Wells Fargo Technology
Position Paper

Post-Quantum Cryptography (PQC) and the Quantum Threat

November 2020

Executive Highlights

- Quantum computing technology has seen dramatic advances in the last few years creating a very real Second Quantum Revolution. This revolution is creating opportunities unimagined in areas of prediction modeling, optimization, material development and devices controls. Unfortunately, these computing advances threaten current cryptographic methods and systems.

- Quantum computer developments will advance such that they will have the capability of breaking the encryption algorithms used in current systems and infrastructure. It could take years to implement new quantum-safe algorithms into the many potentially affected systems, products and services.

- New algorithms that claim to be quantum-safe have been proposed to the National Institute for Standards and Technology (NIST) and are in active rounds of evaluation.

- Many steps can be taken today to formulate a sound path forward so that data, systems, and applications can remain safe in a new world of quantum computing.

- The timing is right to formalize a quantum computing threat strategy and commitment to resource funding to manage the potential risk related to current-state encryption in the forthcoming quantum world.

- Wells Fargo continues to proactively formulate strategic and robust technical solutions so that the data, systems, and applications our customers rely upon can remain safe in a dynamic new world of quantum computing.

Contents

Abstract

For thousands of years, humans have relied on classical (Newtonian) physics to shape and interface with the world. Algebra, geometry, basic chemistry, classical physics and the early laws of motion and gravity were responsible for everything from the wheel to levers & fulcrums, gunpowder, metalsmithing, and even the combustion engine.

About 100 years ago, the First Quantum Revolution fundamentally changed the way humans perceive the world. The revolution was born out of the original quantum theory where light (and all electromagnetic energy) is made of individual particles (photons) that sometimes behave like particles and sometimes like waves; where space is warped by gravity, and time is relative to the observer.

From this set of revolutionary ideas, sprang virtually every aspect of modern technology and gave rise to inventions like television, microwave ovens, transistors/semiconductors, lasers, space flight & satellites, smart phones, the Internet, and the atomic bomb.

The Second Quantum Revolution peers deeper into the strange world of quantum mechanics and an array of fundamental particles that behave in ways we still don't fully understand but are learning to harness and engineer. Physicists, scientists, architects, engineers and inventors are leveraging quantum phenomena like entanglement and superposition of individual quantum particles to usher in a new chapter of human technology.

As in any revolution, there are profound gains to be made, as well as profound risks to be understood and mitigated. This paper addresses the coming risk to much of the landscape of data encryption and protection deployed today.

Scope of This Paper

The scope of this paper is limited to Post Quantum Cryptography (PQC) and its impact and ramifications to the landscape of data security across all industries. As an inherently technical subject, there are discussions and information on quantum-resistant algorithms, and quantum-secure communications; though the team has made efforts to keep this information as non-technical as possible.

It should be noted that the larger encompassing field of Quantum Technology (including, quantum computing, sensing, navigation, quantum networking, etc.) - while compelling and impactful - is not in scope of this paper.

Introduction to Quantum Technology

To understand post quantum cryptography (PQC) one must first understand a little about the nature of quantum technology and computing. Quantum computing relies on phenomena of quantum physics such as superposition and entanglement to perform operations on data. But what does this really mean?

Rather than storing information using traditional binary bits represented by 0s and 1s as in conventional computing, quantum computers use quantum bits (qubits) to encode information as 0s, 1s, or both at the same time. This superposition of states enables quantum computers to act on enormous combinations of states and outcomes (possible solutions) at once.

When large-scale, fault-tolerant universal quantum computers eventually become available, they will effectively be able to quickly break a number of modern public key cryptosystems. When that happens, datasets, encrypted today, concerning people, businesses and transactions will be at risk.

These quantum computers and algorithms will use quantum algorithms that have the potential to render public-key encryption ineffective. So new cryptographic schemes are needed to withstand these attacks. Post-quantum cryptography (PQC) deals with the analysis and development of these new cryptographic schemes.

Today, a significant portion of quantum technology research and development efforts (including significant work inventing and refining algorithms) is focused on quantum security and the race to create quantum-resistant encryption, while potential bad actors (mainly nation states at this point) are racing to find ways to break current classical security encryption.

What is Post-Quantum Cryptography (PQC)?

Simply put, the term post-quantum cryptography (PQC) refers to cryptography implemented on traditional computing systems that are intended to be secure even after the development of commercial-grade, universal quantum computing devices. The related term PQC Migration refers to the migration of data protection on classical systems to use quantum-resistant algorithms and includes, but is not limited to, the updating of system software stacks and infrastructure.

Certain cryptography algorithms used today, such as asymmetric encryption, key establishment (includes both key transport and key exchange methods), and digital signatures rely on mathematical problems that are intractable to classic computers; such mathematical problems include the integer factorization problem (e.g., used in RSA (Rivest–Shamir–Adleman)) and the discrete logarithm problem (e.g., used in Digital Signature Algorithm (DSA), Elliptic Curve DSA (ECDSA), Diffie-Hellman (DH), and Elliptic Curve DH (ECDH). These terms are defined in the Glossary. These asymmetric algorithms have been proven to be vulnerable to potential quantum computing attacks and will be incapacitated with the help of large-scale fault tolerant quantum computers.

Types of PQC

There are a number of PQC cryptographic techniques being developed and evaluated that are designed to be secure. Some of these include hash-based PQC cryptographic techniques, lattice-based PQC cryptographic techniques, isogeny-based PQC cryptographic techniques, code-based PQC cryptographic techniques and multivariate-based PQC cryptographic techniques. Please refer to Appendix A. Types of PQC for further details about these cryptographic techniques.

