ROSA & ROUBINI
ASSOCIATES

FIN-TECH AND DIGITAL ASSETS

Cyber Security

in a Post-Quantum World

By

Weronika Wiesiolek

25 June 2025

Weronika Wiesiolek

Cyber Security in a Post-Quantum World

25 June 2025

Table of Contents

Rosa & Roubini Associates Ltd is a private limited company registered in England and Wales (Registration number: 10975116) with registered office at 118 Pall Mall, St. James's, London SW1Y 5ED, United Kingdom.

For information about Rosa&Roubini Associates, please send an email to info@rosa-roubini-associates.com or call +44 (0)20 7101 0718.

***Analyst Certification**: I, Weronika Wiesiolek, hereby certify that all the views expressed in this report reflect my personal opinion, which has not been influenced by considerations of Rosa & Roubini Associates' business, nor by personal or client relationships. I also certify that no part of our compensation was, is or will be, directly or indirectly, related to the views expressed in this report.*

***Disclaimer**: All material presented in this report is provided by Rosa & Roubini Associates-Limited for informational purposes only and is not to be used or considered as an offer or a solicitation to sell or to buy, or subscribe for securities, investment products or other financial instruments. Rosa & Roubini Associates Limited does not conduct "investment research" as defined in the FCA Conduct of Business Sourcebook (COBS) section 12 nor does it provide "advice about securities" as defined in the Regulation of Investment Advisors by the U.S. SEC. Rosa & Roubini Associates Limited is not regulated by the FCA, SEC or by any other regulatory body. Nothing in this report shall be deemed to constitute financial or other professional advice in any way, and under no circumstances shall we be liable for any direct or indirect losses, costs or expenses nor for any loss of profit that results from the content of this report or any material in it or website links or references embedded within it. The price and value of financial instruments, securities and investment products referred to in this research and the income from them may fluctuate. Past performance and forecasts should not be treated as a reliable guide of future performance or results; future returns are not guaranteed; and a loss of original capital may occur. This research is based on current public information that Rosa & Roubini Associates considers reliable, but we do not represent it is accurate or complete, and it should not be relied on as such. Rosa & Roubini Associates, its contributors, partners and employees make no representation about the completeness or accuracy of the data, calculations, information or opinions contained in this report. Rosa & Roubini Associates has an internal policy designed to minimize the risk of receiving or misusing confidential or potentially material non-public information. We seek to update our research as appropriate, but the large majority of reports are published at irregular intervals as appropriate in the author's judgment. The information, opinions, estimates and forecasts contained herein are as of the date hereof and may be changed without prior notification. This research is for our clients only and is disseminated and available to all clients simultaneously through electronic publication. Rosa & Roubini Associates is not responsible for the redistribution of our research by third party aggregators. This report is not directed to you if Rosa & Roubini Associates is barred from doing so in your jurisdiction. This report and its content cannot be copied, redistributed or reproduced in part or whole without Rosa & Roubini Associates' written permission.*

Weronika Wiesiolek

Cyber Security in a Post-Quantum World

25 June 2025

Executive Summary

- Most data sooner or later undergo encryption, most commonly based on the Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) standards. There is no classical algorithm which can break them – this is the cornerstone of present-day cybersecurity.
- However once large enough quantum computers are built, they will break both the RSA and ECC standards.
- Luckily, there exists other encryption schemes which we believe will be secure towards both classical and quantum computer attacks. These schemes are often called post-quantum cryptography (PQC).
- Major global economies are working towards creating their own standards of PQC schemes. USA's National Institute of Standards and Technology (NIST) leads the international scene and provides the only fully governmentally standardised PCQ protocols in the world.
- Aside from the challenge of selecting the right PQC protocol, cryptographic migrations suffer from the need for thorough cryptographic discovery. This refers to identifying where and how is cryptography used in a given system, and what new methods are suitable for replacing the existing infrastructure
- There has been engagement with cryptographic discovery schemes and some technology firms are already integrating PQC into their core products and have been commissioned by governments to help with national transitions.
- Cost of transition is high. The US's White House reported that the estimated cost of PQC migration for government systems between 2025-2035 is 7.1 billion US dollars (not including those for national security). Japan has announced a government program with a budget of 29 billion yen.
- This paper focuses on classical methods of counteracting attacks by quantum computers, but can quantum computers enhance cybersecurity? Results have established two key applications: quantum key distribution (QKD) and quantum random number generators (QRNG). QKD is currently being pursued by the UK and US for use in national security matters.

