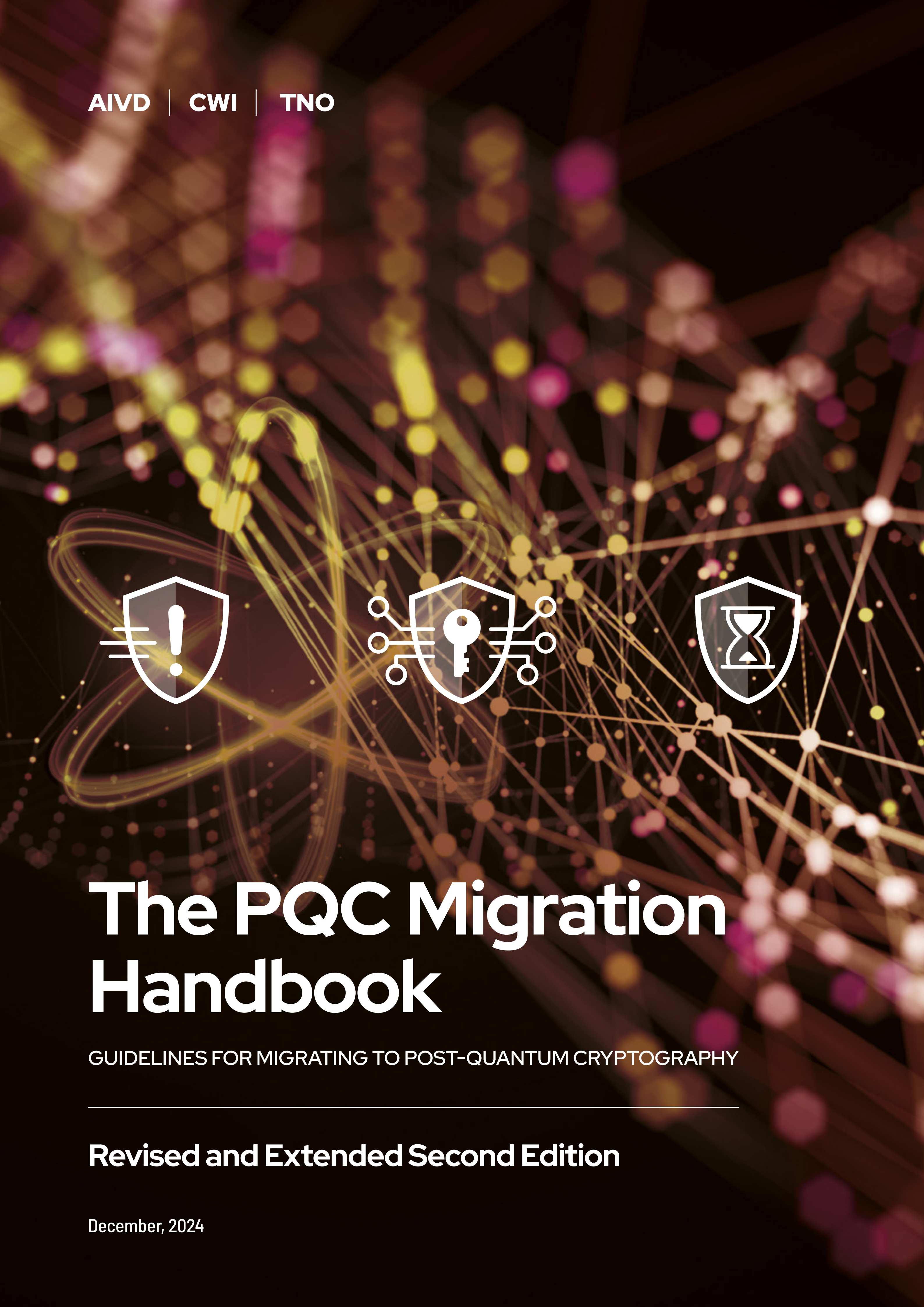
AIVD | CWI | TNO



The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

Revised and Extended Second Edition

December, 2024

AIVD | CWI | TNO

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

Revised and Extended Second Edition

December, 2024

This handbook has been created with the highest standard of care and expertise of the parties involved. The aim of this publication is to create awareness around the urgency to start with migrations and to enhance knowledge of cryptography as an integral part of cybersecurity. Given the fact that its implementation is highly dependent on the type of organisation that is considered and risks involved, this handbook is not intended as a standard approach for each organisation and certain organisations might require additional guidance and advice.

Therefore, no rights can be derived from this publication and included advice may prove to be outdated after publication of this handbook. AIVD, CWI and TNO are under no circumstances liable for any follow-up of the advice given in this publication.

Algemene Inlichtingen- en
Veiligheidsdienst
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

CWI

TNO innovation
for life

Authors Alessandro Amadori, Thomas Attema, Maxime Bombar, João Diogo Duarte, Vincent Dunning, Simona Etinski, Daniël van Gent, Matthieu Lequesne, Ward van der Schoot, Marc Stevens and AIVD Cryptologists and Advisors

Design C10 Ontwerp

Contact thomas.attema@tno.nl

Management Summary

This handbook provides organisations with concrete action perspectives and advice to mitigate the threat posed by quantum computers to today's cryptography. It is an extension of the handbook published in March 2023, incorporating both a revision of the previous content, based on recent developments, and new material.

It is impossible to predict when quantum computers will be able to compromise the cryptographic systems currently in use. Nevertheless, the potential impact of such an event suggests that certain organisations should already begin implementing mitigation measures. For instance, this applies to organisations handling data that should remain confidential for the next decades or those developing long-lived systems that will still be in use decades from now.

The most all-round solution is called *Post-Quantum Cryptography* (PQC). PQC can be implemented in currently used systems and computers, and provides security against attacks by quantum computers. Another touted, partial solution is Quantum Key Distribution (QKD). However, due to the inherent limitations and certain practical and security concerns, currently many security agencies officially recommend only PQC to mitigate the quantum threat.

The migration from quantum-vulnerable cryptography to PQC will be a time-consuming and resource-intensive task. Based on previous migrations, this process could take well over five years. Recently, in August 2024, the first PQC standards were published by the US National Institute of Standards and Technology (NIST), marking the next phase in the PQC migration. Various organisations have already started the PQC migration and regulatory bodies across the globe are preparing and implementing PQC-related legislation. The availability of PQC standards will allow many more organisations to initiate their PQC migrations.

This handbook follows a three step approach to mitigate the quantum threat: (1) *Quantum-Vulnerability Diagnosis*, (2) *Planning* and (3) *Execution*.

The first step, the *Quantum-vulnerability Diagnosis*, contains a number of "no-regret" moves that will enhance an organisation's cyber resilience regardless of the quantum threat. These will help organisations manage their cryptography more effectively and smoothen cryptographic transitions. Proper cryptographic management helps with identifying and resolving risks more easily and reduce response times in the event of an incident, also if this incident is unrelated to quantum computers.

More concretely, all organisations are advised to begin by performing a cryptographic asset discovery to create an inventory of all the cryptography they are using. Furthermore, organisations should already be conducting a quantum risk assessment and integrating it into their existing risk management procedures. Finally, each organisation should review and update its cryptographic policies based on evolving regulatory requirements. This information will provide insight into the stance an organisation should take towards the PQC migration. Having this information in place will also reduce the risk of a hasty, error-prone migration later on, which could introduce unnecessary costs and risks in the future.

During the *Planning* phase, it is important to form a dedicated team to oversee the migration and to ensure that all business processes are in place to facilitate a smooth transition. This handbook pays special attention to so-called *urgent adopters*: organisations that need to start the PQC migration as soon as possible because the impact of a breach in cryptography within the coming decades would be unacceptable. Moreover, it provides tools to assess an organisation's readiness and maturity for a PQC migration.

From a technical perspective, different choices can be made regarding how PQC is implemented, and not all PQC solutions may be suitable for every application scenario. This handbook offers concrete guidance for defining a strategy for deploying PQC, taking into account different application scenarios. PQC deployment may require new hardware or switching to new vendors that support the appropriate PQC solutions.

The final phase is the *Execution* step of the PQC migration. During this phase, organisations must be very careful not to introduce new vulnerabilities. This handbook provides guidance on how to carry out the migration for different types of cryptography and the various strategies developed during the planning phase.

Moreover, cryptography will continue to evolve in the future. For instance, new algorithms or vulnerabilities may be discovered and advancements in cryptanalysis may warrant larger cryptographic keys. Therefore, it is important to establish or maintain a form of *cryptographic agility*. Cryptographic agility enables organisations to quickly modify or replace deployed cryptographic primitives without significantly disrupting organisational processes. This is especially important when cryptographic protocol improvements or new vulnerabilities are identified. This handbook offers direction on how cryptographic agility can be integrated into existing change management processes.

Acknowledgements

We would like to thank Ronald Cramer (CWI & Leiden University) and Maran van Heesch (TNO) for their contributions to the initiation and scoping of this handbook project. Further, we extend our gratitude to the many individuals who contributed to revising and extending the PQC Migration Handbook into this second edition. In particular, we would like to thank Melissa Azouaoui (NXP Semiconductors), Itan Barmes (Deloitte), Nitesh Bharosa (TU Delft), Joppe W. Bos (NXP Semiconductors), Christine Cloostermans (NXP Semiconductors), Oscar Covers (Dutch Banking Association), Gareth T. Davies (NXP Semiconductors), Sander Dorigo (Fox Crypto), Barış Ege (Keysight Technologies), Marie Beth van Egmond (TNO), Dimitri van Esch (Quantum Gateway Foundation), Erik Holkers (DICTU), Andreas Hülsing (TU Eindhoven), Marijn Janssen (TU Delft), Frederik Kerling (TNO), Silke Knossen (KPN), Dion Koeze (NCSC-NL), Ini Kong (TU Delft), Maaike van Leuken (TNO), Anne Nijsten (TNO), Durga Lakshmi Ramachandran (Keysight Technologies), Harld Röling (ABN Amro), Simona Samardjiska (Radboud University), Tobias Schaap (Auditdienst Rijk), Colin Schappin (Deloitte), Pieter Schneider (MinBZK), Peter Schwabe (Max Planck Institute for Security and Privacy & Radboud University), Robert Seepers (NCSC-NL), Thom Sijpesteijn (TNO), André Smulders (MinOCW), Thijs Timmerman (KPMG), Daan van der Valk (Deloitte), Marc van Vliet (TNO), Manon de Vries (TNO), Anita Wehmann (MinBZK), Bas Westerbaan (Cloudflare) and Daniël Worm (TNO). Additionally, we wish to acknowledge the contributions of Shane Gibbons (CWI & Leiden University), Loulou Hanna (MinlenW), Larissa Kalle (NCSC-NL), Oscar Koeroo (MinVWS), Daan Planqué (Ericsson), Eamonn W. Postlethwaite (King's College London), Sterre Romkema (MinlenW) and Germain van der Velden (MinlenW) to the first edition of this handbook.

This handbook is funded by the Dutch General Intelligence and Security Service (AIVD).