Hybrid Cryptosystems

Traditionally, data owners and third-party hosting services use hybrid cryptosystems to safeguard the confidentiality, integrity, and authenticity of enormous volumes of protected data and complex IT systems. These hybrid cryptosystems typically use a combination of asymmetric cryptography (e.g., public key cryptography), such as the RSA cryptosystem, and symmetric cryptography (e.g., secret key cryptography), such as the Advanced Encryption Standard (AES). One example of a modern hybrid cryptosystem is the Transport Layer Security (TLS) protocol, which relies on asymmetric cryptography for authentication and key management to establish session keys, and symmetric cryptography for session encryption and integrity validation.

In the context of PQC, hybrid cryptosystems can take on another meaning. In a PQC world, a hybrid cryptosystem refers to the use of a combination of PQC (quantum resistant algorithms) and traditional cryptography during strategic migrations and transition activities to mitigate risks associated with the breaking of current encryption technology by quantum computers. An effective PQC migration will initially (and for an extended period of time) require both classic cryptographic and PQC cryptographic algorithms to coexist.

PQC Migration

The adoption of quantum resistant encryption can be a complex and lengthy process. There are many different aspects to PQC migrations: for example, from a data perspective, it is migrating the data at-rest and data-in-motion; from a services perspective, the services that get delivered over classic cryptographic have to migrate to infrastructure that can integrate PQC.

It's critical to note that deployment of fundamental changes to infrastructure can take over a decade to complete; for example, the migration from Data Encryption Standard (DES) to Triple Data Encryption Standard (3DES) to Advanced Encryption Standard (AES) has been an ongoing 20-year effort within the financial services industry that is still incomplete. Additionally, security for enterprises will also depend in part on the ability of their suppliers to implement effective PQC strategies.

Recent Advances in Quantum Hardware & Algorithms

The same strange properties that allow quantum computers to do amazing things also present monumental engineering challenges when building even the most basic quantum computer.

Quantum computers must isolate all forms of environmental noise (vibration, temp, EMF) to reach high quality, reliable answers. This includes eliminating even the faintest interference from ambient electromagnetic energy and preventing almost undetectable variations in temperature. Additionally, a quantum computer will use multiple qubits to validate the error of a single qubit, adding significant overhead, expense, and complication to every machine build.

However, an increasing number of companies — including well-funded startups and several major players - have partnered with research institutions to pool wallets and brain power. This is accelerating breakthroughs in quantum computing hardware such as improvements in coherence times and error correction that continue to make news. The following illustration shows the historical increase in quantum hardware capacity in qubits.

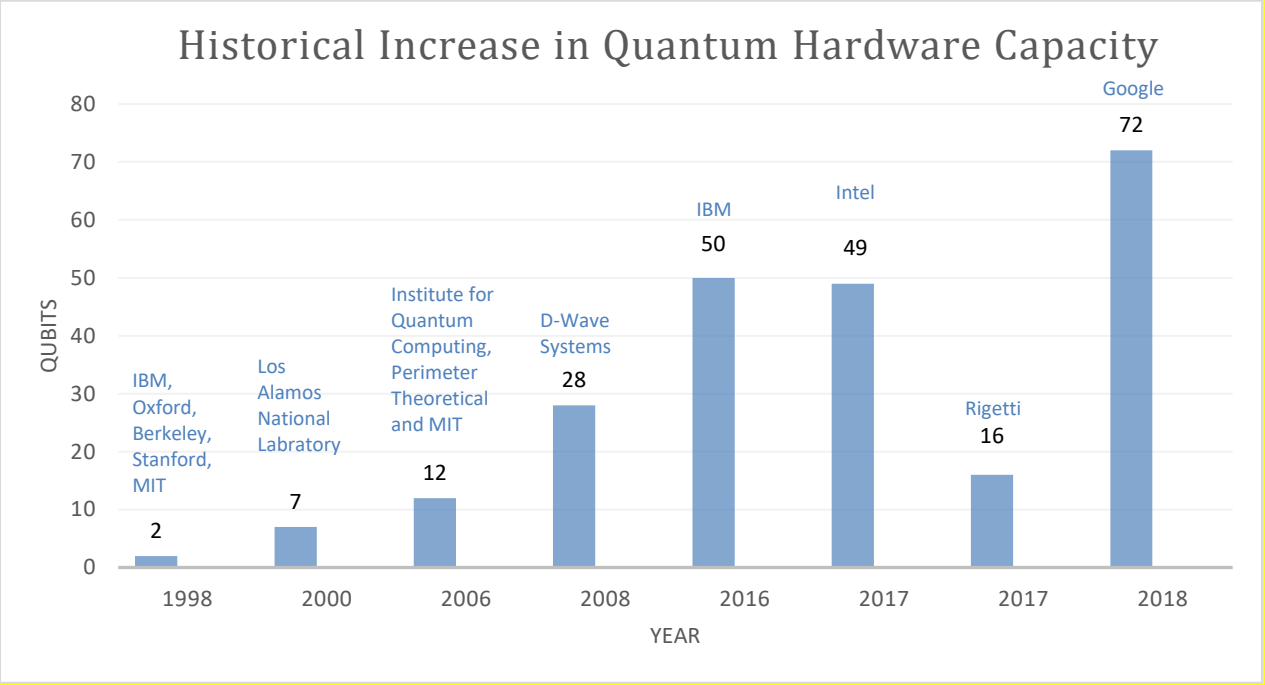

Figure 2: Advances in Quantum Computing Hardware

Probabilistic Bits (P-Bits)

In 2019, engineers from Purdue University and Tohoku University in Japan announced a study where they built and demonstrated how the fundamental units (called p-bits) of what is called a probabilistic computer are capable of performing a calculation that quantum computers would usually be called upon to perform. The study, published in *Nature* on Sept. 18 2019[1], introduces a device that serves as a basis for building probabilistic computers[2] to more efficiently solve problems in areas such as drug research, encryption and cybersecurity, financial services, data analysis and supply chain logistics.