Key Picture: Global Advancements in Post-Quantum Cryptography (2024)

Source: Everest Group. Proprietary & Confidential @2024 Everst Global.inc

Section 1: Introduction

Most of the data we use, share, and create, will sooner or later undergo some sort of encryption. Sending data through the internet, storing on a cloud, or exchanging it with trusted organisations such as banks and governments all require encryption. The most commonly used type of encryption across the industries is based on the RSA and ECC standards. To our current knowledge, there is no classical algorithm which can break them. More precisely, breaking them is exponentially hard, which means it takes an impractical period of time. This apparent unbreakability is the cornerstone of present-day cybersecurity.

This landscape is going to shift dramatically with the advent of quantum computers. Although they are still a nascent technology, there is one thing of which we can be certain - once large enough quantum computers are built, they will break both the RSA and the ECC standards. This is because there is a polynomial-time (fast enough) algorithm, which decrypts the data without knowing any secret “passwords”. Although such computers are some years away, and the precise timelines are difficult to estimate, governments of all major nations are investing heavily in the development of quantum technologies. Especially, the possibility of ”store now, decrypt later” attacks makes present day data vulnerable to future quantum computers. Preparing our sensitive data for the day to come will thus have to start beforehand.

Luckily, there exist other encryption schemes which we believe will be secure towards both classical and quantum computer attacks. In other words, we have not found a quantum algorithm which decrypts them in a polynomial time. These schemes are often called post-quantum cryptography (PQC). Importantly, the schemes themselves are still classical, which means data can be encrypted and decrypted on regular computers. Migration to PQC will be the primary mitigation method to the threat of quantum computers. Such a migration will have to affect IT and operational technologies globally, and the cooperation of parties involved will be crucial in its success - after all, an encryption scheme is only as secure as its weakest link.

The National Cybersecurity Center (NCSC) led by the UK government has included a chapter about PQC in their 2024 Annual Report, highlighting the urgency and inevitability of migration to PQC. As they also stress, it is imperative that the migration targets are uniform across industries cooperating and governments in order to avoid inefficiencies or loopholes in the resultant security scheme. In the summer of 2024, the US National Institute of Science and Technology (NIST) published 3 standards of post-quantum cryptography that should constitute the targets of migration. Other states and industry leaders have been referring to those standards in their guidelines, as well as actively starting the implementation process. The era of post- quantum computing is thus at its dawn, and understanding it is key.

Section 2: Technical Principles and Standards of PQC

2.1 Overview

Post-quantum cryptography is at its core classical. The term encapsulates any classical algorithm that may be used in a cryptographic context and is secure towards quantum attacks. This broad definition leads to the existence of several families of post-quantum cryptographic standards, which in turn can be used in multiple different ways.

These standards are mutually incompatible with each other - all entities partaking in the protocol have to follow the same standard and same scheme to ensure secure communication. Therefore, it is vital to choose a suitable scheme to be enforced onto all parties.

The key trade-offs to consider are not only the time and memory needed to run the algorithm, but also the implementation complexity and security robustness, i.e. under which circumstances is the algorithm guaranteed to be secure.

2.2 Lattice-Based Cryptography

2.2.1 What is lattice-based cryptography?

This family of algorithms is based on the computational hardness of certain mathematical problems involving lattices. Lattices are partially ordered sets where every pair of elements has a unique least upper bound (join) and a unique greatest lower bound (meet). In simpler terms, it's a structure where you can always find the smallest element that is greater than or equal to both elements in a pair, and the largest element that is less than or equal to both elements in a pair. The simplest example of such a problem is the shortest vector problem (SVP), which asks how to approximate the minimal length of a non-zero lattice vector (a vector between 2 points on a given grid). In reality, most popular schemes do not use SVP directly. Instead, they use mathematical problems which have been shown to be equally hard to SVP, or an approximated version of SVP, GapSVP. Reduction to GapSVP is currently deemed sufficient for cryptographic purposes. For instance, the short-integer solution problem (SIS) and learning with errors problem (LWE) are as hard as GapSVP. The term lattice-based cryptography refers to all of them.

Most notably, the learning with errors problem (LWE) is used in 2 of the 3 NIST-approved algorithms, ML-KEM and ML-DSA.