Contents

Contents

1 Introduction

This handbook[1] aims to help organisations identify the risks posed by quantum computers to their IT infrastructures and to offer actionable strategies for mitigating these risks. While various prior works have already highlighted these risks and the urgency of implementing appropriate countermeasures, this handbook builds on those recommendations by providing concrete, actionable guidance. It is particularly aimed at organisations that cannot afford to delay, often referred to as *urgent adopters*. However, as nearly every organisation relies on cryptography, all are, to some extent, vulnerable to the potential threats posed by quantum computers.

Cryptography is of paramount importance in today's digital society, forming an integral part of cybersecurity for all organisations. Strong cryptography is essential for preventing the theft of sensitive or confidential data, ensuring data integrity and authenticity, and preventing unauthorised access to systems. In contrast, weak cryptography poses an unacceptable risk, potentially leading to data breaches, unauthorised access, stolen corporate or state secrets, and even more severe consequences.

However, a significant portion of the cryptography currently in use is weakened or rendered completely insecure by the advent of quantum computers. At present, quantum computers are not yet powerful enough to break the cryptographic systems currently in use, but their development is accelerating. Although somewhat speculative, it is anticipated that within ten to twenty years, quantum computers may be capable of breaking some of the cryptography that is ubiquitous today. Cryptography that is secure against classical computers, but not against quantum computers, is referred to as *quantum-vulnerable*. Cryptography that is also secure against quantum attacks is known as *Post-Quantum Cryptography* (PQC). There are several compelling reasons for organisations to begin addressing the quantum threat today by initiating the migration to PQC, even though cryptographically relevant quantum computers have not yet been realised:

1. **Store-Now-Decrypt-Later Attacks** | Sensitive information is at risk of being intercepted and stored now, only to be decrypted in the future with a quantum computer. Therefore, data that must remain protected over a long period is already at risk of being decrypted before the end of its intended confidentiality period.

2. **Long-Lived Systems** | It may be difficult or even impossible to update long-lived systems and critical infrastructures being developed and deployed today to PQC. Even if software updates are possible, PQC may require more advanced hardware to function, which might be irreplaceable once the system is deployed.

3. **Complexity of Cryptographic Migration** | Updating or replacing a cryptographic infrastructure with post-quantum alternatives is a complex and time-consuming task. Based on previous migrations, it is expected that fully migrating to PQC could take many years. For example, it took many organisations over five years to migrate from the vulnerable primitive SHA-1 to its secure successor SHA-256, even after the necessary specifications and implementations were available.

4. **State-of-the-Art** | PQC is more and more considered to be the state-of-the-art in cryptography, and many organisations, both governmental and industrial, have already begun adopting it. To remain interoperable and up-to-date with the cybersecurity measures, timely deployment of PQC is essential.

[1] A previous version of this handbook was published in 2023. This new edition includes updates and modifications throughout, reflecting new insights and recent developments. Moreover, additional material has been included to further specify the recommended actions and perspectives. Section 1.3.1 provides a detailed overview of the changes relative to the 2023 version.

5. **No-Regret Moves** | Many initial steps in the PQC migration can be considered no-regret moves. These actions are valuable regardless of developments in quantum computing. For instance, besides facilitating the PQC migration, cryptographic asset management enhances the efficient handling of cryptographic incidents beyond quantum attacks, such as key compromise.

Fortunately, the PQC migration is already underway. Front-runners in this field have begun deploying PQC in their IT infrastructures, and regulatory bodies all over the world are preparing and publishing PQC-related legislation. Furthermore, the recent publication of NIST's PQC standards marks a new phase in this migration. With these standards now available, more organisations can begin deploying PQC.

While it is challenging to estimate the exact costs of the PQC migration, it is clear that every organisation will need to allocate resources, including people, time, and money. Moreover, due to the more demanding hardware requirements of PQC, the migration may not be limited to a software update.

To assist organisations migrate to PQC, this handbook offers a three-step approach (1) *Quantum-Vulnerability Diagnosis*, (2) *Planning* and (3) *Execution*. All organisations are recommended to start with the Quantum-vulnerability diagnosis. This involves creating an inventory of the cryptographic primitives and protocols currently deployed within the organisation, as well as identifying the data and communication channels these cryptographic measures are intended to protect. Based on this inventory, a comprehensive (quantum) risk assessment can be conducted, assessing, for example, the urgency of migrating to PQC.

With this diagnosis in hand, organisations can start the next steps: the *planning* and *execution* of a structured PQC migration. Delaying this process and resorting to a hasty migration under pressure increases the risk of costly mistakes. Additionally, many cryptographic assets are managed by vendors. These vendors require time to update their products based on an organisation's evolving requirements. It is advisable to demand PQC readiness from vendors as soon as possible.

Finally, the field of cryptography is still rapidly developing and new cryptographic developments may call for more migrations in the future, e.g., due to newer better fitting standards and/or new security recommendations. For this reason, we recommend establishing as much cryptographic agility as possible when revising existing cryptographic infrastructures. Cryptographic agility allows the upcoming and future migrations to be executed more efficiently.

1.1) Goal of this Handbook

The purpose of this document is to assist organisations in their migration to post-quantum cryptography by offering concrete, actionable guidance. This handbook is specifically aimed at organisations where the impact of a cryptographic vulnerability would be severe, necessitating the prompt initiation of the PQC migration process. However, it is advisable for all organisations to begin this transition as soon as possible to mitigate the risks of unforeseen events.

This handbook provides detailed information on the risks, actionable strategies, and the advantages and disadvantages of early migrating to PQC, along with practical advice on creating a migration plan tailored to an organisation. It is important to note that the responsibility for developing a migration plan that aligns with an organisation's specific risk appetite ultimately lies with each organisation.

For individuals seeking a more high-level overview of the threat posed by quantum computers to cryptography, we recommend referring to earlier publications such as [MvH20] and [NLNCSA21]. In contrast to these works, this handbook offers more concrete recommendations to help organisations begin take action.

We recognise that the diversity of organisations necessitates tailored advice for the PQC migration. Therefore, our recommendations are customised for various organisational groups, enabling each entity to receive guidance that best suits its needs. It is also important to consider that even within a single organisation, different departments or teams may have varying levels of urgency based on the specific data or systems they manage.

1.2) The Quantum Threat

Many assets currently protected by cryptography are at risk of being compromised by quantum computers. However, accurately quantifying this risk is challenging, and precise predictions are difficult to make. This section outlines the considerations surrounding the risks posed by quantum computers.

First, certain quantum algorithms, most notably Shor's and Grover's algorithms [Sho94; Gro96], have the potential to weaken or completely break specific cryptographic primitives. Executing these algorithms requires a sufficiently powerful quantum computer, often referred to as a *cryptographically relevant quantum computer*. While such a quantum computer does not yet (appear to) exist, significant progress in quantum computing has been made over the past years. As a result, the cryptographic community has increasingly focused on the development and deployment of cryptography that can withstand quantum attacks. Although new cryptographic standards have recently been introduced, many systems have yet to migrate to post-quantum cryptography.

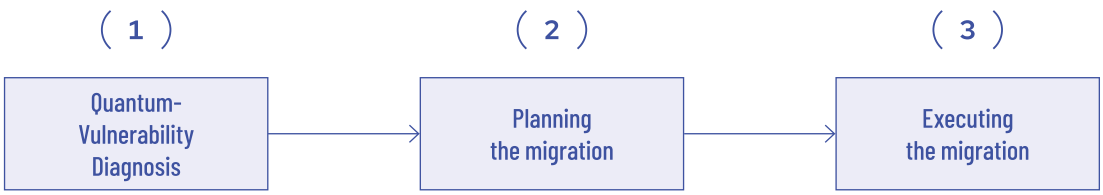
Various attempts have been made to predict when a cryptographically relevant quantum computer will become available, with estimates ranging from 10 years to "it will never happen." However, such predictions are fraught with uncertainty, as unforeseen developments could drastically alter these timelines. At the same time, it is clear that the impact of a cryptographically relevant quantum computer will be significant, and the risk to organisations will increase the longer they delay their migration to PQC. Therefore, we strongly recommend that organisations take the initial steps towards PQC migration as soon as possible.

Second, the level of risk depends on the type of assets being protected. If an asset, such as a system or a dataset, has a lifespan that extends beyond the anticipated arrival of cryptographically relevant quantum computers, the risk is already high. In such cases, migration should be prioritised and undertaken as soon as possible. Conversely, assets related to functions like authentication and system availability, which cannot be attacked retrospectively, are only at risk of immediate attack once a quantum device becomes fully operational. Consequently, these assets may require a different level of urgency in the migration process.

Finally, the duration of the migration process for all assets is uncertain. Based on previous (and smaller) migrations, it is likely that a full transition could take more than five years. Therefore, depending on their risk appetite, organisations should begin preparing for migration now. Without undertaking the actual migration, organisations can start by identifying vulnerable assets, prioritising them, and developing a migration plan. This proactive approach minimises the risks associated with delays and the costs of unexpected setbacks during the eventual migration.

1.3) Document Structure & Reading Guide

On a high level, this handbook follows a three-step approach as also described in [ETSI20a]:



(1) In Chapter 2, the Quantum-vulnerability diagnosis is described. This chapter is primarily intended for strategy and policymakers and may require the involvement of individuals with knowledge of the type of data and assets within an organisation. First, the urgency for an organisation to migrate is assessed. To this end, the concept of *PQC Personas* is introduced. These personas are designed to help organisations determine their stance towards PQC migration. To identify an organisation with one or more personas, (visual) decision trees and schemas are provided. Following this, an inventory should be made of all cryptographic protocols and the systems using this cryptography.

Chapter 3 outlines the planning of the migration process at both a technical and organisational level. Based on the urgency identified in the previous chapter, it is recommended that urgent adopters read this section thoroughly. After the diagnosis, the urgency level and the cryptography that needs to be migrated will have been identified. Using this information, the next step is to decide on the mitigation strategies to be implemented for vulnerable assets. Additionally, the timing of the migration process for various assets must be determined at this stage. The target audience for this chapter remains strategy and policymakers, as they are responsible for planning and prioritising the migration process and assembling the right team to carry out the migration. Furthermore, this chapter will be of interest to (security) architects who will lead the migration process from a technical perspective.

Chapter 4 is primarily intended for a technical audience. In this chapter, technical guidelines are provided to determine *how* the cryptography needs to be migrated. First, general strategies and considerations for migrating cryptography are presented. This is followed by strategies for specific cryptographic algorithms and protocols.

Chapter 5 discusses recent developments in the field of (post-quantum) cryptography, including PQC standardisation initiatives and legislative developments. This chapter is mainly intended for a technical audience.

Finally, Chapter 6 provides in-depth technical information on various popular cryptographic constructions. This chapter mainly serves as a reference for looking up details of cryptography being used by an organisation. It is not necessary to read this chapter in its entirety. The intended audience for this chapter includes technical leads of the migration process as well as (security/cryptographic) developers who will be working on the migration.