A circuit within the device successfully solved integer factorization, which is often considered a "quantum" problem. Integer factorization is the breaking down (factoring) of numbers such as 35,161 and 945 into smaller numbers. While hundreds of p-bits would actually be needed to solve bigger problems, many researchers do not believe that is too far off. One key point is that while qubits need near-absolute zero temperatures to operate, p-bits work at room temperature.

[1] Borders, W. A., Pervaiz, A. Z., Fukami, S., Camsari, K. Y., Ohno, H., & Datta, S. (2019, September 18). *Integer factorization using stochastic magnetic tunnel junctions*. Retrieved from Nature: https://www.nature.com/articles/s41586-019-1557-9

[2] University, P. (2019, September 18). *'Poor man's qubit' can solve quantum problems without going quantum*. Retrieved from Science News: https://www.sciencedaily.com/releases/2019/09/190918131437.html

Qubit Efficiency

As QC hardware continues to advance, quantum algorithms are also becoming more sophisticated and are being adapted more effectively to the existing noisy and qubit-limited QC systems. New algorithm techniques are being devised that make more efficient and effective use of the number of qubits currently contained in today's QC systems.

Variational Quantum Factoring is an alternate to Shor's algorithm that uses Quantum Approximate Optimization Algorithm (QAOA) techniques to reduce the number of qubits required for Integer factorization[3]. Additionally, an approach by Bernstein and others[4], uses standard heuristics to reduce the qubit requirements for Shor's algorithm for all numbers above a certain size, though the time taken has increased for those situations.

Noisy Circuits

QC systems are similar to classical computers in that they run algorithms by applying sequences of logic gates—in this case, "quantum gates", which together form quantum circuits—to bits of information. The problem with current quantum computing hardware is that noise (interference from control electronics, stray magnetic fields, or even material impurities) builds up within the quantum circuit and degrades accuracy of the resulting calculations.

However, in the summer of 2019, a team of Virginia Tech chemistry and physics researchers advanced quantum computing by devising an algorithm that can more efficiently calculate the properties of molecules on a noisy quantum computer.[5] Future advances in creative, noise-adaptive algorithm development may help accelerate usability of universal quantum computers.

[3] Anschuetz, E. R., Olson, J. P., Aspuru-Guzik, A., & Cao, Y. (2018, August 27). Variational Quantum Factoring. Retrieved from Arxiv: https://arxiv.org/abs/1808.08927

[4] Bernstein, D. J., Biasse, J.-F., & Mosca, M. (2017). *A Low-Resource Quantum Factoring Algorithm*. Retrieved from Semantic Scholar: https://www.semanticscholar.org/paper/A-Low-Resource-Quantum-Factoring-Algorithm-Bernstein-Biasse/17b2dbfbf945c5e96f8d9e31776c4c0b770ee3f5

[5] Tech, V. (2019, July 25). *Researchers lead breakthrough in quantum computing*. Retrieved from Phys Org: https://phys.org/news/2019-07-breakthrough-quantum.html

Defining the Quantum Threat

The main concern of cryptographic vulnerability today is public key cryptography (based on algorithms such as RSA or Elliptic Curve), which is used to securely exchange data encryption keys. These vulnerabilities mean that the public key cryptosystems that are currently being used are not appropriate to secure data requiring long-term security. An adversary could record encrypted data today and wait until one of these vulnerabilities materializes to decrypt the data.

When considering the specific threat to cryptographic systems, the problem can be broken into a simple diagram that illustrates the threat to public key and symmetric encryption systems. The following figure delineates the overall view of the security threat.