2.2.2 Why is standard LWE not efficient enough?

Lattice-based cryptography in its original formulation is good for security, as it has been proven to be as hard to decrypt as the worst-case lattice problems. However, the size of keys and digital signatures generated with it are very large - too large to be widely implemented in practice. Hence, derivative schemes have been created. In general, excessive size of keys is a recurring issue in various PQC schemes.

2.2.3 Ring-LWE

Ring-LWE is a similar scheme, which is using a modification of the LWE problem using polynomial rings. It has much smaller key signature sizes, and retains the same hardness for the search version of LWE (Given some noisy linear equations satisfied by the secret key, can you find the secret key?) and the decision version of LWE (Given some noisy linear equations satisfied by the secret key, can you distinguish that they are satisfied by the secret key?). These are all desired properties for cryptographic purposes, as if the search problem is easy, it is easy to break encryption, but if the decision problem is easy, one can easily distinguish between encrypted data and random noise. One of the properties of ”good” cryptographic methods is that the attackers cannot even tell whether the data was encrypted. Both search and decision hardness is thus vital for security.

On the other hand, its hardness is only proven to be as hard as the worst-case ideal lattice problems, i.e. it is as hard as a special subset of lattice problems. It is not known whether worst-case ideal lattice problems are as hard as worst-case general lattice problems, but at the moment no known quantum algorithms solve it efficiently.

2.2.4 Module-LWE

Module-LWE, used for the NIST-approved schemes, has been argued to have security advantage over Ring- LWE, or at least be no worse security-wise while offering some implementation advantages, e.g. easier parameter tuning. It is based on module lattices, which have more structure than general lattices, but less structure than ideal lattices, which are a basis for Ring-LWE. While the exact security properties of Module- LWE is still an active area of research, it is currently considered a safer and more conservative alternative to Ring-LWE for standardization.

2.3 Code-Based Cryptography

This family of algorithms is based on the computational hardness of the general linear decoding problem, which solves the following question: given a noisy message and a set of errors that might have occurred during its

transmission, what is the most likely noiseless message that was supposed to be transmitted? This problem is NP-hard for general linear codes.

The size of public keys in code-based cryptography is 10 to 100 times larger than ML-LWE, making implementation more difficult.

However, the security properties are in general better-studied for code-based cryptography schemes. Encryption and decryption are also efficient and easily implemented in hardware. Currently, 3 code-based algorithms are being considered by NIST: Classic McEliece, HQC and BIKE, which makes them a likely new candidate for a NIST-standardised PQC protocol. However, no code-based crypto- graphic scheme has been standardised yet.

2.4 Isogeny-Based Cryptography

This family of algorithms is based on the hardness of computing maps between elliptic curves. Importantly, SIKE, an isogeny-based algorithm was broken by a classical computer in 2022 after qualifying to Round 4 of the NIST call. Similar algorithms are being researched, but for all practical implementations isogeny-based cryptography is currently not considered a viable candidate. This example shows that one cannot forget about classical security when researching new protocols - it may be the case that an encryption scheme cannot be broken by a quantum computer, but it can be broken by a classical one.

2.5 Multivariate Systems-Based Cryptography

This family of algorithms is based on the hardness of solving systems of quadratic equations with many variables. Two algorithms of this kind, Rainbow and GeMSS, advanced to the third round of the NIST call, but were broken since. Currently, those algorithms have also lost their status as potential promising candidates, especially as they would also suffer from large key sizes even if their security was improved.

2.6 Hash-Function-Based Cryptography

This family of algorithms is based only on hash functions, i.e. functions which are easy to compute one- way but hard to invert. One hash-based algorithm, SLH-DSA, is among the ones selected by NIST. It enables one-shot and multiple-shot digital signatures. In terms of memory, public keys are much smaller than ML-LWE (32 or 64 bytes), however, digital signatures are around 10 times larger.

Section 3: Motivation Behind Unification

3.1 Cooperation is Necessary for Security

A cryptographic system can only be used if all parties involved in the protocol follow the same principles. For instance, a server and all its clients have to use post-quantum cryptography in order for the server-client connections to be quantum-secure all the time. In tightly intertwined systems where each machine may be a part of multiple connections, it is necessary to ensure that everyone uses the same cryptographic scheme. It is also possible for a machine to support multiple schemes, although the complexity (and thus cost) of the system increases with the number of supported schemes. Hence, ideally the decision on which algorithms are chosen for PQC transition would be unified between cooperating countries and organisations.