1.3.1 Revisions and Extensions Since the First Edition

This handbook extends and revises the PQC Migration Handbook that was published in March 2023. All previous content is included but revised to reflect the developments that have taken place. Additionally, the following new material has been incorporated into this second edition:

- Section 1.6 provides a list of no-regret moves;
- Section 2.3 covers cryptographic asset management, detailing the creation of a cryptographic inventory;
- Section 2.4 offers a methodology for performing a quantum risk assessment;
- Section 3.2.2 addresses common organisational challenges towards mature cryptographic management and provides a PQC maturity assessment strategy;
- Section 4.4 discusses cryptographic agility;
- Chapter 5 presents recent international developments related to the PQC migration;
- Section 6.5 offers an overview of advanced security requirements such as side-channel resistance and hardware security;
- Section 6.6 discusses cryptographic libraries that have implemented PQC.

1.4) Cryptography Background

Before going into the PQC migration itself, we explain some fundamentals from cryptography.

	Symmetric-key	Asymmetric-key
Encryption	Authenticated Encryption, Block Cipher + Mode, Stream Cipher	Public-key Encryption
Authentication / Integrity	Authenticated Encryption, Message Authentication Code	Digital Signature
Key Generation / Distribution	(Pseudo) Random Number Generator	Key Exchange, Key Encapsulation

Table 1.1 | Overview of some building blocks used to achieve certain cryptographic goals, using either symmetric or asymmetric keys.

Cryptography aims to protect information and communication channels from adversarial entities. It focuses on four main principles:

- Confidentiality ensures that sensitive data is not disclosed to unintended recipients;
- Authenticity involves verifying the source of a message;
- Integrity aims to ensure that data has not been altered by untrusted entities;
- Non-repudiation prevents senders and recipients from denying their involvement in sending or receiving specific messages.

The building blocks in cryptography are referred to as cryptographic primitives. These low-level algorithms can be combined to form more complex cryptographic protocols. Examples of *primitives* include RSA and AES, while examples of *protocols* include TLS and SSH. An overview of essential functionalities is provided in Table 1.1.

One of the most well-known cryptographic functionalities is provided by encryption schemes. They protect the confidentiality of data and prevent it from being intercepted by unauthorised parties. *Encryption schemes* use an encryption key to transform the data into ciphertext, which can only be decrypted with the correct decryption key.[2]

Another widely used cryptographic functionality is provided by *signature schemes*. These schemes aim to prove the authenticity and integrity of data. A signing key is used to sign the data, and the signature can then be verified with a verification key.

Cryptographic primitives require cryptographic keys to operate securely. It is crucial that these keys are generated in a secure manner. The cryptographic primitives responsible for generating keys are referred to as *key generation* mechanisms.

Cryptographic keys can be either *symmetric* or *asymmetric*, leading to symmetric-key or asymmetric-key cryptography. In symmetric-key cryptography, encryption and decryption (or signing and verification in the case of signature schemes) are done with the same key. Hence, the involved paries must agree on such a key in advance. The problem of establishing a shared key between two parties intending to use symmetric-key primitives is known as the *key distribution problem*.

[2] Some encryption schemes can also provide authenticity and non-repudiation.

Asymmetric-key cryptography, also known as public-key cryptography, does not suffer from the key distribution problem because it uses two different keys: a *public* key and a *private* key. One party generates the key pair and publicly announces the public key, allowing anyone to encrypt messages or verify signatures. However, only the holder of the private key can decrypt messages or generate signatures.

Symmetric-key cryptography is generally more efficient than asymmetric-key cryptography. For this reason, the less efficient asymmetric primitives are often used to establish a symmetric key, thus solving the key distribution problem. Once the symmetric key is shared, more efficient symmetric primitives, such as AES, can be used to protect the communication channel. The asymmetric primitives used to establish a shared symmetric key between two parties are referred to as *Key Exchange* (KE) algorithms or *Key Encapsulation Mechanisms* (KEMs). There is a subtle difference in how KEs and KEMs solve the key distribution problem, but this difference is outside the scope of this document. Therefore, we will group these two types of primitives throughout. We do note that, in most application scenarios, the functional difference between KEs and KEMs does not play a significant role. However, replacing a KE with a KEM, or vice versa, may present certain cryptographic engineering challenges.

Additionally, *hash functions* convert a message into a digest, making it easy to verify that a given digest corresponds to a specific message. At the same time, it is difficult to reverse-engineer the original message from the digest or to find two different messages with the same digest. Hash functions do not necessarily require a cryptographic key to operate, but when a key is used (as in keyed hash functions), it is a symmetric key. For this reason, hash functions are often grouped with symmetric-key primitives. Finally, *Message Authentication Codes* (MACs) ensure authenticity and integrity by creating a tag for a message, allowing the receiver to verify that the message was sent by the intended party and has not been altered in transit. MACs are typically constructed from hash functions or block ciphers.

Threat of Quantum Computers

The impact of quantum computers on the above primitives varies. Grover's quantum algorithm [Gro96] theoretically provides a quadratic speed-up in attacking symmetric-key cryptography. This means that the security level of a hash function or symmetric-key encryption scheme is effectively halved. This reduction can be mitigated by doubling the key size of symmetric primitives. However, more detailed cost evaluations of the Grover attack suggest this approach might to be overly conservative [JNRV20]. In fact, there is growing consensus that quantum computers offer limited advantage in attacking symmetric-key primitives (and hash functions) [GLRS16].

Conversely, the most common asymmetric-key primitives today will be completely compromised by Shor's quantum algorithm [Sho94]. As a result, algorithms such as RSA, ECDH, ECDSA, and EdDSA will no longer be secure once a cryptographically relevant quantum computer becomes available. Therefore, quantum computers are primarily expected to affect asymmetric-key cryptography.

About Quantum Key Distribution

One of asymmetric-key cryptography's main applications is key distribution; establishing a shared symmetric key between two entities. By using symmetric-key cryptography, such a key can be used to encrypt and authenticate communication channels. Combining asymmetric and symmetric cryptography in this manner is typically much more efficient than solely relying on asymmetric cryptography and therefore common practice.

In contrast to asymmetric cryptography, Quantum Key Distribution (QKD) leverages quantum mechanical properties in order to solve the key distribution problem. The security of QKD protocols does not rely on computational hardness assumptions, and QKD is therefore secure against both classical and quantum adversaries. For this reason, QKD is oftentimes promoted as an alternative for post-quantum cryptography.

However, QKD suffers from certain inherent limitations, impacting its applicability. Additionally, many security experts believe QKD currently lacks the maturity to achieve the level of security desired in most applications. For this reason, in order to mitigate the quantum threat, migrating to PQC should be prioritised over QKD deployment. Various security agencies share this position on QKD, e.g., ANSSI (France) [ANSSI20], BSI (Germany) [BSI22], NLNCSA (The Netherlands) [NLNCSA21], NSA (USA) [NSA21b] and UK-NCSC (UK) [NCSC-UK20b]. Moreover, recently the Dutch, French, German and Swedish agencies published a position paper on QKD [ABNS24], elaborating on the main limitations of this technology. Below the main observations from this position paper are summarised.

First, whereas PQC serves various cryptographic purposes, QKD only realises a key distribution functionality and the technology itself requires cryptographic authentication. Second, QKD has not undergone a thorough standardisation process, providing the confidence required in cryptographic applications. Third, QKD protocols currently do not admit satisfiable security proofs. Although significant progress has been made, the abstract mathematical models currently used to prove QKD's security do not adequately capture reality. Fourth, QKD suffers from distance limitations. More precisely, two parties using QKD must be connected via a quantum communication channel, i.e., via an optical fibre or an optical (free-space) communication channel. A low noise level on this communication channel is required, limiting its maximal distance. A solution to overcome this distance limitation is the use of repeaters. Currently the technological maturity of untrusted repeaters is insufficient to overcome the QKD distance limitation. For this reason, one must rely on trusted repeaters, introducing trusted third parties with access to the unencrypted sensitive information. In other words, end-to-end security over longer distances is currently unachievable. Finally, to communicate securely using QKD, dedicated and expensive quantum hardware is required. Hence, QKD requires large infrastructure investments, and the specific equipment used for QKD introduces new attack vectors.

Altogether, post-quantum cryptography is more mature, more flexible and less expensive than quantum key distribution. PQC can replace quantum-vulnerable cryptography in all contexts as it is able to be executed on machines similar to the ones in use now. There is much research focusing on reducing the current limitations of QKD and improving its security guarantees. However, for the time being, we advise against relying on the security of QKD solutions.

1.5) International Regulations and Advice

Several international organisations have released guidelines regarding the threat of quantum computers. There is a strong consensus on the urgency of migrating to quantum-safe cryptographic primitives, and many organisations emphasize the importance of a well-coordinated PQC migration effort. The first step being the inventory of the cryptographic assets to migrate, and the development of a precise roadmap. To ensure a smooth transition, stakeholders are encouraged to remain cryptographically agile so as to be able to quickly adapt to new developments.

However, some contradictions arise regarding the specifics of the implementation and the pace of the PQC migration. Some EU member states such as Germany, France and The Netherlands advocate the deployment of PQC in hybrid combinations with established, but quantum-vulnerable, cryptography. Hybridisation mitigates the risk of undiscovered vulnerabilities in the PQC primitives. However, hybridisation may potentially increase the attack surface, as it increases the complexity of the cryptographic solution. For this reason, the UK recommends hybridisation only when absolutely necessary.

Finally, even though the European Commission considers QKD as a potential solution to mitigate the threat of quantum computers, security agencies generally agree that it is currently not mature enough for widespread adoption.

1.6) No-Regret Moves

Today's encrypted data is already at risk of being harvested now to be decrypted later by quantum computers. While quantum computers are steadily growing stronger, handling more qubits and performing more complex computations, it remains unclear when the quantum threat to cryptography will manifest. Some sceptics even argue that a cryptographically relevant quantum computer will never see the light of day. Nevertheless, for many organisations the impact of a quantum breach in their cryptographic defences would be too severe to ignore. In fact, the first post-quantum standards have now been published and their deployment has already begun.

At the same time, the field of post-quantum cryptography is still an active research area, with many open questions and much potential for new developments. In particular, both NIST and ISO will continue their PQC standardisation efforts, likely expanding the list of available PQC standards in the years to come.

The above uncertainties, regarding both the risks posed by quantum computers and their mitigation measures, may cause reluctance in starting the PQC migration. However, procrastinating this complex task is a risky endeavour. Fortunately, the first steps of the PQC migration, detailed in this handbook, can be considered to be no-regret moves. These actions are valuable regardless of the developments in quantum computing and post-quantum cryptography. Below we summarise a number of no-regret moves in the context of the PQC migration.

Assess Supply Chain Dependencies (Section 2.1) | Cryptography is typically incorporated in IT products and organisations rely on their vendors to update these cryptographic algorithms. Appropriate risk management involves inventorying such dependencies. Subsequently, organisations can initiate the discussion about and alignment of PQC migration strategies with their vendors. The other way around, it is also important to inventory the organisations that are impacted by your cryptographic decisions.