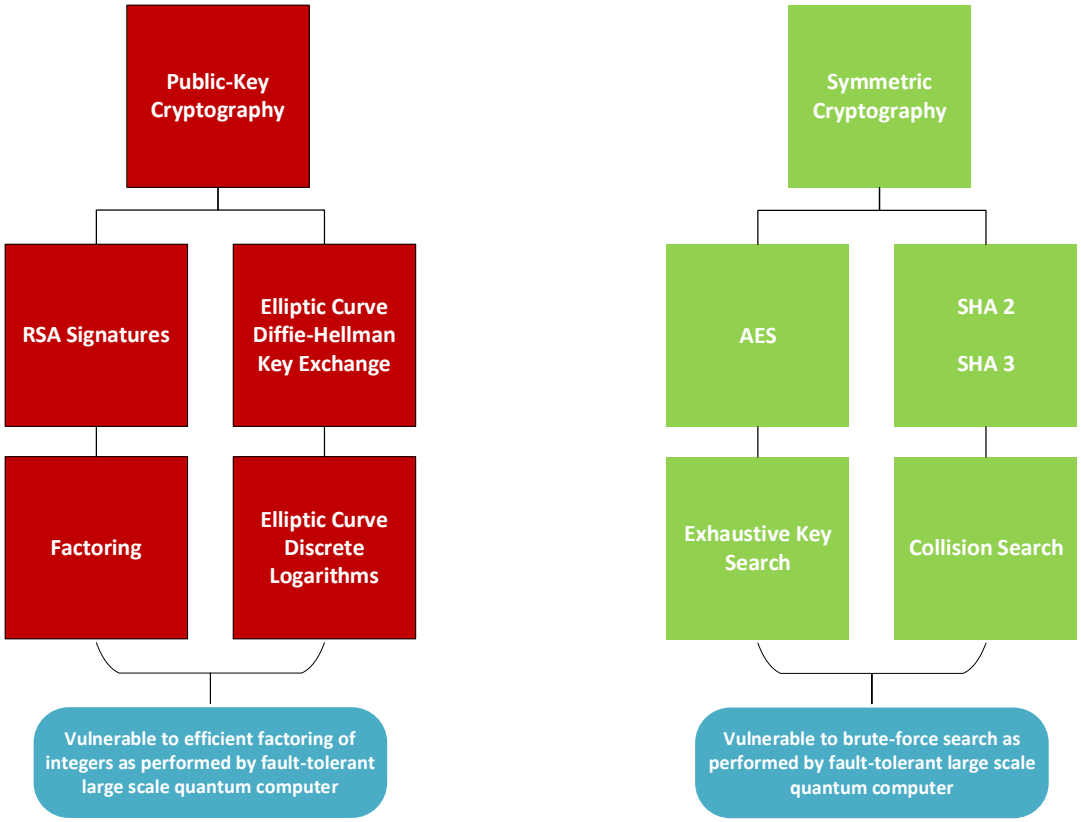

Figure 3. Overview of the Threat to Cryptographic Systems

Cryptographic Algorithms and Key Strength

The cryptosystems that we use today have already been impacted by the anticipated "Quantum Attack", this has led to a drop in their effective strength. The quantum threat to symmetric algorithms stems from the exhaustive key search that can be performed more efficiently on the quantum platform with quadratic speedup using Grover's algorithm[6]. And while most analysts agree that doubling the key length will be sufficient protection, the impact on the performance of the applications and the resource requirements has to be tested and evaluated. Advances in approaches to factoring large numbers, particularly Shor's Algorithm decreases the complexity of breaking asymmetric cryptography. This is due to the efficiency of the quantum Fourier transform over its classical counterpart. So RSA, Elliptic-Curve Cryptography (ECC) and Ephemeral Diffie- Hellman (DHE) are deemed quantum-breakable, because their vulnerability increases as quantum computers become more powerful. The following table shows the changing relative key strength when considering the effect of quantum computing.

Table 1. Relative Key Strength

Type	Algorithm	Classic Key Strength (in bits)	Quantum Key Strength (in bits)	Quantum Attack
Asymmetric	RSA-20482048	112	0	Shor's Algorithm
	RSA-30723072	128		
	ECC-256	128		
	ECC-521	256		
Symmetric	AES-128	128	64	Grover's Algorithm
	AES-256	256	128	

As shown above a quantum brute force search can be defeated by doubling the key length, as shown for Symmetric Key Cryptography. A 256 bit security level on a conventional computer is considered equivalent to 128 bits of security level on a quantum Computer.

The following table illustrates a technical and historical comparison of DES, 3DES and AES encryption algorithms.

[6] Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020, Febuary 21). *Implementing Grover oracles for quantum key search on AES and LowMC*. Retrieved from Cryptology ePrint: https://eprint.iacr.org/2019/1146

Table 2. Comparative Study between DES, 3DES, AES

	DES	3DES	AES
Key length	56 Bits	112 Bits (2-key) 168 Bits (3-key)	128 / 192/256 Bits
Developed	1977	1978	2000
Block Size (in bits)	64	64	128/192/256
Attack	Broken in 1997 (Brute Force)	Broken by better than Brute-force attack	No known attack
NIST Recommendation	NIST recommended till 1999	OpenSSL deprecated it in Aug 2016. Microsoft in Dec 2018. NIST has it designated 80 bits of Security Level.	
Clock Cycle/Byte (during Enc/Dec)	90	216	32

Harvest Now, Decrypt Later

Though the quantum computers that pose the threat are still a few years away, the threat of "Harvest now and Decrypt later attacks" make this an immediate real security risk, which has to be addressed today.

This is a long-game attack[7] where bad actors scrape/collect/harvest encrypted data, by the way of breaches or undertake passive interception and hoard the encrypted data, waiting for the day when quantum computers can decrypt it. So it is imperative to start using quantum resistant algorithms as soon as possible.

A bad actor can record and store (harvest) encrypted data that is streaming through the internet or cloud today. This bad actor could be storing data to or from a specific website, server, email client, or whatever target they deem worthy of attack. With enough resources, a bad actor could capture petabytes of data (or more) from general Internet traffic. Bad actors can be 'Nation-States', internet service providers (ISP) harvesting on a limited basis, or even vendors with backdoors to harvest encrypted data.

The threat lies in the fact that quantum computers will be able to break the asymmetric encryption, disclosing the private keys (when given the public key), thus giving the bad actor unfettered access to the previously 'encrypted' data. With advancement in artificial intelligence and machine learning and with the exponential rise of data processing compute power, it would be relatively easy to extract meaningful information from the stored petabytes of data once the keys are broken. This attack is also known as "Data Vaulting"[8].

[7] Carter, G. (2016, February 18). *Your Best Kept Secrets Aren't Really Secrets*. Retrieved from Security Innovation: https://blog.securityinnovation.com/blog/2016/02/why-your-best-kept-secrets-arent-really-secrets.html

[8] CSA. (2017). *Applied Quantum-Safe Security*. Retrieved from Cloud Security Alliance: https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf

Data Shelf Life

Financial companies today have massive amounts of customer data and trillions of transaction data stored in various databases. In addition, millions of transactions are happening on a daily basis. The security shelf life of a piece of data is very much driven by risk and regulatory requirements.

These risks are amplified by the lengthy data retention requirements (e.g., security shelf-life) mandated by government agencies, such as the U.S. Federal Deposit Insurance Corporation (FDIC). Example data retention requirements for various classes of data records are listed in the FDIC's Records Retention Schedule shown below in Table 3.