The optimistic part of the challenge is that cryptographic tasks at its core are all very similar. They all involve two parties exchanging information, and require either encryption and decryption of data, or a proof of validity of the exchanged data. Within such a conceptually simple use case, one can reasonably attempt standardisation.

3.2 The Key Cryptographic Tasks in PQC

3.2.1 Overview

State-of-the-art approaches to PQC rely on two different types of protocols: Key Exchange Mechanisms (KEMs) and Digital Signatures (DS). Key Exchange Mechanisms lead to a shared secret and enable the use of standard

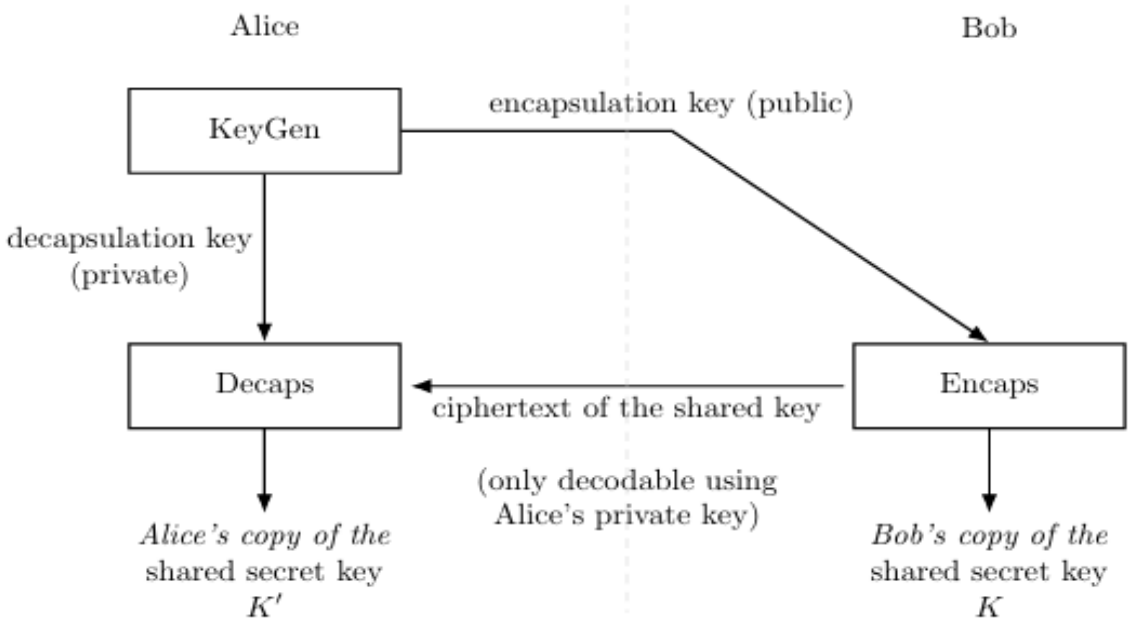
symmetric encryption such as Advanced Encryption Standard (AES). Digital Signatures are a stand-alone asymmetric application of PQC, enabling parties to sign messages or validate signatures.

3.2.2 Key Exchange Mechanisms

KEMs are used to exchange a symmetric key over a public channel, using asymmetric encryption. A symmetric key is essentially a shared secret, unknown to anyone but the two parties which want to communicate. This enables for efficient encryption and decryption of any message on both sides.

Once the symmetric key is exchanged, one can use existing symmetric cryptography schemes such as AES or ChaCha20 to exchange information. A flow of a KEM is as follows:

Figure 1: A simple View of Key Establishment Using a KEM.



Source: Author Generated

Importantly, both parties must follow exactly the same KEM protocol in order to succeed.

3.2.3 Digital Signatures

Digital Signatures, not unlike real ones, are added to a message by its sender as a proof. If Alice signs a message sent to Bob, Bob can verify the following properties:

1. Authentication – ”This message really came from Alice.”
2. Integrity – ”This message has not been changed since Alice sent it.”
3. Non-repudiation – ”Alice cannot deny she signed this.”

To create the DS, Alice uses a private key. To verify the properties above, recipients use a public key.

This scheme is used in many contexts, such as:

- Software updates: software users ensure the update is from the real vendor and has not been modified from the official release version,
- TLS/HTTPS: websites use certificates (with digital signatures) to prove their identity,
- Cryptocurrencies: wallet owners prove that they are authorized to spend coins from a wallet,
- Emails or documents: to prove the identity of the sender or to sign legally binding documents.

