but with sufficient key length such attacks are computationally impractical or intractable using classical computers.

Also known as asymmetric cryptography.

public-key infrastructure (PKI)
The set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption, used for authenticating users and devices in the digital world.

quantum advantage
See quantum supremacy.

quantum computing
Using the attributes and principles of quantum mechanics to perform calculations and solve problems.

quantum-resistant cryptography
See quantum-safe cryptography.

quantum-safe cryptography (QSC)
Cryptographic algorithms that are known to be resilient to quantum computer-enabled attacks.

Also known as post-quantum cryptography or quantum-resistant cryptography.

quantum supremacy
The goal of demonstrating that a programmable quantum device can solve a problem that no classical computer can feasibly solve.

In October 2019, Google claimed to achieve quantum supremacy with an array of 54 qubits out of which 53 were functional.

Also known as quantum advantage.

quantum risk
General term referring to the collection of information security, economic, operational, continuity, etc. risk exposure of a particular organization or entity due to the quantum threat.

quantum threat
General term referring to the threat to information security, economic prosperity, organization continuity, etc. resulting from the unique capabilities of quantum computing (in particular, the ability to break public-key cryptography).

qubit
A two-state quantum-mechanical system that serves as the basic unit of quantum information. Unlike classical systems, in which a bit exists in one state or the other, the qubit can exist in a coherent superposition of both states simultaneously.

Shor's algorithm
A quantum algorithm that can find the prime factors of a given input and calculate discrete logarithms, making Shor's algorithm capable of breaking public-key cryptography.

symmetric cryptography
A cryptographic system where only one key (a secret key) is used to both encrypt and decrypt electronic information.

Y2Q
A shorthand for "years to quantum"; while technically framed as a countdown, the term is often employed as the quantum computing parallel of the Y2K bug to represent the date when a quantum computer can crack public-key cryptography.

NOTES AND REFERENCES

[1] The Wikipedia entry provides a useful summary: https://en.wikipedia.org/wiki/Logjam_(computer_security)

[2] Microsoft 365 Status [@Microsoft365Status]. (2020 Feb 3). We've determined that an authentication certificate has expired causing, users to have issues using the service [Tweet]. Twitter. https://twitter.com/MSFT365Status/status/1224351597624537088

[3] Nichols, S. (2020, Feb 3). Apple drops a bomb on long-life HTTPS certificates: Safari to snub new security certs valid for more than 13 months. The Register. https://www.theregister.co.uk/2020/02/20/apple_shorter_cert_lifetime/

[4] Hoffman-Andrews, A. (2020, Feb 29). 2020.02.29 CAA Rechecking Bug. Let's Encrypt. https://community.letsencrypt.org/t/2020-02-29-caa-rechecking-bug/114591

[5] Leurent, Gaëtan & Peyrin, Thomas. (2020, Jan). SHA-1 is a Shambles. https://eprint.iacr.org/2020/014.pdf

[6] Goodin, D. (2020, Jan 7). PGP keys, software security, and much more threatened by new SHA1 exploit. Ars Technica. https://arstechnica.com/information-technology/2020/01/pgp-keys-software-security-and-much-more-threatened-by-new-sha1-exploit/

[7] Horvath, M. & Mahdi, D. (2017, Mar 30). Better Safe Than Sorry: Preparing for Crypto-Agility. Gartner. https://www.gartner.com/en/documents/3645384

[8] Wikipedia contributors maintain a curated list of the world's known quantum computers at: https://en.wikipedia.org/wiki/List_of_quantum_processors

[9] When it comes to running quantum algorithms, logical qubits are what matter, and the numbers in this paper refer to logical qubits. At present, thousands of physical qubits are required to create a single logical qubit. Skeptics often point to this fact as evidence that Y2Q is decades away, but in doing so they overlook three concurrent—and vitally important—trends: (1) our ability to build physical qubits is advancing quickly, so tomorrow's quantum computers will have orders of magnitude more physical qubits than do today's and, accordingly, many more logical qubits; (2) the number of physical qubits required to create a single logical qubit is dropping steadily, again substantially raising the number of logical qubits at our disposal; and (3) error correction algorithms are improving, further optimizing our designs. The combined result of these trends is that the number of logical qubits in state-of-the-art quantum computers will grow rapidly.