Table 3. FDIC's Records Retention Schedule

Tax Info	7 years
Mortgage	30 Years
Auto loan	6 years
Equal Credit Opportunity Act	25 months
Truth in Lending Act	2 years
Bank Secrecy Act	5 years
FDIC Activities	Permanent
Personnel Management (PER4100)	56 years
Non-Judicial Matters (LAW1330) (incl. Loans, Foreclosure, …)	Close of Matter + 10 years
Judicial Matters (LAW1400) (incl. Loans, Foreclosure, …)	Close of Matter / Entry of Criminal Restitution + 20 years

Data at Rest vs. Data in Motion

Different cipher suites are required depending upon whether the data that is being encrypted is going to be Data at Rest or Data in Motion.

Data in motion typically involves asymmetric key exchange protocols or key establishment protocol to initiate the transfer of data from one secure endpoint to the other secure endpoint. Data in Motion uses symmetric keys to protect session data, however the session keys are established using asymmetric cryptography. This leaves them vulnerable to a quantum attack, so key management will, by necessity, need to be quantum resistant (or regress to pre-asymmetric methods).

In a PQC world, data in motion is the most vulnerable to the threat of quantum computing. The cryptographic techniques used are also driven by regulations and National Institute of Standards and Technology (NIST) recommendations. The testing of PQC algorithms is happening today and the final approval is expected to be two or so years away.

Data at Rest is most often managed using symmetric (AES) cryptography and can be made resistant by just increasing key lengths. However, strategies for mitigating Data at Rest may have additional complexities whether it is stored (and in transit) on-premises or off-premises. Data stores kept off-premises may have additional consideration, such as key management, security auditing, as well as Data in Motion protection issues.

Industry Adoption

In any paradigm-shifting market disruption, whomever becomes a rapid adopter is assured to garner a significant advantage. In this newly (and quickly) emerging quantum technology space, some industry players have begun to emerge. Some of the more significant entities, as well as some of the partnerships and activities by other financial institutions are listed below in Table 4.

Table 4. Early Quantum Industry Players

Entity	Description
Cambridge QC	Cambridge QC's (CQC) proprietary quantum encryption device, IronBridge, provides current and post-quantum cybersecurity. http://cambridgequantum.com/cqc-unveils-the-worlds-first-commercially-ready-certifiable-quantum-cryptographic-device/
DigiCert	DigiCerts PQC toolkit contains everything necessary to create a hybrid transport layer security (TLS) certificate. https://docs.digicert.com/certificate-tools/post-quantum-cryptography/pqc-toolkit-setup-guide/
Envieta	Envieta has developed a suite of quantum resistant cryptographic implementations. https://envieta.com/post-quantum-cores
evolutionQ	Tailoring quantum-safe cybersecurity – Dr Mosca's firm - https://evolutionq.com/
Google	Chrome and Google experimented with a post-quantum key-agreement primitives in TLS. https://www.imperialviolet.org/2016/11/28/cecpq1.html
IBM	IBM quantum computing-safe tape drive prototype is based on a state-of-the-art IBM TS1160 tape drive and uses both Kyber and Dilithium in combination with symmetric AES-256 encryption. IBM has submissions to NIST's Standardization process. https://www.zurich.ibm.com/securityprivacy/quantumsafecryptography.html
ID Quantique	Thales partners with ID Quantique and ISARA to combat the future security threats of quantum computing. https://www.idquantique.com/random-number-generation/overview/
Infineon	Infineon implemented the world's first post-quantum cryptography on a contactless security chip. https://www.infineon.com/cms/en/product/promopages/post-quantum-cryptography/
ISARA	ISARA Radiate™ Quantum-Safe Toolkit and Catalyst™ Agile Technologies help enterprises migrate their networks and solutions to quantum-safe security without sacrificing interoperability and crypto-agility. https://www.isara.com/isara-radiate/
Microsoft	Microsoft published an open source project called "PQCrypto-VPN" that implements post-quantum cryptography. https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

Entity	Description
Onboard Security	Quantum Safe Hybrid (QSH) approach using NTRU Cryptography - https://www.onboardsecurity.com/products/ntru-crypto
PQ Solutions	PQ Solutions is developing protection against the quantum threat and offering a range of unique commercial and government solutions. https://www.post-quantum.com/
Thales / Gemalto	DigiCert, Gemalto and ISARA Partner to ensure a secure future for the internet of things (IoT), using post-quantum-ready public key infrastructure (PKI). https://safenet.gemalto.com/digicert-gemalto-isara-partner-to-ensure-secure-future-for-the-internet-of-things-iot/
Utimaco	Utimaco's PQC SDKs (w/ Hybrid Implementation) and hardware security modules (HSM) let you design for "Crypto Agility". https://hsm.utimaco.com/solutions/applications/post-quantum-crypto-agility/

In addition to the companies listed in Table 4, there are open source projects that relate to PQC. Some of the more notable ones are listed below in Table 5.

Table 5. PQC Open Source Projects

Entity	Description
BouncyCastle	Post-quantum crypto library that provides support for LMS and HSS (RFC 8554), XMMS and XMSSMT, McEliece, SPHINCS-256 and Rainbow. https://www.bouncycastle.org/
eBACS SUPERCOP	SUPERCOP is a toolkit developed by the VAMPIRE lab for measuring the performance of cryptographic software. https://bench.cr.yp.to/supercop.html
libOQS	C library for quantum-resistant cryptographic algorithms. Many NIST submissions are available here. https://github.com/open-quantum-safe/liboqs
PQClean	Clean implementations of the post-quantum schemes that are in the NIST post-quantum project. https://github.com/PQClean/PQClean
PQCrypto	Libpqcrypto is a cryptographic software library produced by the PQCRYPTO project. https://pqcrypto.eu.org/
Pqm4	Post-quantum crypto library for the ARM Cortex-M4. https://github.com/mupq/pqm4

PQC Migration Takes Time

The PQC landscape is vast, spanning the entire digital universe and includes virtually every application, data store, and system of record; as well as an entire landscape of data transmission networks, platforms, and entities.