Establish Cryptographic Asset Management (Section 2.3) | Software, and thus also cryptographic implementations, may contain bugs and vulnerabilities, even if a cryptographically relevant quantum computer will never materialise. Cryptographic asset management helps organisations to efficiently identify and resolve such vulnerabilities. Moreover, cryptographic asset management can significantly reduce incident response times, and therefore limit the impact in the case of key compromise or certificate expiration. It is an important step in realising cryptographic agility. Furthermore, it is an essential step in order to conduct a quantum risk assessment.

Review Cryptographic Policies (Section 2.3 and 4.4) | Given both the technical and regulatory developments, an organisation's cryptographic policies may require revision. Ensure policies are compliant with legislation, anticipate regulatory changes and reflect the findings from the quantum risk assessment.

Conduct Risk Assessment (Section 2.4) | Organisations should incorporate the quantum threat in their risk management procedures. This quantum risk assessment is essential in determining when and how to migrate to post-quantum cryptography.

Estimate the Costs of Migration (Section 3.3) | Decision makers require a detailed cost overview when deciding on various aspects of the PQC migration. For instance, determining the optimal timing for migrating different parts of the cryptographic infrastructure. A comprehensive cost overview, encompassing both financial and capacity considerations, will streamline decision-making processes and avoid unnecessary delays.

Inventory Regulatory Requirements (Chapter 5) | In many sectors, the deployment of appropriate cryptographic algorithms, as a cyber security measure, is mandatory. It is expected that regulatory bodies will at some point require the deployment of new PQC standards, and soon publish timelines for the deprecation of older cryptographic standards. For this reason, it is important to stay informed not only about technical developments, but also about the regulatory changes.

Provide a Back Up Plan | In case of unforeseen developments, such as a breakthrough in quantum computing or an attack on an established cryptographic standard, a deviation from the original migration plan may be required. Plan how to establish business continuity and avoid down-time in such events.

Collaborate with Peers | The PQC migration is a global challenge that should be tackled collaboratively. Many organisations face similar challenges and thus collaboration will allow for an effective and efficient PQC migration. Organisations can share experiences and lessons learnt, both on a technical and organisational level. Additionally, collaboration is essential in maintaining interoperability across organisations.

1.7) Cryptographic Maturity

Beyond the scope of the PQC migration, it is extremely valuable for organisations to achieve a certain level of maturity in managing their cryptographic assets. In fact, achieving cryptographic maturity can be considered a no-regret move; valuable regardless of the quantum threat.
An organisation is considered mature with respect to its cryptographic management if:

- it has a complete overview of its cryptographic assets;
- it has insights into the risks related to its cryptography;
- it has a cryptographic policy in line with relevant rules and regulations;
- it continuously monitors and updates the preceding items.

First of all, proper management and monitoring of cryptography will not only help an organisation to facilitate the PQC migration, but to mitigate risks related to cryptography in general. While cryptographic maturity saves time and effort, for many organisations it is difficult to implement or maintain.

A number of steps are required before an organisation can be considered cryptographically mature. A schematic overview of common organisational challenges with respect to cryptography management before and during the PQC migration can be found in Figure 1.1. The figure shows how a properly executed PQC migration will establish cryptographic maturity.
As can be seen, an essential first step in a cryptographic migration is acknowledging when the migration needs to happen. While this sounds straightforward, a lack of urgency from decision makers is a typical bottleneck.
Afterwards, a diagnosis needs to be performed. A mature organisation should have streamlined asset management in place, which continuously updates a cryptographic inventory. If this is not yet the case, the PQC migration is a good opportunity to improve an organisation's cryptographic asset management. For example, implementing centralised cryptography management across an organisation can help in obtaining better visibility and easier management.
Next, a quantum risk assessment should make clear what assets are under what level of threat from a quantum computer. The methodology provided in Section 2.4 gives handles to perform the assessment against the threat of the quantum computer. The quantum risk assessment needs to be repeated continuously to give an accurate overview of the current risks. Mature organisations should typically have dedicated

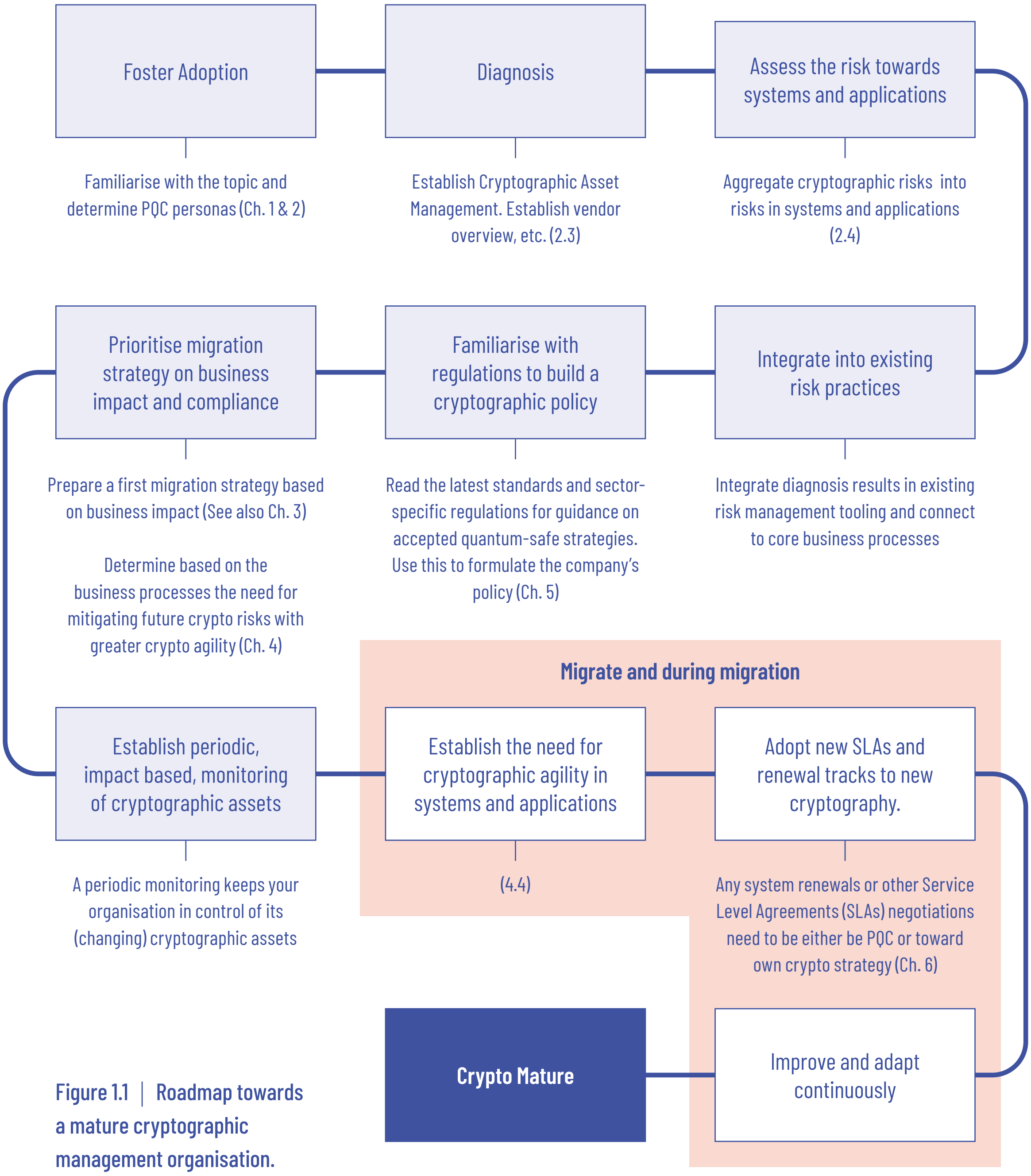

Foster Adoption
Familiarise with the topic and determine PQC personas (Ch. 1 & 2)
Diagnosis
Establish Cryptographic Asset Management. Establish vendor overview, etc. (2.3)
Assess the risk towards systems and applications
Aggregate cryptographic risks into risks in systems and applications (2.4)
Integrate into existing risk practices
Integrate diagnosis results in existing risk management tooling and connect to core business processes
Familiarise with regulations to build a cryptographic policy
Read the latest standards and sector-specific regulations for guidance on accepted quantum-safe strategies. Use this to formulate the company's policy (Ch. 5)
Prioritise migration strategy on business impact and compliance
Prepare a first migration strategy based on business impact (See also Ch. 3)
Determine based on the business processes the need for mitigating future crypto risks with greater crypto agility (Ch. 4)
Establish periodic, impact based, monitoring of cryptographic assets
A periodic monitoring keeps your organisation in control of its (changing) cryptographic assets
Migrate and during migration
Establish the need for cryptographic agility in systems and applications
(4.4)
Adopt new SLAs and renewal tracks to new cryptography.
Any system renewals or other Service Level Agreements (SLAs) negotiations need to be either be PQC or toward own crypto strategy (Ch. 6)
Improve and adapt continuously
Crypto Mature

Figure 1.1 | Roadmap towards a mature cryptographic management organisation.

systems and people to manage all sorts of risks an organisation faces. Integrating the risks introduced by a potential threat is an essential step to manage these risks properly as well. By integrating it into existing risk management strategies, a connection between risks and their effects on core business processes can be established.

While organisations can manage their dependencies and cryptographic assets themselves, there will also be regulations in place that force them to adhere to certain best practices with regards to cryptographic management as well as migration to new cryptographic solutions. Therefore, it is essential for each organisation to be aware of which regulations apply to them. Based on these regulations and their own objectives, a mature organisation should have a proper policy for cryptographic management in place. Furthermore, this policy should comply with the relevant regulations. The contents and form of such a policy is explained in Section 2.3.1.

Based on compliance with the regulations and insights into risks to the organisation as a whole, a mature organisation should make a priority list of what systems, applications, data, etc. should be migrated in what order. Furthermore, this prioritisation should identify what future risks should be dealt with, for example by implementing a greater level of agility. As mentioned before, all of these steps (diagnosis, risk assessment, policy and prioritisation) should be reassessed periodically to maintain an up-to-date overview of the current status.

Finally, during the migration, a mature organisation can implement a greater level of cryptographic agility, especially for assets that they are managing themselves. For assets that are managed by others, an organisation should assess whether the suppliers' timelines with respect to integrating new cryptography match their own timelines and objectives and if not, find new suppliers or start managing the cryptography themselves. An overview of forms of cryptographic agility is provided in Section 4.4.

An organisation that has achieved a higher level of cryptographic agility can more easily switch cryptographic algorithms and systems to meet new standards, security practices, and face new threats. This shows that the organisation is mature in its use of cryptography and can quickly adapt to maintain its security levels.

Step 1

2 Quantum-Vulnerability Diagnosis

Summary

This chapter provides concrete guidance on how to determine the quantum risk and the urgency for migrating to PQC standards and what organisations need to start this migration. The first part of this chapter gives handles for whether an organisation should already start taking first steps towards PQC migration. This is achieved by dividing the landscape of organisations into different personas, so that each (sub)organisation identifies as at least one of these personas. The second part advises on the infrastructure diagnosis that organisations should make before embarking on the PQC migration.

