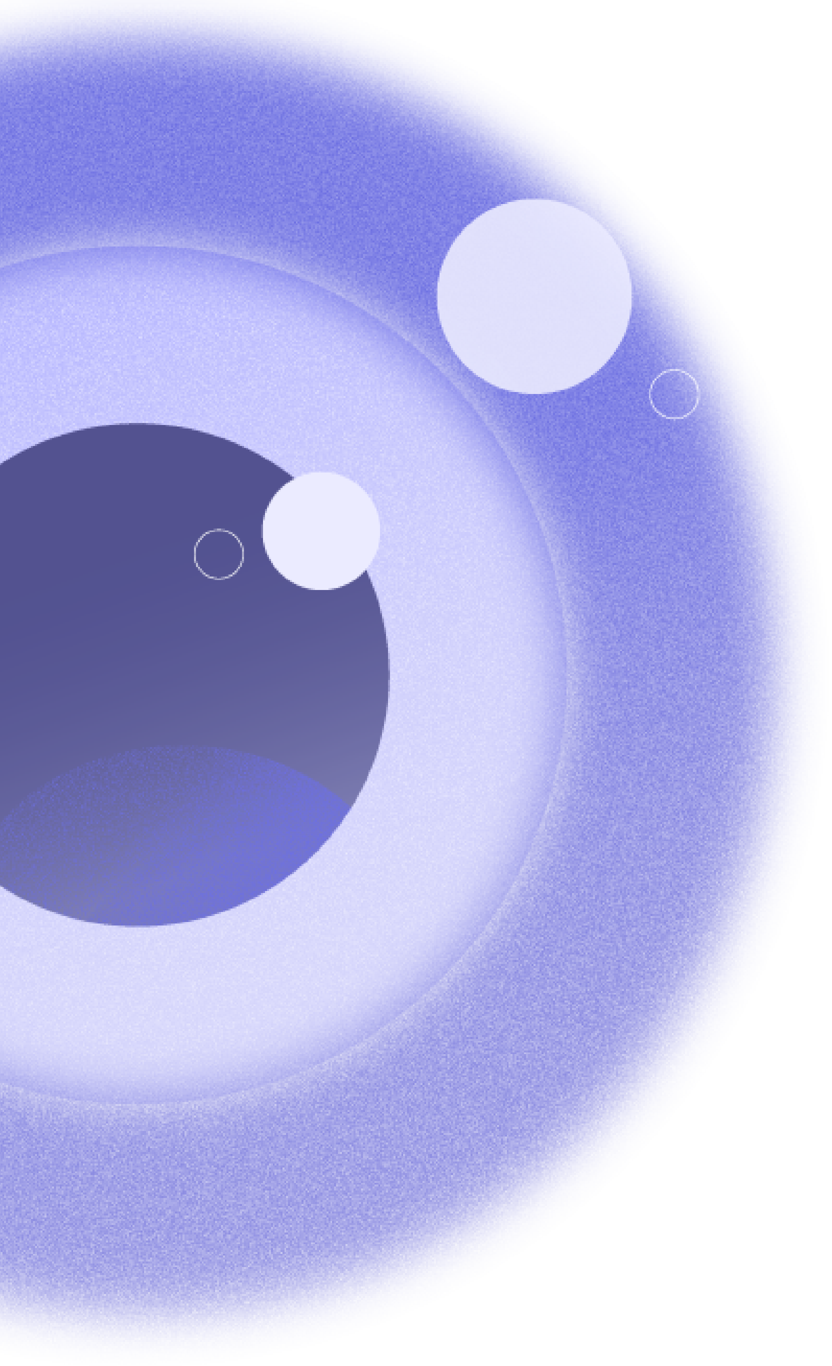
FS-ISAC

Preparing for a Post-Quantum World by Managing Cryptographic Risk



Prepared by

FS-ISAC's Post-Quantum Cryptography Working Group

March 2023

Contents

WHAT IS PQC?

Post-quantum cryptography (PQC), also known as quantum-proof, quantum-safe, or quantum-resistant cryptography, refers to cryptographic algorithms (typically public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer.

WHY PQC MATTERS

The security of most standard algorithms relies on extremely difficult mathematical problems that take years to solve with current computers. Modern public-key encryption protocols are satisfactory for protecting against most technological tools at the disposal of today's threat actors. However, that won't last. Quantum computers will be capable of breaking these math-based systems in a matter of seconds. In addition, threat actors are now harvesting large quantities of encrypted data and storing it until they can break the encryption keys using quantum computing. Data that is encrypted today is vulnerable to decryption tomorrow.

When large-scale quantum computers are built, they will be capable of breaking many of the current public-key cryptography systems. Global funding for quantum computing startups increased by 13.5% last year, to $1.1 billion. According to McKinsey, China plans to invest $15.3 billion in the industry, and the European Union has set aside $7.2 billion for investment.