Again, both the sender and any party verifying the signature must follow exactly the same guidelines to ensure compatibility and validity of the scheme.

Section 4: International Government Initiatives

Currently, major global economies are working towards creating their own standards of PQC schemes. The following is a list of selected countries and their list of confirmed or considered protocols.

4.1 USA: NIST

NIST leads the international scene in terms of finalised standardisation procedures - currently, it provides the only fully governmentally standardised PQC protocols in the world. Although the second round of the competition is still ongoing, the 3 protocols present in the standard have already been referred to by other countries' cybersecurity bodies. They are also utilised in current early industrial migrations.

4.1.1 Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM, FIPS 203)

This is a KEM based on modular lattice cryptography. It is a derivative of the Crystals-Kyber scheme. Crucially, it consists of two steps. Firstly, modular lattice cryptography ideas are used to construct a public-key encryption (PKE) scheme, referred to as K-PKE. Then, a cryptographic function called the Fujisaki-Okamoto (FO) transform is used to construct a KEM from a PKE.

FO is in principle unrelated to the PQC nature of the scheme, or modular lattice cryptography. It can be used with other schemes to construct a KEM from a PKE. Its advantage is that it enhances the security of the scheme. As a result, ML-KEM is believed to satisfy so-called IND-CCA2 security. Importantly, the scheme K-PKE is not IND-CCA2-secure and shall not be used as a stand-alone scheme.

This highlights the need for using KEMs instead of PKEs. As KEMs yield a symmetric key, the PQC landscape is dominated by symmetric encryption schemes as opposed to public-key cryptography. This is very important for implementation planning, and has informed the actions of businesses engaged in early migrations.

4.1.2 Module-Lattice-Based Digital Signature Standard (ML-DSA, FIPS 204)

This is a digital signature scheme based on module lattice cryptography. It is a derivative of the Crystals-Dilithium scheme. It consists of 3 distinct functions: key generation, signing, and verifying a signature. An important consideration in this scheme is the source of randomness - depending on who and when generates the randomness seed, the scheme gains and loses different security features. In particular, the use of fresh randomness during signing helps mitigate side-channel attacks, while the use of precomputed randomness protects against flaws in the random number generator used by the signer. This suggests that different systems should take different implementation decisions depending on which party or device is more trusted.

4.1.3 Stateless Hash-Based Digital Signature Standard (SLH-DSA, FIPS 205)

This is a digital signature scheme based on combining other currently used hash-based signature schemes together. It is a derivative of the SPHINX+ scheme. It consists of 3 distinct functions: key generation, signing, and verifying a signature. The component schemes are: (1) a few-time signature scheme, forest of random subsets (FORS), and (2) a multi-time signature scheme, the eXtended Merkle Signature Scheme (XMSS). Conceptually, an SLH-DSA key pair consists of a very large set of FORS key pairs. The possibility

to reuse existing and currently used hash-based schemes in SLH-DSA may simplify the implementation. On the other hand, the large size of the signatures may require a significant redesign of other existing infrastructure.

Crucially, all 3 schemes have 10-20 parameters which can be modified, such as private key range, dimensions of matrices involved in mathematical operations, etc. These are all described in their respective FIPS specifications. They influence the key sizes and security of the schemes, thus providing a vast landscape of potential optimisations for particular usages and systems. NIST-suggested parameter sets are assigned numbers, e.g. ML-DSA-44.

Their security assessment is separate, e.g. ML-DSA-44 is claimed to be in security strength category 2, ML-DSA-65 is claimed to be in category 3, and ML-DSA-87 in 5. Definition of security strength categories can be found in another NIST specification.

4.2 UK: NCSC (National Cybersecurity Centre)

On the 20th of March 2025, UK's NCSC published a statement with tangible timelines and examples of necessary migrations. Most notably, their key stages of PQC implementation for an organisation are:

- By 2028, define migration goals according to NCSC guidelines, perform complete cryptographic discovery (find out which systems need an upgrade) and build a migration plan.
- By 2031, perform high-priority PQC migrations and refine the plan.
- By 2035, carry out complete migration to PQC of all your systems, services, and products.

Regarding the PQC standards, while the NCSC mentions the existence of other schemes and technologies, when discussing examples of necessary migrations, they refer exclusively to the NIST standards above. Other organizations highlighted within the report also use NIST-approved schemes; these organizations were listed as providers of key services involved in PQC migrations, whose plans the UK's industry leaders should follow. This suggests that for the NCSC, the earliest migrations are assumed to be done using the NIST-approved schemes.