The persona(s) of an organisation depend on a couple of factors, such as the sort of data and systems handled, the threat level and its dependency on other organisations. With these factors, three main personas can be drafted, namely *Urgent Adopters*, *Regular Adopters* and *Cryptography Experts*. Firstly, Urgent Adopters are organisations that should already start taking steps towards PQC migration now, or should already have done so. Secondly, Regular Adopters are organisations that can take a more reactive stance towards PQC migration for now, as their assets allow awaiting further development of PQC standards and production-ready implementations before starting with migration. Lastly, Cryptography Experts are organisations that supply, service or deliver cryptographic knowledge or infrastructure to other organisations. This chapter contains sufficient information for organisations to decide which persona(s) they identify as.

If an organisation identifies itself as an Urgent Adopter, we advise to start its *Quantum-Vulnerability Diagnosis* as soon as possible. This involves gathering the necessary data concerning the current security architecture to decide which assets should be migrated first. This step requires the establishment of four documents a risk assessment; an inventory of cryptographic assets used in the organisation; an inventory of the data handled by the organisation; and an inventory of the suppliers of cryptographic assets. Organisations that do not identify as Urgent Adopters can wait before performing this Quantum-Vulnerability diagnosis, although in some cases it might be beneficial to start this diagnosis now as well as it is considered as part of the no-regret moves.

The subsequent chapters focus on advice for the Urgent Adopters. It is vital that PQC personas get determined accurately, to ensure that all organisations that need to take PQC migration steps now, indeed do so.

2.1 PQC Personas

Before embarking on the PQC migration journey, organisations must find out when they should start this journey. To help organisations with this choice and to best address the different needs of organisations when making the PQC migration, we have divided the landscape of organisations into a small number of categories, called PQC personas. Firstly, this allows us to identify which organisations need to take steps towards migration as soon as possible and which organisations can wait a bit longer. Secondly, this allows us to tailor advice to different organisations with similar structure.

We have drafted different concrete action steps for each of the personas, varying in terms of urgency, timeline, risk analysis, attention to be taken and more. We used the following characteristics to make this distinction:

- **Attack surface** | What infrastructure does the organisation provide/have which is prone to attacks aided by a quantum computer?
- **System types** | Which kind of systems are handled and what is the impact of a malfunction of these systems?
- **Data types** | Which kind of data and information is handled in terms of criticality, disclosure sensitivity and the consequences of unauthorised and undetected modification?
- **Time pressure** | How quickly does PQC migration need to take place to ensure safety of data and systems?
- **Dependency on other organisations** | How do different organisations depend on one another?
- **Threat level** | How realistic is it that a malicious actor with a quantum computer will choose to attack this organisation?

The PQC persona can be divided into three main categories

Urgent Adopters | Organisations that handle sensitive data or provide critical or longlived infrastructures. These organisations should start taking first steps on PQC migration as soon as possible. Within this category, we have made a distinction between the different kind of organisations that need to move quickly, depending on why they are at risk of being attacked by a quantum computer.

Regular Adopters | Organisations that do not handle sensitive data and do not provide critical or long-lived infrastructures with a high risk of being attacked. These organisations may, for example, still handle sensitive data, but it is unlikely that data is currently being stored for decryption by a future quantum computer.

Cryptography Experts | Organisations that supply cryptographic standards or infrastructure. The main differences between cryptography experts and urgent adopters are that cryptography experts should have most of the necessary cryptography knowledge for PQC migration in house already, and that they are responsible for cryptographic assets of other organisations as well.

This manual mainly focuses on giving advice and concrete steps to urgent adopters, and hence the main goal of this section is for organisations to determine whether they are an urgent or regular adopter. The following chapters contain extensive advice for urgent adopters, however there will also be advice for the other two categories.

2.1.1 Urgent Adopters

Within the urgent adopters persona, various subpersonas can be drafted out. These subpersonas are not meant as a division of the urgent adopters persona, but can be thought of as examples of urgent adopters. These examples are based on the different risks quantum computers bring to urgent adopters. In general, advice for these subpersonas will be the same, but some action points will be stressed more for certain subpersonas than others. More information on this will follow in the next chapter.

Personal Data Handlers

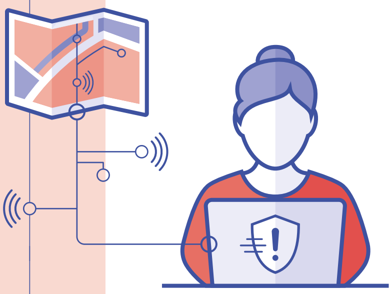
Organisations that handle **personal data with a long confidentiality shelf-life**. These organisations are required by law to protect such personal data. The biggest risk these organisations face are store-now-decrypt-later attacks that are happening either now or soon. Personal data is any information related to an identified or identifiable individual. This includes but is not limited to social security number, telephone number, credit card number, health data, appearance or address. Such data are prone to store-now-decrypt-later attacks if there are other parties for which this data is interesting even in 20 years or more. Thus, even though most organisations handle personal data, this persona focuses on personal data for which a quantum computer already poses a significant threat. For more intuition on how to judge the risks an organisation is facing from attackers, see Section 2.4.1. This means for example that sport clubs, web shops and universities do not fall under this persona. Examples of organisations that do fall under this persona are governments, organisations in healthcare such as hospitals, financial organisations and insurance providers.

It should be noted that there are currently no laws for protecting personal data against quantum computers or the use of PQC to mitigate it. However, if a future quantum computer is used to decrypt data that is currently being stored, it is likely that the owners of this data will still be held accountable.

Organisationally Sensitive Data Handlers

Organisations that handle **organisationally sensitive data with a long confidentiality span**. This entails state secrets, transactions, minutes, trade secrets, and any information that is classified for entities outside of the organisation. The biggest risk these organisations face are store-now-decrypt-later attacks. Such data is prone to store-now-decrypt-later attacks if there are other parties for which this data is interesting even in 20 years or more. Examples of such organisations are the military, national intelligence organisations, governments, financial organisations, knowledge institutes, universities and companies producing sensitive technologies that are of interest to state actors.

The main difference between personal and organisationally sensitive data is that personal data needs to be kept secret to protect the privacy of individuals, while organisationally sensitive data needs to be kept secret from an organisational perspective. A data breach of the first would result in a company breaking laws regarding personal information, while a data breach of the second would likely result in a company losing (some of) its competitive advantage in the market, a loss of knowledge or state security, or a general negative impact on the entire economy.

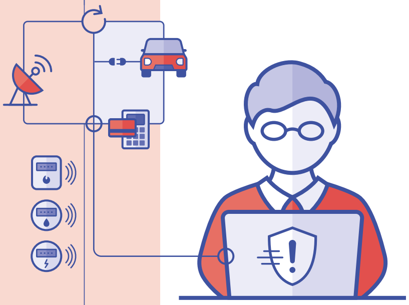


Critical Infrastructure Providers

Organisations that provide **systems that are crucial for the functioning of large groups of people**, such as towns, cities, provinces or even countries. There are a variety of such systems, but most of these are concerned with providing large groups of people with basic needs, such as water, electricity, transport, communication and healthcare. A malfunction of these systems can have different results with different degrees of impact. Usually, malfunctioning results in many people having their daily lives seriously disrupted, but in some cases it might even result in serious damage, injury or even death.

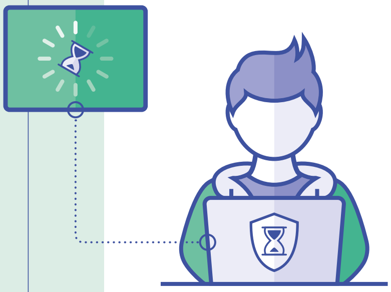
There are many examples of cyber attacks on critical infrastructure, one of the most notable being the Triton malware attack on Saudi petrochemical plant, designed to cause loss of life. To read more about this and other examples, please look at [Wei21].

The difference with the first two personas is twofold. On the one hand is availability of much greater importance than integrity and reliability for these organisations. On the other hand is the risk appetite much lower, as malfunctioning usually has a major impact. The migration process might look different. Examples of critical infrastructure providers are energy or water providers, transport organisations such as train companies or airports, communication companies such as telecom providers, web browsers and healthcare providers such as hospitals.



Long-lived Infrastructure Providers

Organisations that **provide systems which are built to have a long life-span**, because they are otherwise not profitable. The main risk these organisations face is that the systems which are produced over the next decade will probably still be in use once quantum computers become available. Hence these systems should have the ability to be swiftly updated to quantum-safe standards. Post-quantum cryptography usually has different (usually heavier) hardware requirements than current cryptography, because of which the production of systems with a life-span of more than 20 years should already take these hardware requirements into account. Examples are satellites, payment terminals, cars, telecommunication networks, energy providers, smart meters, smart industry (4.0) and sensor networks.

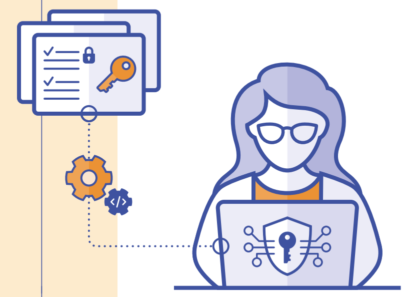


2.1.2 Regular Adopters

Any organisation that does not identify as any of the urgent adopter personas. These organisations possibly handle data or provide systems, but the kind of data is not currently prone to store-now-decrypt-later and the kind of systems are not critical or long-lived. Note that in later stages these organisations may be prone to attacks using a quantum computer, but for these organisations it is more beneficial to await further PQC standards and / or the availability of production-ready implementations of PQC algorithms and services based on PQC solutions, as early migration also comes with extra risk, as mentioned before. There are, however, steps these organisations can already take now and they should also remain mindful about possible changes in advice or their own persona(s). More information on this can be found in the next chapter. Most organisations will be regular adopters, some examples being retailers, schools and sport clubs.

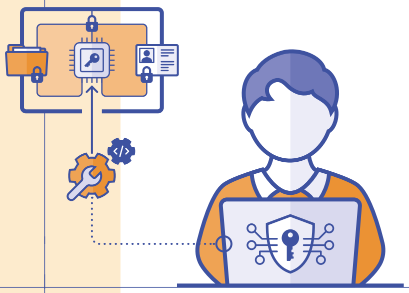
2.1.3 Cryptography Experts

Although the aim of this work is not to give concrete advice to these sorts of organisations, as they should have all the necessary knowledge themselves, we do mention them for a couple of reasons.
Firstly, it is important for our main audience of urgent adopters to know that this group exists and what to expect from them. Most urgent adopters have cryptography experts as vendors of their cryptography. Urgent adopters who want to start migrating to PQC should be able to ask these vendors whether their products are quantum-safe and if not, when they expect their products to be quantum-safe. In some cases these urgent adopters may have to choose to switch to a different vendor for their cryptographic assets.
Secondly, the above brings concrete advice to the cryptography experts. They should be ready to expect questions from their customers related to PQC, such as timelines to achieve PQC in their products and which algorithms they are planning to implement. Because of this, they should start migrating their products to PQC standards as soon as possible as well.