Without significant preparation for moving to post-quantum cryptography, quantum computers in the wrong hands would significantly compromise the privacy and security of the digital communications on which the world, and the financial system, increasingly relies on.

▶ Current Status of Quantum Computing: What's Taking so Long?

A quantum computer's design presents difficulties. Just as bits are the units of classical computers, qubits are the fundamental building blocks of quantum computers. Being able to control the qubits, which are notoriously flimsy, is key to creating quantum computers. Information loss can occur when qubits are unable to function properly due to seemingly insignificant environmental factors, like interference from a nearby electromagnetic field. Also, qubits must be kept at a temperature of roughly -273.13 degrees Celsius in order to reduce disturbances. For comparison, deep space is roughly -270.45 degrees Celsius. Building a quantum computer has proven challenging due to the need for rather extreme conditions to maintain stability.

Although there are working quantum computers that can perform some tasks, these models are far from being fully operational. Existing quantum computers are limited in the quantum systems they can implement and the problems they can solve. However, it is anticipated that cryptographically relevant quantum computers that could break current encryption standards will be available in the next 10-30 years. It is challenging to foresee with precision the availability of fully operational quantum computers or the extent of their capabilities. The field of quantum computing is undergoing continued research and development, and it is anticipated that significant advancements will be made over the next few years.

THE BUSINESS CASE TO INVEST NOW

Regardless of our ability to predict the exact arrival of the quantum computing era, we must immediately begin preparing our information security systems to resist quantum computing capabilities that fall into the wrong hands. There is no urgent cause for alarm. However, financial services organizations should be aware of quantum cryptography's potential impacts. While the development of quantum computers will result in advancements in both classical computer design and algorithms, it will gradually erode the security of our public-key systems. The goal of PQC preparation is to develop security protocols that secure data against both quantum and classical computers and can interoperate with existing practices.

▶ Current Status of PQC Standards

Since 2016, US National Institute of Standards and Technology (NIST) has been leading an effort to identify and standardize PQC. In July 2022, NIST announced that it had selected several algorithms for standardization. It is expected that NIST will finalize the standards for the selected algorithms soon.

A ROADMAP FOR POST-QUANTUM PREPARATION

I. INVENTORY EXISTING ENCRYPTION ASSETS

It is important for an organization to understand its ability to react to changes in the cryptographic landscape. That understanding requires knowledge of all uses of cryptography across its businesses. Maintaining a cryptographic asset inventory entails more than just knowing the encryption keys and algorithms; it must also include the underlying technology and business processes that are supported.

By building a clear inventory of cryptographic assets and uses, an organization can proactively identify risks and challenges being introduced by advances in PQC and will allow the organization to be crypto agile in planning for future changes in cryptographic requirements.

This information can then be used to develop and implement a risk model. To ensure the potential impact on an organization is adequately monitored, the following items should be considered, captured, and maintained (at a minimum):

- Application Considerations
  - In-house applications and their use of cryptographic algorithms
  - Vendor applications and their use of cryptographic algorithms
  - Inventory of critical and high availability applications
  - Inventory of internal and external application connections
- Vendor Management
  - Vendor roadmaps to support PQC
  - Procurement consideration to support PQC
- Data Considerations
  - How long does the data asset need to be protected
  - Keeping inventory of the organizations most sensitive and critical datasets
  - Is the data at risk from a harvest now/ decrypt later attack scenario
- Regulatory Considerations
  - Be prepared to address questions that may arise from regulators
- Location of Data
  - There may be different timelines associated with different regions

In addition to this brief explainer document, FS-ISAC's Post-Quantum Cryptography Working Group has created a suite of guides to help financial services firms begin the journey of migrating to PQC.

Current State Crypto Agility >

Infrastructure Inventory >

Risk Model >

Future State >

II. ASSESS RISK

The goal of a risk assessment is to understand the likelihood and impact of any particular risk and to help prioritize risks for remediation. The assessment includes identifying the assets, threats, vulnerabilities, and potential impacts of a security incident or data breach. The outcome of the risk assessment should include:

- A comprehensive list of all the risks
- Controls in place to mitigate the risk
- Any actions that are needed to further mitigate the risk

This is sometimes called a risk register and is a comprehensive, well-organized list of every risk that has been identified, as well as any measures being taken to reduce or manage the risk. Risk assessments should also identify higher value and/or higher risk assets that should be leveraged to prioritize quantum remediation. Businesses have a complex task ahead to identify, evaluate, and prioritize remediation efforts to protect their data from cryptanalysis breaches and compromise. Much like the call to action from Y2K, the changes needed in Y2Q (years to quantum) are deep in the fabric of business infrastructure. Replacing cryptographic methods across business processes is a complex endeavor that will necessitate a concerted technological and transformational campaign. Before this tipping point, businesses must immediately begin ensuring that they are resistant to the threats posed by quantum processing.