4.3 European Union: ENISA, European Commission and the NIS 2 directive

The European Union has not yet collated a specific standard such as NIST's FIPS 203-205. Instead, PQC was mentioned in several various reports, so far mostly in the context of increasing awareness and creation of specific national-level and EU-level commissions, whose aim will then be to standardise the PQC schemes and their implementation.

Starting from the broadest viewpoint, documents mentioning PQC refer to EU's NIS 2 Directive (Directive (EU) 2022/2555). NIS 2 aims to enhance cybersecurity across the European Union by establishing a high common level of security for network and information systems.

This framework consists of requirements for certain kinds of organisations, aiming to answer the question: which organisations and companies have what kinds of responsibilities when it comes to ensuring digital safety for the EU? It provides a comprehensive list of priority digital infrastructure followed by a series of obligations to ensure that they are sufficiently protected.

Aside from NIS 2, a new kind of directive was introduced recently: the EU Cyber Solidarity Act (Regulation (EU) 2025/38). Among other purposes, it specifies details about immediate responses and time-sensitive actions. Additional acts address safety of specific sectors, e.g. the financial sector must also comply with the Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554).

The key insight here is that the cybersecurity directives of the European Union give a prominent role to the member states to account for diverse existing infrastructures. Simultaneously, under NIS 2, member states need to designate or establish a competent authority to oversee cybersecurity and compliance with the

EU-wide obligations (Article 8 NIS 2 Directive). On one hand, this may incur overhead in implementation time and cost. On another hand, it may possibly open an opportunity to compare differing systems and provide a market for cross-platform solutions.

The recommendation of European Policy Centre encourages the following roadmap: 1) By 2025, publish the Coordinated Implementation Plan on Post-Quantum Cryptography, and mandate risk assessments of quantum cybersecurity vulnerabilities in key sectors and areas of the European economy. 2) By Autumn 2025, the European Commission should publish a PQC toolbox to help member states and organisations move on to post-

quantum encryption. 3) By the end of 2027, all operators of essential services and public administrations must be able to certify that all sensitive information is PQC-protected.

However, this timeline is not a strict policy declaration from the European Commission themselves - it should be read as a policy advice from the European Policy Centre. So far, no clear implementation timelines have been published by the EC itself.

In January 2024, the EU adopted the first ever European cybersecurity certification scheme. Although not directly related to PQC, it is expected that quantum-safety will become an extension of this framework.

The technical entity overseeing the guidance for PQC implementations is ENISA - the European Union Agency for Cybersecurity. Its last comprehensive report was constructed in 2021, before finalisation of the aforementioned NIST standards. It describes Crystals-Kyber Crystals-Dilithium from the NIST specification, alongside some other encryption schemes/KEMs (e.g. Classic Mc-Eliece, NTRU, Saber, SIKE) and digital signature schemes (e.g. Falcon, Rainbow). Notably, some of the algorithms mentioned have been broken since the publication (SIKE and Rainbow).

Some member states have issued their own reports. For instance, the German Federal Office for Information Security has issued an official recommendation for PQC schemes in January 2025, admitting NIST-approved schemes as well as two other schemes, FrodoKEM and Classic McElliece.

A new report from ENISA is necessary to pursue the roadmap mentioned above. Until then, involved parties have to balance assumptions such as acceptance of the NIST schemes and existence of a centralised infrastructure involving particular PQC protocols, while also admitting the possibility of using other schemes, not yet standardised by NIST, as well as differences in the leading PQC scheme between member states.

4.4 Japan: New Energy and Industrial Technology Development Organization (NEDO)

Japan has not yet published any government-imposed objectives with clear timelines. In July 2024, a project on Strengthening Advanced Cyber Defense Functions and Analytical Capabilities was launched in cooperation with the Cybersecurity Research Consortium, an agglomeration of domestic cybersecurity companies. The project is running continuously from July 2024, and is planned to conclude in June 2027.