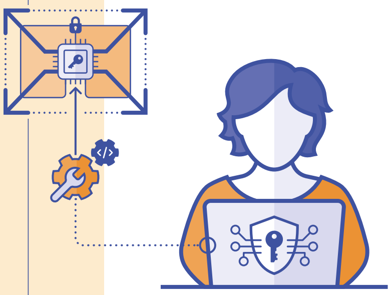
Standard Developing Organisations

Organisations that define **cryptographic standards and/or protocols**. These are standards and protocols that are standardised for a wide variety of applications, using cryptography in some way. Most of these standards are used for either communication or security, such as safe communication, safe data storage, protection of systems or TLS. These organisations almost always operate at a national or international level because of the importance of interoperability between regions and nations. Examples are NIST, ETSI, IETF, TLS, IEEE, ISO/IEC, TCG, ANSI, W3C and ENISA.



Cryptographic Infrastructure Providers

Organisations that develop, implement or service **cryptographic infrastructure for other companies to use**. These organisations usually operate at a national or international level. Examples are management security providers and developers of cryptographic libraries.



Providers of Cryptography Beyond Secure Communication

Organisations that develop, implement or service **infrastructure based on cryptographic protocols that are used for purposes beyond secure communication**. Note that this sort of cryptography does not necessarily give higher security guarantees. The difference lies in the fact that the cryptographic protocols developed by these organisations are used for different purposes and may be based on different principles. Examples of such protocols are blockchain, Zero-Knowledge Proofs, Multi-Party Computation and Idemix. This persona is mentioned separately as the sort of cryptography developed can be so significantly different, that different measures have to be taken by these organisations than by organisations which develop more standard cryptographic functionalities. As these forms of cryptography are relatively young in practice, most organisations of this persona are currently start-ups that use one of the mentioned techniques for specific use cases.

2.1.4 Determining Personas

In this section, guidance on how an organisation can determine their persona(s) is given.

Levels of Cryptography

Generally speaking, there are three levels of cryptography that an organisation is responsible for, namely: 1) their own cryptographic infrastructure; 2) their cryptographic knowledge; 3) the cryptographic infrastructure related to the supplying of services or products to other organisations.

Each of these three have to be taken into account when migrating to PQC and hence influence what kind of persona an organisation is. Level 3 is treated separately as by supplying to other organisations, attacks on this supplying organisation can work through to these supplied organisations via so-called supply-chain attacks. A supply-chain is a chain of organisations where each organisation supplies to the next organisation in the chain. An example of certain organisations forming a supply-chain can be found in Figure 2.1.

In this diagram, the arrows indicate that organisations supply to one another (e.g., the Software Supplier supplies to the recruitment agency and the telecom provider). Attacks on organisations higher on the supply-chain can also pose a risk to organisations further down the supply-chain.

An example of a supply chain attack is the SolarWinds hack in 2020. In this attack, hackers inserted a malicious piece of code into one of the products offered by software company SolarWinds. After this insertion, SolarWinds (unknowingly) shipped this as an update to thousands of organisations including major multinationals and the US government, whose data, networks and systems could then be accessed by the hackers. Examples of suppliers are IT/software vendors such as Microsoft and IBM, Cloud providers and anti-virus/IDS vendors.

Determining Personas

When determining their persona, an organisation has to take into account all three of the levels of cryptography mentioned above. Firstly, it should consider its own infrastructure to come up with one (or more) suitable persona(s). Secondly, an organisation may identify as certain personas because of the cryptographic knowledge it possesses. This results in a cryptography experts persona. Lastly, an organisation inherits the same persona as all the organisations it supplies to, because it has to follow the same advice as the organisations it is supplying to. Otherwise, it poses too high a risk to the organisations it supplies to. This inheriting of personas continues even further down the supply-chain, meaning that an organisation inherits all the personas of organisations that are below it in the supply-chain. As an example, this means that in Figure 2.1, the recruitment agency is both an organisationally sensitive as personal data handler, the software solution provider is also a long-lived infrastructure provider, and Microsoft is both a organisationally Sensitive data Handler, personal data handler as well as critical infrastructure provider.

Taking all these personas together, each organisation should be able to identify itself as an urgent or regular adopter and potentially also a cryptography expert. If an organisation is an urgent adopter, it might identify as more than one of the subpersonas.

Additionally, it should be noted that the persona(s) of an organisation may change over time, because the risks it faces over time may change. We advise to carefully reassess which persona the organisation identifies as each time the organisation starts taking new steps in PQC migration. We also emphasize that some organisations may think they are regular adopters, while they are an urgent adopter in practice because of either their own cryptographic infrastructure or the infrastructure of one of the organisations it supplies to. Because of this, we advise organisations to be conservative in determining their PQC persona. If an organisation is on the boundary of being an urgent or regular adopter, it is advised to follow the advice in Section 3.2, as this section will give further guidelines on when they should start migrating certain assets.

The best way to find out which persona(s) suit(s) an organisation or the organisations they supply to is to read the descriptions of all the personas above and see which description(s) apply to the relevant organisations. In addition, the flowchart in Figure 2.2 aims to give a visual aid for determining their PQC persona(s).

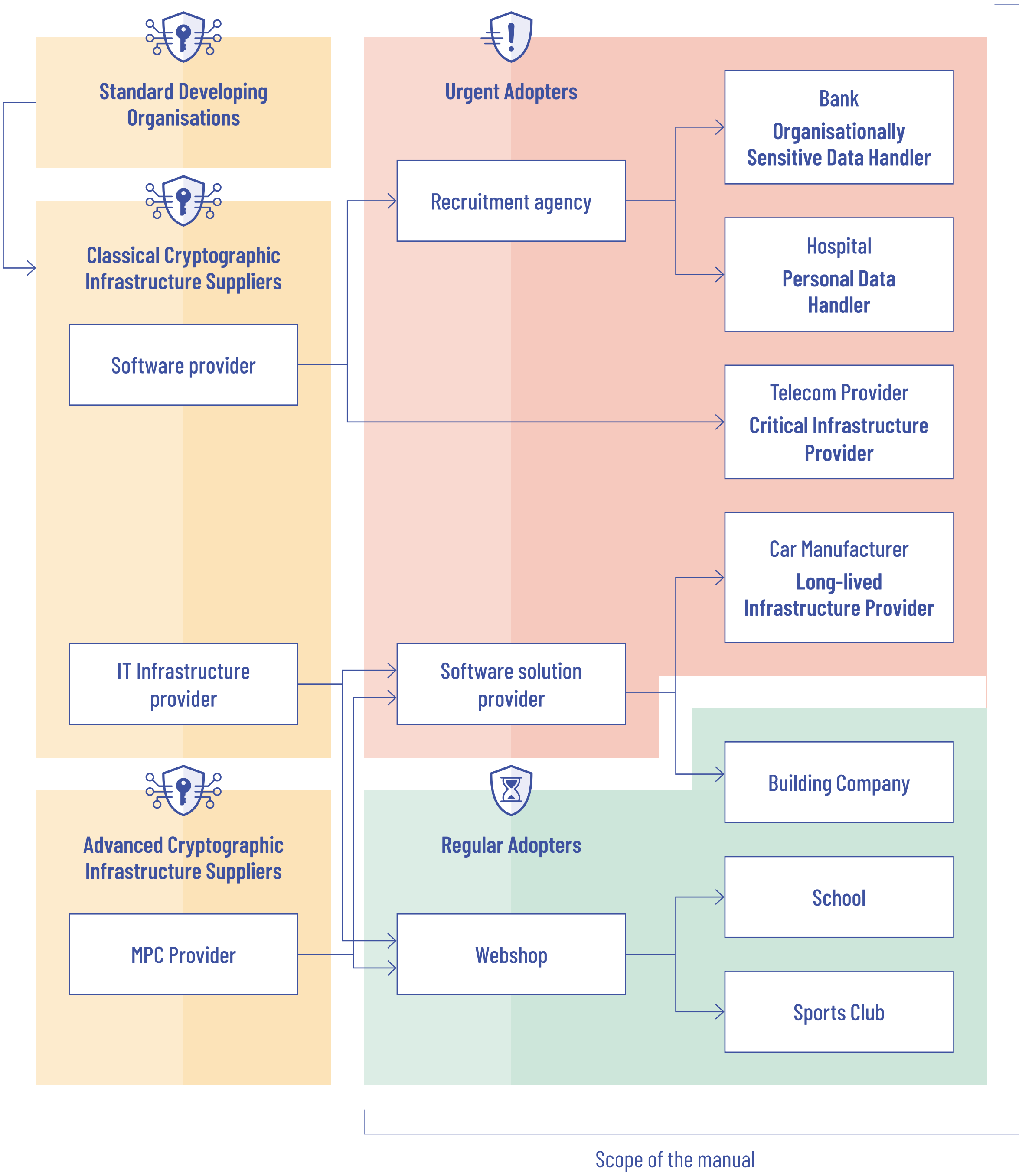

Standard Developing Organisations
Classical Cryptographic Infrastructure Suppliers
Software provider
IT Infrastructure provider
Advanced Cryptographic Infrastructure Suppliers
MPC Provider
Urgent Adopters
Recruitment agency
Software solution provider
Bank
Organisationally Sensitive Data Handler
Hospital
Personal Data Handler
Telecom Provider
Critical Infrastructure Provider
Car Manufacturer
Long-lived Infrastructure Provider
Building Company
Regular Adopters
Webshop
School
Sports Club
Scope of the manual

Figure 2.1 | Visual example of organisations with their PQC Personas.

Advice for Organisations That Have Multiple Personas

As mentioned above, some urgent adopter personas may identify themselves as multiple of the urgent adopters personas. For instance, financial institutions are both personal data handlers and organisationally sensitive data handlers. Although this does not change the advice mentioned in the next section, the different subpersonas do give an indication which action steps should receive more focus. The first action steps (the one in Conducting the Quantum-vulnerability diagnosis, see next section) are the same for the different subpersonas. For the later steps, the diagnosis should make it clear which cryptographic asset falls most under which persona and hence which action steps should receive most focus for this asset.