[10] Feynman, R. (1981, May) Simulating Physics with Computers. Keynote address delivered at the MIT Physics of Computation Conference.

[11] Deutsch, D. (1985, Jul 8). Quantum theory, the Church–Turing principle and the universal quantum computer. Proceedings of the Royal Society A. https://doi.org/10.1098/rspa.1985.0070

[12] Shor, Peter. (1994, Nov) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Proc. R. Soc. Lond. A40097–117. http://doi.org/10.1098/rspa.1985.0070

[13] Grover, Lov K. (1996, May). A fast quantum mechanical algorithm for database search. https://arxiv.org/pdf/quant-ph/9605043.pdf

[14] IBM (1991, Dec 10). IBM's Test-Tube Quantum Computer Makes History. IBM. https://www-03.ibm.com/press/us/en/pressrelease/965.wss

[15] Preskill, J. (2012, Mar 26). Quantum computing and the entanglement frontier. https://arxiv.org/abs/1203.5813

[16] Per https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-a-Post-Quantum-World

[17] Per https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

[18] IBM (2016, May 4). IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation. IBM. https://www-03.ibm.com/press/us/en/pressrelease/49661.wss

[19] Per https://csrc.nist.gov/Events/2018/First-PQC-Standardization-Conference

[20] IBM (2019, Jan 8). IBM Unveils World's First Integrated Quantum Computing System for Commercial Use. IBM. https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use

[21] IBM (2019, Mar 4). IBM Achieves Highest Quantum Volume to Date, Establishes Roadmap for Reaching Quantum Advantage. IBM. https://newsroom.ibm.com/2019-03-04-IBM-Achieves-Highest-Quantum-Volume-to-Date-Establishes-Roadmap-for-Reaching-Quantum-Advantage

[22] Per https://csrc.nist.gov/Events/2019/second-pqc-standardization-conference

[23] Martinis, J. (2019, Oct 3). Quantum Supremacy Using a Programmable Superconducting Processor. Google. https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

[24] Microsoft (2019, Nov 4). Experience quantum impact with Azure Quantum. Microsoft. https://cloudblogs.microsoft.com/quantum/2019/11/04/announcing-microsoft-azure-quantum/

[25] Barr, J. (2019, Dec 2). Amazon Braket – Get Started with Quantum Computing. Amazon. https://aws.amazon.com/blogs/aws/amazon-braket-get-started-with-quantum-computing/

[26] There are many straightforward explanations of how this property is used to enable public-key cryptography in practice, including Wikipedia's explanation of the Rivest–Shamir–Adleman (RSA) algorithm, available at: https://simple.wikipedia.org/wiki/RSA_algorithm

[27] NCSC (2020, Mar 24). Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[28] NCSC (2020, Mar 24). Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[29] Horvath, M. & Mahdi, D. (2017, Mar 30). Better Safe Than Sorry: Preparing for Crypto-Agility. Gartner. https://www.gartner.com/en/documents/3645384

[30] Barker, W., Polk, W., & Souppaya, M. (2020, May 26). Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05262020-draft.pdf

ABOUT ISARA

ISARA is the world's leading provider of crypto-agile and quantum-safe security solutions.

We have particular expertise in building practical cryptographic systems for the constraints of real-world operational environments.

Our high-performance, standards-based quantum-safe cryptography and integration tools are ready to help you test and deploy robust solutions for the quantum world.

isara.com | quantumsafe@isara.com | +1 877 319 8576
560 Westmount Road North, Waterloo, Ontario, Canada N2L 0A9

Version 1.0 | 2020-06-20