III. ASSESS VENDORS

Assessing third-party service provider PQC readiness may be a little premature at this time since industry standards, including those being developed by the NIST are in their infancy. However, companies can and should begin thinking about vendor PQC requirements, updating existing risk assessment processes, and updating legal/contract requirements to include PQC provisions. In addition, companies should focus on increasing awareness of PQC amongst vendors. This can be accomplished via information sharing platforms, third-party risk conferences, informational brochures, and social media. The FS-ISAC PQC Working Group developed questions based on the DHS PQC Roadmap to help institutions understand their vendors' PQC status (see Appendix C in the PQC Risk Model paper).

IV. CREATE A RISK ASSESSMENT FRAMEWORK

A risk assessment framework provides an organization with a method to understand and evaluate the threats quantum computing may pose to its information security. These frameworks provide an initial point of reference for risk assessments, allowing processes to develop over time. A risk assessment framework can also serve as a tool that assists in effectively communicating risks to key stakeholders, regardless of their technical expertise. In addition, these frameworks can assist in aligning security goals with existing operational goals and objectives.

The most important aspect of selecting a framework is ensuring that it is "fit for purpose" and optimally suited for the desired results.

Two such framework examples are Mosca's Quantum Risk Assessment (QRA) and the Crypto Agility Risk Assessment Framework (CARAF) Framework (see Appendix B in the PQC Risk Model paper).

V. APPLY A RISK MODEL

The threat of cryptographic relevant quantum computers (CRQC) is significant, but the timeline for when this will happen is unknown. How can an organization quantify the risk of a cryptographically relevant quantum computer when they don't yet exist? The immediate best practice suggests creating several scenarios on the risk a quantum threat is to a specific asset, with some of these scenarios being "more likely" than others.

▶ Wells Fargo Risk Model Example

Wells Fargo has developed a PQC risk model to measure the risk posed by cryptographically relevant quantum computers (CRQCs). The mathematical model is inspired by the methods used to capture the economic externalities of climate change. The risk management challenges posed by climate change and the potential deployment of CRQCs are similar in a few key ways. Both involve highly complex systems with many interconnected variables, and both involve significant uncertainty about the timing and magnitude of potential impacts.

The Wells Fargo PQC risk model involves identifying the risks associated with CRQCs, by compromise, the cryptography utilized by those nodes, and the remediation/cost required to mitigate the nodes. This approach can provide a risk view across applications (data sources) and specific nodes. This approach can help organizations better understand the potential risks posed by CRQCs and take proactive measures to protect against those risks.

Risk Model >

VI. REMEDIATION

Remediation will require companies to migrate to PQC algorithms once they are available. Throughout this process organizations should consider increasing their crypto agility to keep up with the changes in cryptographic technologies and protocols that are going to consistently be changing and evolving due to quantum computers. Companies will also need to work with their third-parties to ensure they are implementing PQC to safeguard against quantum computers.

As the standards evolve, the FS-ISAC working group and others will work with NIST to determine which PQC standards fit the appropriate financial services use cases.

CONCLUSION: WE CANNOT AFFORD TO WAIT

Academic and technology experts, as well as governmental bodies, advise to start now on a multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography. The threat of "harvest now, decrypt later" attacks make this an immediate security risk that needs to be addressed today. This type of harvesting is a long-term strategy where threat actors scrape, collect, or harvest encrypted data through breaches or by undertaking passive interception to hoard encrypted data, waiting for the day when quantum computers can decrypt it. Therefore, it is imperative to start enacting quantum-resistant measures as soon as possible.

In 2023 the FS-ISAC Post-Quantum Cryptography Working Group will work with member institutions to complete the infrastructure, current state, and risk assessments; identify common gaps or needs across the industry for remediation; work with NIST on standards applicability to financial services use cases; and more.

Join >

the All-Members PQC Working Group

CONTRIBUTORS

Peter Bordow *Wells Fargo, Chair, Subgroup Lead*

George Webster *HSBC, Outgoing Vice Chair*

Andrew Mulvenna *HSBC, Incoming Vice Chair*

Mike Silverman *FS-ISAC Lead, Subgroup Lead*

Don Aliberti *Valley, Subgroup Lead*

Sudha Iyer *Citi, Subgroup Lead*

Aaron Chow *Scotiabank*

Robby Burko *Scotiabank*

Bassem Nasser *HSBC*

Carl Mehner *USAA*

Chris Ratcliff *HSBC*

Carlos Recalde *Sheltered Harbor*

Dale Miller *Wells Fargo*

David Edelman *Citi*

Debi Robertson *HSBC*

Erwin Carrow *US Bank*

Guilherme Silva *Scotiabank*

Hala Shakra *Principal Financial*

Jeff Stapleton *Wells Fargo*

Jöerg-Cornelius Schneider *Deutsche Bank*

Joe Chelbeck *Wells Fargo*

Richard Toohey *Wells Fargo*

CIBC