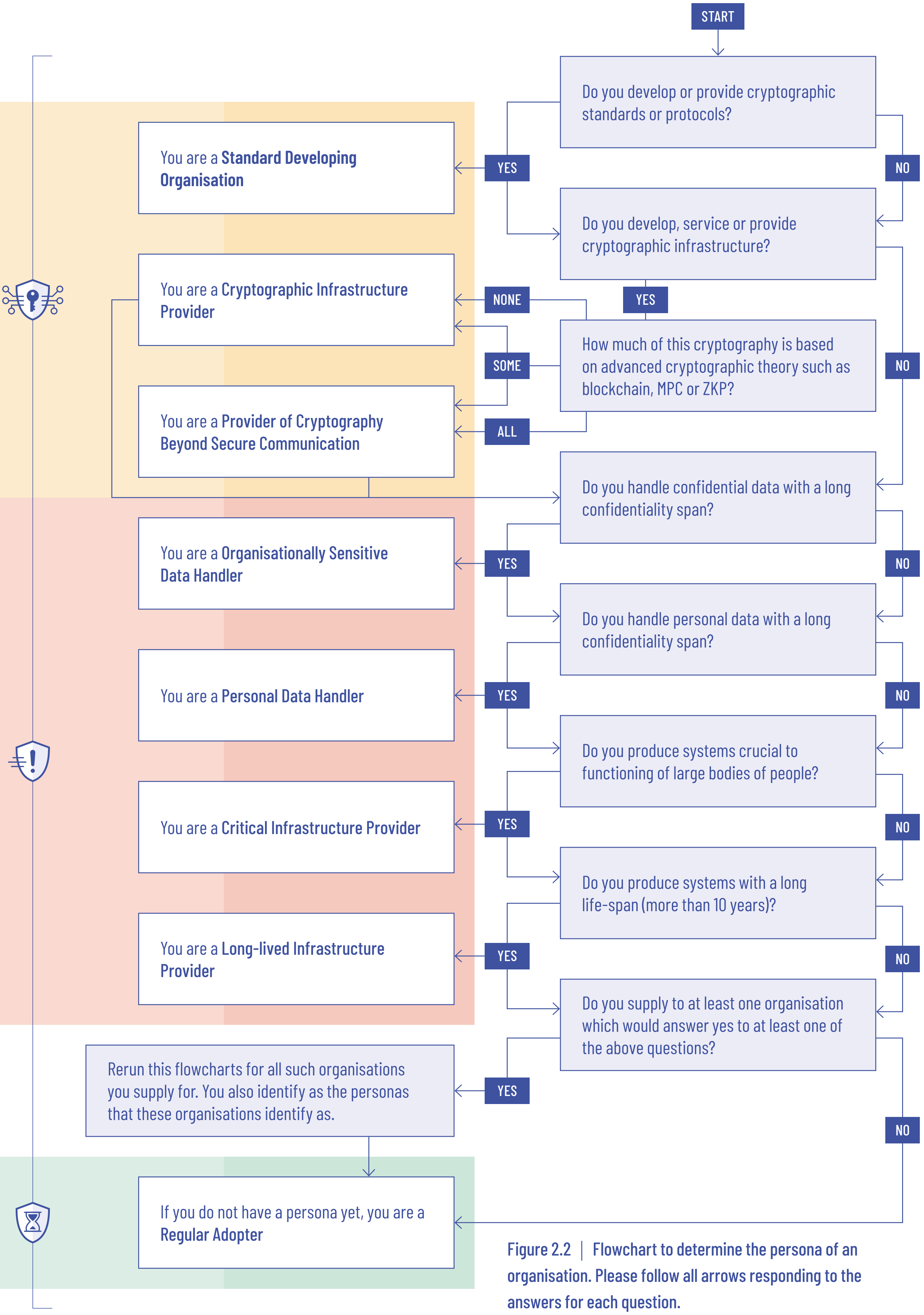

START
Do you develop or provide cryptographic standards or protocols?
YES
You are a Standard Developing Organisation
NO
Do you develop, service or provide cryptographic infrastructure?
YES
NO
How much of this cryptography is based on advanced cryptographic theory such as blockchain, MPC or ZKP?
NONE
You are a Cryptographic Infrastructure Provider
SOME
ALL
You are a Provider of Cryptography Beyond Secure Communication
Do you handle confidential data with a long confidentiality span?
YES
You are a Organisationally Sensitive Data Handler
NO
Do you handle personal data with a long confidentiality span?
YES
You are a Personal Data Handler
NO
Do you produce systems crucial to functioning of large bodies of people?
YES
You are a Critical Infrastructure Provider
NO
Do you produce systems with a long life-span (more than 10 years)?
YES
You are a Long-lived Infrastructure Provider
NO
Do you supply to at least one organisation which would answer yes to at least one of the above questions?
YES
Rerun this flowcharts for all such organisations you supply for. You also identify as the personas that these organisations identify as.
NO
If you do not have a persona yet, you are a Regular Adopter

Figure 2.2 | Flowchart to determine the persona of an organisation. Please follow all arrows responding to the answers for each question.

Interoperability During PQC Migration

PQC migration is often not a process that can be executed by individual organisations because of dependencies between different organisations. This dependency can happen both at an organisational as well as a technical level. In order to maintain interoperability between different organisations, coordination between these organisations during PQC migration is required.

This can happen in a variety of ways. If an organisation A depends directly on an organisation B, organisation B needs to migrate to PQC standards before organisation A can do so. Oftentimes such dependencies between organisation are not so linear but happen in the form of a certain network structure. If this is the case, all the organisations involved in this network structure should coordinate their PQC migration to ensure both interoperability as well as security of their data and systems. If this is the case, organisations should take into account all the PQC personas of the respective organisations when performing PQC migration.

2.2) Quantum-Vulnerability Diagnosis

Now that an organisation identifies as a persona, they can determine if they should proceed with the migration, starting with performing the Quantum-vulnerability diagnosis.

Urgent Adopters

Organisations identified as urgent adopters should start their Quantum-vulnerability diagnosis as soon as possible to ensure migration happens as soon as possible. The rest of this document is mainly intended to guide such organisations through the migration process.

Regular Adopters

Organisations identified as regular adopters do not need to react to the quantum threat yet. However, these organisations should make sure that they are in the best condition to migrate later. The following recommendations apply.

First, these organisations should make sure they are up-to-date with the latest security guidelines (for instance migrate from TLS 1.2 to TLS 1.3) and favour crypto-agile solutions. For more information about crypto-agility, please see Section 4.4. They can also anticipate the fact that future updates will have an impact on the performance of cryptographic algorithms. These organisations can also start doing the risk-assessment and diagnosis steps of the migration plan described in Section 2.2.1.

Second, these organisations should stay well-informed and follow the standardisation efforts. A couple of years after the publication of the post-quantum standards, new recommendations specifically dedicated to these organisations are expected to be announced, taking into account the developments and lessons learnt from early adopters.

Finally, some organisations identified as regular adopters may want to act proactively and go further in applying the migration plan described in this manual, in particular starting with the Quantum-vulnerability diagnosis. There are various reasons for doing this, some of which are: the organisation is about to make large infrastructure investments; the organisation changes its activity or the organisation has new clients, which changes the risk assessment. Either way, these steps will have to be taken at some point, so it will never hurt to initiate the first migration steps now.

Cryptography Experts

Organisations identified as cryptography experts should also start applying the migration recommendations to their own infrastructure. Moreover, as suppliers of cryptographic assets, all other actors of the supply-chain rely on them. Therefore, they should be ready to start implementing quantum-safe algorithms as soon as the standards are available.

In order to facilitate planning the migration for organisations they are supplying to, cryptography experts should communicate clearly to their clients. For each of their products, they should state whether it resists quantum attacks. If it is not the case, they should propose quantum-safe alternative solutions. They should provide clear timelines for when they intend to offer such solutions.

Concerning Providers of Cryptography Beyond Secure Communication, we highlight that some widely used advanced cryptographic protocols are not quantum-safe.

2.2.1 Conducting the Quantum-Vulnerability Diagnosis

Having decided to start PQC migration, the first step consists of making a diagnosis of the current situation of an organisation with respect to cybersecurity. This step aims at gathering the necessary data to decide which assets should be migrated first, identify the dependencies and anticipate the consequences of the migration. Note that organisations do not necessarily have to gather the information in a particular order. Typically, multiple typesofinformation gatheringor assessments can and should be performed in parallel. For example, an organisation might decide to conduct apartial risk assessment first, and focus the initial inventory only on the high-risk components of their organisation.

In general, knowing the following information is a prerequisite to the establishment of a suitable migration plan in the next chapter:

- Inventory of all cryptographic assets used in the organisation;
- Inventory of all the data handled by the organisation;
- Inventory of the suppliers of cryptographic assets;
- Risk assessment.

Inventory of Cryptographic Assets

In order to conduct the migration, it is necessary to identify all the cryptographic assets within an organisation, including assets that will soon enter the organisation. Guidance on how to build a cryptographic inventory can be found in Section 2.3. This is an important step to make sure that all assets are correctly migrated. If one algorithm remains that is vulnerable to a quantum attack, this could serve as en entry point for a larger attack on the entire system.

Therefore, an organisation should aim to obtain an exhaustive list of all uses of cryptography, both software and hardware. The information collected should be as detailed as possible, including the algorithm, key length, usage, etc. It will be used to determine whether a cryptographic asset is vulnerable to quantum attacks and which quantum-safe solution could be used instead. For assets that are not controlled by the organisation itself, the suppliers shouldbe identified. This inventory could take the form of a Configuration Management Database (CMDB). Past cryptographic migrations have shown that creating an inventory of cryptographic assets is the most important and most difficult part of the diagnosis. Organisations should take into account that this step will take a significant amount of time.

In addition, one should consider that such an inventory is useful outside the scope of this migration project. Indeed, having a full picture of the exact cryptographic algorithms deployed can help identify vulnerabilities

in the current system. Such vulnerabilities are far from uncommon and need to be fixed. Hence, a good inventory of all cryptography at use will ease the mitigation of both quantum and non-quantum threats.
Furthermore, maintaining a cryptographic inventory can be made part of a more general cryptographic policy. A cryptographic inventory can help in identifying non-compliant cryptography usage.
It should be noted that due to the continuously changing nature of cryptographic landscapes, this inventory should be continuously updated as well. In addition, it should be noted that such an overview is very sensitive as it contains vulnerabilities of an organisation. It is hence of utmost importance that it is properly secured and cannot be accessed by unauthorised parties.

Inventory of Data Assets

In order to plan a migration, a list of the data assets handled by an organisation will help you make good decisions. More precisely, an exhaustive list of the data is not necessary, but rather a list of types of data, depending on several factors:

- Kind of data (data at rest, data in transit or data in use);
- Location of the data;
- Value of the data (confidentiality, availability);
- Classification of data;
- Risk assessment for each data asset.

Inventory of Cryptographic Dependencies

For most organisations, a significant part of the cryptographic assets (hardware and software) are provided by external suppliers. Therefore, a large part of the migration consists of making sure that suppliers are migrating and offering new quantum-safe solutions, or finding new suppliers otherwise. The goal of this inventory is to identify the cryptography supply-chain. Note that it is expected that vendors will not always be explicit about their (lack of) support for PQC.
For each supplier, it is recommended to list all the products that are supplied, whether there are ongoing contracts with them, and how to contact them. This list should also include certificate authorities. Besides the official suppliers of cryptographic assets, an organisation should also consider internal communication tools (instant messaging, collaborative platforms) as well as shadow IT.
The organisations that are being supplied to will be making a similar assessment of their dependencies and might require their supplier to properly communicate your intentions with respect to PQC. For the supplying organisation, it is not necessary to make an exhaustive list of all clients but keep this in mind when deciding on an appropriate strategy.