The Data Landscape

- The migration process is challenging due to the sheer volume of data created and consumed by systems, as well as the general complexity of the systems. For example, financial services providers and their partners each may have data for millions of customers and trillions of transactions stored in various databases.
- Data is stored in more places than ever before and must be encrypted using different cryptographic keys depending upon whether the data is going to be protected while in transit, while at rest in-cloud, or while at rest on-premises. Governmental regulations, NIST recommendations, and industry standards and best practices may also drive the cryptographic techniques that are used to encrypt data.
- There is the need to protect data for varying durations to manage legal and regulatory risk, sometimes as long as 20 to 30 years, and even in some cases for over 50 years.

Cryptography Considerations

- Although some quantum resistant cryptographic algorithms are available today, the adoption of these algorithms is a complex and time-consuming process. There are some significant issues and complexities as organizations prepare for post-quantum cryptography.
- Many organizations use several types of encryption, hashing, and other cryptographic algorithms with varying implementation designs, based on the needs of the data owner or hosting service.
- Current testing of proposed quantum-safe algorithms indicates significant increases in time to execute and needed compute resources over the comparable performance and compute requirements of current classical PKI algorithms. This will require additional study and testing to determine implementation designs that will minimize these performance impacts to current applications.

Migrating Infrastructure

- Deployment of fundamental changes to infrastructure might take a decade or more, and there is very little tolerance for incurring risk while deploying changes.
- PQC migration can also include translations of networks. For example, networks A, B, and C can only do classic cryptography today, but tomorrow network C is migrated to be PQC enabled. At that point, Network C can drop in a PQC gateway to translate back and forth to Networks A and B. As the other networks become PQC compliant, a fully secure internetworking system can be established. Figure 1, illustrates this hybrid approach to PQC networks.

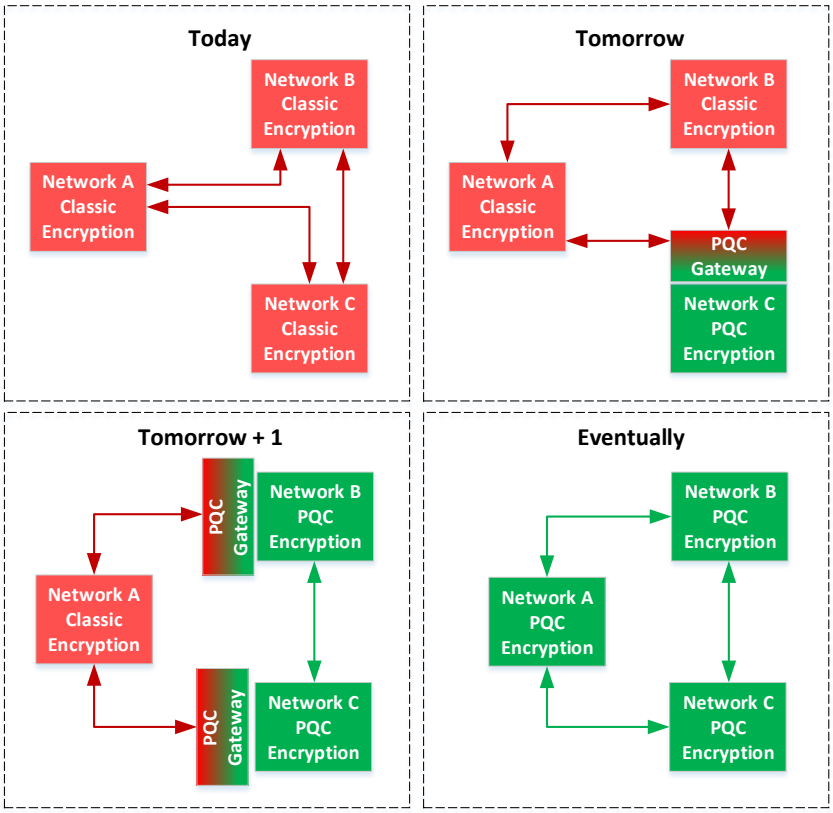

Figure 4. Hybrid Approach to PQC Networks

Other Considerations

The transition is further complicated by interoperability, integration with existing systems and security architectures, scalability, compliance and regulatory requirements, maintenance, and backward compatibility requirements. Vendor systems (and other externally hosted SaaS solutions) present additional control challenges for PKI applications.

All of these considerations introduce additional levels of complexity, and thus data owners and hosting services must methodically and systematically begin to design and migrate their cryptographic infrastructure to quantum-resistant cryptography as soon as possible.

What Can Be Done Now?

There are a number of activities that enterprises can do to support or lead the discovery, inventory, and mitigation of the PQC landscape. These activities will increase preparedness, effectiveness, and the efficiency of PQC migrations through improvements in policy, data management, education, governance, controls, and technology:

- Improve data governance and data management.
    - Investigate and deploy tools and activities to improve data discovery.
    - Aggregate data reporting to provide a more comprehensive view.
    - Implement a data tagging strategy that includes data classification and cryptography used.
- Understand vendor roadmaps to PQC; including “embedded” cryptography systems.
- Build and improve tools to evaluate and test algorithms, libraries and better ways to evaluate vendor toolkits.
- Create an application testbed that allows integration of select PQC approaches into a real world applications in a safe, controlled non-production environment. This should include secure file transfer, secure messaging, and certificate and key management applications.
- Explore hybrid certificates that allow transition to a PQC environment.
- Plan for PQC migration at the Infrastructure level that includes development of an infrastructure test bed that integrates PQC with a real word applications on a limited / restricted scale to assess impacts to current infrastructure and systems.
- Increase the ability to centrally manage and monitor cryptographic related settings associated with IoT devices (including things like alarm panels, DVRs, cameras, turnstiles, and printers).
- Increase participation in standardization activity such as X9/TC68, INCITS and JTC1.
- Design for crypto-agility as a key element to be studied and architected so that as algorithms and key structures change, the incorporation of those changes can be integrated with minimal impact.
- Identify migration approaches that support the transition to new PQC algorithms, without loss of interoperability and functionality during the transition period.
- Stay abreast of continued advances in current PQC algorithms, such as lattice-based approaches, code-based cryptography, multivariate cryptography and hash-based cryptography.
- Participate in industry standards with peer organization not only for PQC algorithms but updates to security protocols (e.g. TLS) and developments in cryptography and key management governance models.

Appendix A. Types of PQC

There are a number of PQC cryptographic techniques, including hash-based PQC, lattice-based PQC, isogeny-based PQC, code-based PQC, multivariate-based PQC, zero-knowledge proof PQC. Each of these cryptographic techniques is described in more detail below.

Hash-Based PQC: PQC techniques that are suitable for one-time use, wherein a tuning parameter provides a trade-off between signature size and key generation, signing, and verification speed, and can be can be used with any secure hashing function. Hash-based PQC cryptographic techniques is used to provide digital signatures, such as Leighton-Micali Signature (LMS), eXtended Merkle Signature Scheme (XMSS), and SPHINCS+.

Lattice-based PQC: Lattice-based PQC techniques that are based on the shortest vector problem, the leading replacement for prime factorization and discrete logarithm. Lattice-based PQC cryptographic techniques is used to provide digital signatures, such as Dilithium and qTESLA. Lattice-based PQC cryptographic techniques are also used to provide key exchange by key encapsulation, such as NewHope, Frodo Key-Encapsulation Mechanisms (FrodoKEM), Nth degree-Truncated polynomial Ring Units (NTRU) Prime, and Kyber.Lattice-based PQC cryptographic techniques are used to provide key exchange by key agreement, such as NewHope Classic, Frodo Diffie-Hellman (FrodoDH), and Ring Learning With Errors Key EXchange (RLWE-KEX).

Isogeny-Based PQC: Isogeny-based PQC techniques use very small keys and typically are more computationally resource intensive in relation to lattice-based and other PQC cryptographic techniques. Isogeny-based PQC cryptographic techniques may be used to provide key exchange by key encapsulation, such as Supersingular Isogeny Key Encapsulation (SIKE). Isogeny-based PQC cryptographic techniques may be used to provide key exchange by key agreement, such as Supersingular isogeny Diffie–Hellman (SIDH) key exchange.

Code-Based PQC: Code-based PQC techniques use very large key sizes yet are typically the fastest PQC cryptographic techniques at the comparable security level (e.g., extremely fast in encryption and reasonably fast in decryption). Code-based PQC cryptographic techniques are used to provide key exchange by key encapsulation, such as Classic McEliece, McEliece Quasi-Cyclic Moderate Density Parity Check (QC-MDPC), and Bit Flipping Key Encapsulation (BIKE).

Multivariate-Based PQC: Multivariate-based PQC techniques use small public keys and fast verification yet, encryption is less efficient than those of other PQC cryptographic techniques. Multivariate-based PQC cryptographic techniques may be used to provide digital signatures, such as Rainbow.

Zero-Knowledge Proof PQC: Zero-knowledge proof PQC techniques use very small key pairs and derive their security entirely from the security of symmetric-key primitives and are believed to be quantum- secure. In some instances, zero-knowledge proof PQC cryptographic techniques may be used to provide digital signatures, such as Picnic.

X9.95 Lattice-Based Polynomial Public Key Establishment Algorithm: A PQC technique that was published by ASC X9 in 2010 X9.95 is one of the NIST finalists remaining in the third round. This is a non-traditional approach based on alternate technologies (e.g. X9.84 Biometric Management and Security).

NIST driven PQC Standardization: In July 2020, NIST announced seven finalists and eight alternate algorithms, with lattice based PQC algorithms having among the most promising results. The standardization has now entered the final round. The details can be found here[9].

[9] *PQC Standardization Process: Third Round Candidate Announcement*. (2020, July 22). Retrieved from NIST: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

Glossary: Definitions and Descriptions

This section provides definitions, descriptions and examples to many of the key terms used in this paper relative to quantum computing.