Section 5: The Curse of Cryptographic Discovery - Why Implementation Matters

Aside from the challenge of selecting the right PQC protocol, cryptographic migrations suffer from another difficulty - the need for thorough cryptographic discovery. Cryptographic discovery refers to identifying where and how is cryptography used in a given system, and what new methods are suitable for replacing the existing infrastructure. For instance, in the case of systems using public/private cryptographic keys, it is necessary to identify:

- What are all the devices involved in PKEs and their roles,
- How often and under what conditions it happens,
- How much data is exchanged,
- What are the size limits, latencies and throughputs of the exchanging protocols,
- What is the source of randomness.
- Are there any external libraries involved and how does the system depend on them,
- Which further entities in the system rely on the security of the exchanged keys.

This last point is specifically important, as the process “branches” out into further and further dependencies. In government- or industry-scale applications, cryptographic discovery can be responsible for a substantial part of migration costs.

The US National Cybersecurity Center of Excellence (NCCoE), a government entity collaborating with industrial partners, has initiated a campaign to bring awareness to the issue of cryptographic discovery during PQC migrations, which will include developing white papers, playbooks, and proof-of-concept implementations.

Progress is underway in two main ways. Firstly, NIST and NCCoE aim to create resources streamlining the process of cryptographic discovery across main industrial use cases. This involves:

- Outreach to standards developing organizations (SDOs) to raise awareness of necessary algorithm and dependent protocol changes (e.g., Internet Engineering Task Force [IETF], International Organization for Standardization/International Electrotechnical Commission [ISO/IEC]),
- Discovery of all instances where NIST-approved documents will need to be updated or replaced (targetting the FIPS-800 series),
- Identification of automated discovery tools,
- Development of an inventory of where and for what public-key cryptography is usually used in enterprises.

For instance, the early report contains a list of necessary data points to collect during cryptographic discovery, e.g. current key sizes and hardware/software limits on future key sizes and signature sizes, latency and throughput thresholds, etc. Similar, more comprehensive checklists and SoPs are expected to appear in future reports.

Secondly, industry partners are creating automated discovery tools adhering to NIST standards and suitable for the task of PQC migration. Companies focusing on cryptographic discovery aim to alleviate the effort of individual companies and organisations. Further information about particular US industry partners exist on the NCCoE website. While there is no exactly equivalent body in the UK or EU, the UK's NCSC maintains a list of assured providers of cybersecurity-related services and assets, which could be updated to account for PQC services. The NCSC has also stressed the importance of cryptographic agility, noting that most systems will need to support both classical and PQC algorithms during the transition period. To account for this, cryptographic discovery will have to be conducted with a hybrid classical-PQC utility in mind.

Section 6: Industrial Engagement

6.1 Overview

As evident from the engagement in cryptographic discovery schemes, some technology firms are already integrating PQC into their core products, and have been commissioned by governments to help with national transitions. NIST has published a list of companies, currently encompassing 47 members, which will collabo- rate with the NIST within one of 2 streams: The Cryptographic Discovery workstream, focusing on creating the tools to allow organisations to learn where and how cryptography is being used in their systems, as well as conducting risk assessments and prioritisation The Interoperability and Performance workstream, focusing on integrating PQC KEMs and digital signatures within the most common schemes, e.g. the Transport Layer Security (TLS) protocol, the Secure Shell (SSH) protocol and hardware security modules (HSMs).

6.2 Example Engagements of Key Companies

6.2.1 Amazon

Cooperates with NIST, the Internet Engineering Task Force (IETF), The European Telecommunications Standards Institute (ETSI) to standardise cryptographic discovery, implementations, and auditing for PQC migrations. Included ML-KEM and ML-DSA in AWS Libcrypto (AWS-LC), a general-purpose cryptographic library maintained by the AWS Cryptography team for AWS and its customers. Engaged in research and development and purpose-specific optimisations of PQC. Published a migration plan for the coming years.

6.2.2 Microsoft

Participates in an open-source project, Open Quantum Safe, where they help develop the liboqs library to further post-quantum cryptography. Contributes to the following key projects: Post-Quantum Crypto VPN, Post-Quantum TLS, and Post-Quantum SSH.

6.2.3 Google

Extensively working on PQC for web browsing. Introduced hybrid Post-Quantum Key Exchange in Chrome, specifically a combination of the classical X25519 and post-quantum Kyber-768 (X25519Kyber768) in TLS connections from Chrome 116 onwards. Additionally, the Google Cloud Key Management System enabled ML-DSA in February 2025.

They are also currently working on optimising PQC for mobiles and enabling it on Android devices, as well as cooperating within the open-source software group Post-Quantum Cryptography Alliance.