- **AES:** FIPS 197 Advanced Encryption Standard: an algorithm that uses a symmetric block cipher that can encrypt and decrypt information.
- **Block Cipher:** the cryptographic algorithm used to encrypt data blocks.
- **Certificate:** an electronic document provided by certification authorities (CA) that cryptographically binds information that identifies the owner with a public key.
- **Ciphertext:** encrypted data that is not readable to the user.
- **DH**: Diffie-Hellman[10]: a static key exchange scheme published by Diffie and Hellman to securely exchange cryptographic keys over an insecure / public channel.
- **ECC**: Elliptic-Curve Cryptography: the key structure is based on the algebraic structure of elliptic curves over a field of finite elements. ECC provides for smaller keys or increased security for similar key lengths.
- **DHE**: Ephemeral Diffie- Hellman: Also referred to as EDH based on the cypher suite. DHE is a modification of DH that uses ephemeral keys, typically once in a TLS session. DH keys are deemed quantum-breakable, because their vulnerability increases as quantum computers become more powerful.
- **Digital Signature:** the value that provides data integrity and authentication in an electronic document.
- **DSA:** FIPS 186 Digital Signature Algorithm. Is based on modular exponentiation and discrete logarithms to generate a digital signature that can be verified with a public key. It is not used to encrypt data.
- **ECDH**: Elliptic Curve Diffie Hellman (DH): a DH key exchange that uses elliptic curve public-private key pairs.
- **ECDSA**: Elliptic Curve DSA: a variant of DSA that uses elliptic curve public-private key pairs.
- **Electromagnetic Energy**: a form of energy reflected or emitted in the form of electrical and magnetic waves; e.g., x rays, visible light, microwaves and radio waves.
- **Entanglement:** a term used in quantum theory to describe the way particles of energy/matter can become correlated and predictably interact with each other regardless of how far apart they are; i.e., the spin state of a particle being measured (decided at the time of measurement) is "identical" to the correlated particle.
- **Intractable Problems**: mathematical problems which cannot be solved for a specific computing resource, so what is an intractable problem to classical computing may not be intractable to quantum computing.
- **Quantum Mechanics** (Quantum Theory): the branch of physics that describes atoms and subatomic particles at very small scales and energy levels. It includes the mathematical description of the motion and interaction of subatomic particles, and incorporates the concepts of quantization of energy, wave-particle duality, and the uncertainty principle.

[10] Diffie, W.; Hellman, M.E. (November 1976). "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6): 644–654.

- **Quantum Resistant Cryptography**: algorithms that are believed to be invulnerable to Shor's Algorithm and other quantum algorithms.
- **Qubit**: the fundamental unit of information in a quantum computer.
- **RSA:** Rivest-Shamir-Adleman[11]: a public-key cryptosystems used for secure data transmission. Key asymmetry is based on the practical difficulty of factoring the product of two large prime numbers.
- **Secret Key**: a shared cryptographic key known only to the parties involved
- **Shor's Algorithm**[12]: named after mathematician Peter Shor, is an algorithm for integer factorization and discrete logarithms. Formulated in 1994, it solves the problem: given an integer N, find its prime factors.
- **Superposition**: in quantum mechanics, the phenomenon of superposition means a measured particle has no single spin direction before being measured, but is simultaneously in both a spin-up and spin-down state. The spin state of the particle being measured is actually decided at the time of measurement.
- **TLS:** Transport Layer Security: TLS supports different methods for exchanging keys, encrypting data, and authenticating message integrity.

[11] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). Communications of the ACM. 21 (2): 120–126.

[12] *Shor, P.W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134.*

Contributors

Peter Bordow – Principal Architect, Enterprise Architecture, WF Technology (Lead)

Jason Buck – Information Security Area Manager, Information Protection Technologies, Information Security

Robert Carter - Senior Architect, Cryptography, Enterprise Information Security Architecture

John (Dave) Cooper – Information Security Manager, Information Protection Technologies, Information Security

Andrew Garner – Strategy Consultant, Innovation R&D, Innovation Group

Phillip Griffin - Senior Architect, Cryptography, Enterprise Information Security Architecture

Stephen Jordan – Information Security Senior Leader, Information Protection Technologies, Information Security

Akhlaq Khan – Technology Manager, Innovation Technology, Innovation and Strategic Services Technology

Ram Ramanathan – Strategic Planning Manager, Innovation R&D, Innovation Group

Abhijit Rao – Strategy Consultant, Innovation R&D, Innovation Group

Jeff Stapleton – Senior Architect, Cryptography, Enterprise Information Security Architecture

Ramesh Yarlagadda - Strategy Consultant, Strategic Services & Advanced Technology, WF Technology

References

Anschuetz, E. R., Olson, J. P., Aspuru-Guzik, A., & Cao, Y. (2018, August 27). *Variational Quantum Factoring*. Retrieved from Arxiv: https://arxiv.org/abs/1808.08927

Bernstein, D. J., Biasse, J.-F., & Mosca, M. (2017). *A Low-Resource Quantum Factoring Algorithm*. Retrieved from Semantic Scholar: https://www.semanticscholar.org/paper/A-Low-Resource-Quantum-Factoring-Algorithm-Bernstein-Biasse/17b2dbfbf945c5e96f8d9e31776c4c0b770ee3f5

Borders, W. A., Pervaiz, A. Z., Fukami, S., Camsari, K. Y., Ohno, H., & Datta, S. (2019, September 18). *Integer factorization using stochastic magnetic tunnel junctions*. Retrieved from Nature: https://www.nature.com/articles/s41586-019-1557-9

Carter, G. (2016, February 18). *Your Best Kept Secrets Aren't Really Secrets*. Retrieved from Security Innovation: https://blog.securityinnovation.com/blog/2016/02/why-your-best-kept-secrets-arent-really-secrets.html

Computer Security Resource Center CSRC. (2020, July 30). Retrieved from NIST: https://csrc.nist.gov/projects/post-quantum-cryptography

CSA. (2017). *Applied Quantum-Safe Security*. Retrieved from Cloud Security Alliance: https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf

Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020, Febuary 21). *Implementing Grover oracles for quantum key search on AES and LowMC*. Retrieved from Cryptology ePrint: https://eprint.iacr.org/2019/1146

Post-Quantum Cryptography. (2020, August 11). Retrieved from NIST: https://csrc.nist.gov/projects/post-quantum-cryptography

PQC Standardization Process: Third Round Candidate Announcement. (2020, July 22). Retrieved from NIST: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

Tech, V. (2019, July 25). *Researchers lead breakthrough in quantum computing*. Retrieved from Phys Org: https://phys.org/news/2019-07-breakthrough-quantum.html

University, P. (2019, September 18). *'Poor man's qubit' can solve quantum problems without going quantum*. Retrieved from Science News: https://www.sciencedaily.com/releases/2019/09/190918131437.htm