6.2.4 Cisco

Researching and selling PQC hardware for networking purposes since 2013, initially using experimental algorithms. Cisco PQC hardware based on the new NIST standards is expected to become available in late 2025 or 2026. They are also involved in developing discovery and auditing methods such as Quantum Risk Assessment.

Section 7: Cost of the Transition: Key Considerations

The US's White House reported that the estimated cost of PQC migration for government systems between 2025-2035 is 7.1 billion US dollars. This does not involve any migrations for the national security systems, such as those related to intelligence. These are undeniably expected to have a higher per-system cost. The Department of Defense, the Office of the Director of National Intelligence, and the National Manager for NSS are developing separate funding estimates for the migration of NSS to PQC.

The report also highlighted that a large proportion of the cost is stemming from the systems unable to migrate. Those systems will have to be redesigned from scratch, thus incurring very significant costs.

Japan's newly announced governmental program has a budget of 29 billion yen. However, the project does not specifically aim to completely undertake the PQC transition for all governmental infrastructure, so additional costs are likely to follow.

No other organisations have given specific figures on the entire process of PQC migrations. It is clear that the cost will be significant and strongly volatile with respect to changes in research developments, pol- icy, requirements, and specification.

The key costs to consider from the point of view of the organisation are:

- Human resources: as PQC is niche, a team of at least 5-10 specialists will be necessary for most organisations,
- Tools and time needed for cryptographic discovery and creating resources about the cryptographic systems in place,
- Extensive risk-assessment and software testing,
- Procurement, integration and testing of PQC-enabled hardware,
- Replacement of systems which cannot undergo migrations,
- Cost of implementing, maintaining, and rolling back hybrid schemes for the transition period,
- Delays incurred by waiting for a key item or protocol to be finalised by other parties,
- Timing the market: migrating too soon as well as too late could result in security risks and additional costs.

Section 8: Quantum Cryptography: An Alternative?

All the information above was concerned with classical methods of counteracting attacks performed by quantum computers. On the other hand, a question remains: can quantum computers enhance cybersecurity?

This is a vast area of research, with two key applications among the leading established results: quantum key distribution (QKD) and quantum random number generators (QRNG). QKD refers to any protocol which aims to distribute a shared secret between two parties connected by a quantum channel, i.e. the parties can send quantum states between each other. QRNG refers to any method which uses quantum states to generate random numbers. This would supersede classical pseudo-randomness, and guarantee truly random numbers as long as the laws of quantum physics hold, and the QRNG device functions as intended.

Both the public and private sector are investigating the most feasible ways to implement both solutions. Choosing between PQC and QKD/QRNG is by no means necessary - these are two distinct areas, with different research bodies and companies leading the fields.

Before the QKD takes place, there has to exist an authenticated classical channel. In other words, in order to conduct a successful QKD, one needs a classical channel with the following property: it may be eavesdropped on, but it cannot allow for injecting messages, i.e. man-in-the middle attacks. As such, QKD complements classical cryptography, but does not completely eradicate the need for classical PQC.

The key challenge to QKD remains the difficulty of hardware implementations. Importantly, the infrastructure needed for QKD is different from quantum computers - one needs a quantum communication channel and devices which connect to it. Currently, both landline methods such as optical fibres and satellite implementations are being pursued, although the timescales needed for commercialisation of said techniques

are believed to be significantly longer than those of quantum computers. Pragmatically, incorporating QKD into everyday use cases such as web browsers would require everyone connected to use a quantum device. A more promising application for the medium term would be matters of national security, where only very selected devices have to participate in quantum communication. This avenue is currently pursued by the US and the UK.

QRNGs are closer to commercialisation, as selected quantum devices can act as randomness sources for many classical devices, as long as the provider of the device is trusted. It is also possible to combine QRNGs with PQC, incorporating a quantum randomness source as one of the parties in a PQC protocol.

Another actively researched question is: how much trust do all parties have to have in the manufacturer of the quantum device? Surprisingly, certain protocols enable secure exchanges even on devices which may differ from the specification of the manufacturer. This area of research is called device-independent quantum cryptography, or device-independent quantum key distribution (DI-QKD).

In short, quantum cryptography is an active area of research that is expected to complement PQC methods. Its challenges are both theoretical and hardware-related, with the latter being especially prominent in QKD. States and industry leaders engage in quantum cryptography research and development and early implementations. However, as of now, this market is assumed to have no great influence on the future of PQC, and exists largely in parallel.