Risk Assessment

Each organisation regularly assesses the risk of its IT infrastructure being subject to attacks and the potential consequences (financial, reputational, legal, etc.). Guidance on how to perform a quantum risk assessment can be found in Section 2.4. The risk is assessed depending on several parameters the value of the information, the vulnerability and the threat.
The first phase of the risk assessment consists of reassessing the risk of the current IT infrastructure in a new scenario where an adversary has access to a large scale quantum computer. The quantum threat does not affect the value of the information the valuable assets remain the same. However, it creates new vulnerabilities; some information that was protected by cryptographic algorithms considered secure against non-quantum enhanced attackers is not protected against quantum attackers. Moreover, one should anticipate new threats attackers targeting the new vulnerabilities created by this situation. Hence, the risk should be reassessed accordingly. A proper risk assessment will be vital to decide which systems should be migrated first.

2.3) Cryptographic Asset Management

Creating an inventory of cryptographic assets is fundamental for a successful diagnosis and planning for any organisation to migrate to post-quantum cryptography. Asset management is an integral part of the life-cycle management of software, hardware, services, and artefactst. In particular, maintaining cryptographic assets is important for risk management, vulnerability response and compliance.
The importance of building a cryptographic inventory as the first step into establishing quantum-readiness is also recognised by European [BSI22] and American entries [CISA23; NIST21] as well as international organisations for standardisation [ETSI20c; PCI22; GSMA24].

2.3.1 Cryptographic Policies

Before embarking on cryptographic discovery, it is essential to identify and understand the organisation's cryptographic policies. This preparatory step ensures that cryptographic efforts are aligned with legal requirements and organisational security goals and defines the roles and responsibilities related to cryptographic tasks. Cryptographic policies guide in:

- Establishing procedures for key generation, distribution, storage, rotation, and destruction;
- Defining cryptographic key life-cycle;
- Defining algorithms and parameters for data encryption and data integrity;
- Providing mechanisms for ensuring authentication and authorisation;
- Providing guidelines for preventing unauthorised data modification;
- Permitting and prohibiting specific protocols and protocol versions;
- Specifying road-maps and deadlines for cryptographic migrations;
- Other related topics.

Understanding what is needed to comply with is another critical aspect. Different industries and regions have specific regulations and standards regarding data protection. These standards act as the guiding principles for how cryptography is implemented and managed within an organisation. For instance, financial institutions might need to adhere to the Payment Card Industry Data Security Standard (PCI DSS) [PCI22], while healthcare providers must comply with the Health Insurance Portability and Accountability Act (HIPAA) [US96]. Organisations across various sectors that handle sensitive information, especially those involved in IT technology, finance, healthcare, and software development, often comply with the ISO-27001 standard [ISO22a]. Additionally, the General Data Protection Regulation (GDPR) [EU16b] emphasizes the use of cryptography to reduce risks, particularly in the context of data breaches, and mandates appropriate technical and organisational measures to ensure the security of processing systems and services, including the use of cryptography for pseudonymisation and anonymisation. Lastly, the NIS2 Directive [EU22a] requires entities to implement robust cryptographic measures to protect confidentiality, integrity and availability of data.
Identifying cryptographic policies is a strategic approach for creating a cryptographic inventory. First, it helps to prioritise assets by clearly defining what needs protection and the level of protection required. Secondly, understanding these policies gives insights about where the assets are used and aids you in locating them more efficiently. Knowing the specific areas and contexts in which cryptographic measures are necessary allows for a targeted and efficient discovery process, saving time and resources. Additionally, it can be useful to identify adjacent topics relating to cryptography such as data classification, ICT risk management, third party risk management and incident response.
These two aspects will support in coming up with a plan for the next step defining a strategy for cryptographic discovery.

2.3.2 Establishment of a Strategy for Cryptographic Discovery

Once cryptographic policies are identified and understood, the next step is to define a strategy for cryptographic discovery. This strategy serves as a structured approach to identifying, evaluating, and documenting cryptographic assets within an organisation. Defining such strategy can be done in several steps, however it might be necessary to adapt them to specific organisations:

1. **Defining Objective** | Establish the purpose of performing the discovery of cryptographic assets. This might include goals such as ensuring compliance, performing maintenance, updating cryptographic measures;
2. **Defining Scope** | Determine the types of assets that need to be retrieved and what to prioritise. This could include keys, meta-data of cryptographic algorithms certificates, depending on their criticality and on what is pertinent to the organisational needs;
3. **Defining Discovery Methodology** | Identify the tools and techniques to deploy for discovery. This involves selecting appropriate tools, determining the systems to be investigated, and dividing tasks among team members;
4. **Defining Data Analysis** | Specify the type of information required for each asset type and the level of detail needed. This can include metrics for evaluating the effectiveness, compliance, and risks associated with each cryptographic asset;
5. **Reporting** | Establish how the collected data should be inventoried and analysed. Define the format and structure for reporting findings, ensuring that the information is presented in a clear and actionable manner;
6. **Reviewing** | Determine how and how often the inventory should be reviewed and updated. This ensures that the cryptographic inventory remains current and relevant, addressing any changes in assets and policies over time.

After defining a strategy, the process of performing the discovery of cryptographic assets in their systems can begin.

2.3.3 Execution of Cryptographic Asset Discovery

To ensure comprehensive cryptographic asset discovery, it is crucial to locate all services that rely on the principles of confidentiality, integrity, authenticity, and non-repudiation (see Section 1.4). These services include instant messaging, cloud storage, virtual conferences, secure file transfer, digital seals and signatures on legally binding contracts, bank transactions, access control through smart cards (physical) or tokens in VPN (digital), authentication mechanisms like password login and two-factor authentication, email communication, electronic voting, IoT management, OS booting, software updates and digital right management.

A prominent initiative concerning the study of discovering cryptographic assets, creating and managing a cryptographic inventory, is being carried out by the National Cybersecurity Center of Excellence (NCCoE), which has released the special publication [NCCoE23] as one of the outputs of the Migration to Post-quantum Cryptography project.

In this publication they investigate the process of discovering cryptographic assets while trying to identify the challenges and possible solutions.

The report identifies three main scenarios in which cryptographic assets are used and should be detected to obtain a complete inventory:

- Software development;
- Operational systems and applications;
- Network traffic.

Software Development | Cryptographic software libraries facilitate software developers in the creation and management of a wide scope of cryptographic components. This ranges from creating and using cryptographic keys to running encryption and signing algorithms, to managing password credentials and tokens. Typical examples of cryptographic libraries used in software developments are OpenSSL [OpenSSL03], Bouncy Castle [BC24a], Libsodium [Libsodium13], Crypto++ [Dai23], wolfCrypt [Wol24b].

In software development, the investigation is performed by inspecting which cryptographic library is required as well as what cryptographic functionalities are imported and used in the development. Although identification and discovery of cryptographic operations and/or cryptographic materials (such as keys, tokens and credentials), can be implemented manually in code development (e.g., in code-reviewing) this process is prone to error. It is desirable to integrate static and/or dynamic analysis tools in the Software Development Life Cycle in the development environment and/or in the continious integration/continuous deployment (CI/CD) pipeline to automate this process.

Operational Systems and Applications | Operational systems are constantly used to perform daily tasks within an organisation, like VPN connections, two-factor authentication (2FA), login via credentials, encryption and decryption of data at rest (for example data populating databases) and secure booting and updating of operating systems.

These services are enabled by using executable and non-executable cryptographic assets. Executable assets include cryptographic software, firmware, hardware and libraries. Even if an organisation is not actively developing with cryptographic libraries, executable cryptographic assets are necessary to support in their activities. An example is the OpenSSL library which is included in most Linux distributions and supported, among others, in CISCO AnyConnect which is commonly used in VPN connections for remote working.

Non-executable assets are cryptographic data that are either at rest and accessed via secure protocols like 2FA, or used or generated by the executable assets. Examples include personal access tokens, OpenPGP keys, key-stores and X.509 digital certificates.

Network Traffic | Naturally, it is possible to identify which IT component is using cryptography by monitoring network traffic. In fact, it is possible to use a network scanning tool to detect what type of cryptographic algorithms and security measures are negotiated and employed. Communication can occur on-premise, in the cloud, or over untrusted networks with entities outside the enterprise.

Every layer of the ISO-OSI stack for internet communication is protected by a secure protocol, therefore, it is essential to thoroughly investigate all of them. Table 2.1 provides an overview of example secure protocols for every layer of the OSI stack.

Level	Layer	Application	Secure Protocols
7	Application	PKI, Web of Trust, Email, Web Browsing	PGP, S/MIME, SSH, X.509
6	Presentation	PKI	SSH, TLS, X.509
5	Session	PKI, FTP, Password Authentication	PAP, SMB, SSH, X509
4	Transport	TCP, UDP	QUIC
3	Network	IP Routing, VPN	IPSec
2	Data Link	Wi-Fi, Ethernet	WPA3, MACsec
1	Physical	Cable, Wave	

Table 2.1 | Secure protocols used over the OSI stack for network communications.

Some security protocols operate on more than one level of the OSI stack. This does depend on the different applications these protocols are used for and the sometimes unclear distinction between layers 5, 6 and 7. For example, digital certificates in X.509 format are used to set up a HTTPS connection in TLS, which operates on level 6, but they can also be used for email or document signing and verification. For a more in depth overview of the most used protocols, you can consult Section 4.3.

It is important that an appropriate tool is utilised to examine all relevant OSI layers of network communication and that the use of scanner is allowed in the systems.

An example on how to investigate network traffic is by using different open-source port scanners like *nmap* [Lyo24] and *testssl.sh* [Wet24] and networks scanners like *Wireshark* [Wir24] and *tcpdump* [Gro24] to scan TLS traffic. These tools can help create an overview of the network and identify where cryptography is used. Subsequently, combining this network analysis with agent-based detection allows for a more precise and complete investigation.

As part of the cryptographic asset discovery process, inventory of the found assets is a crucial step for maintaining a clear and complete overview.

2.3.4 Cryptographic Inventory Format Cryptographic Bill of Materials

There are several ways to build and manage a cryptographic inventory, and the way it is created and managed should benefit an organisation and their use case. However, using a standard format for a cryptographic inventory is desirable because it provides a more streamlined way of creating, managing and analysing an inventory; for example, it can be easily managed not only by the organisation itself, but by their suppliers and their clients as well. This feature adds transparency and prevents interoperability issues between user and supplier.

The Cryptographic Bill of Materials (CBOMs) is a machine-readable standard format that is based on the already existing CycloneDX Software Bill of Materials (SBOMs) [Cyc24] for the security of supply chains and life-management of software assets. CBOMs aim at both capturing the cryptography used, including metadata on this usage, and to track dependency between cryptographic algorithms, while also providing a means to couple a classical and quantum security vulnerability score to the found assets. They have been developed by IBM with the goal of creating an inventory specialised in cryptographic assets and as of April, 2024 CBOMs are fully supported in version 1.6 of the CycloneDX SBOMs [OWA24].

A CBOM can accommodate a very detailed and thorough cryptographic inventory listing any type of cryptographic asset secure protocols, cryptographic algorithms, cryptographic keys, cryptographic materials like ciphertexts, signatures, digests, initialization vectors, tokens, nonces, and artefacts like digital certificates, credentials, passwords and more.

Table 2.2 provides some examples of the type of information available for different cryptographic assets.

Asset	Example	Data
Protocol	TLSv1.2	version, ciphersuite
Algorithm	AES-128-GCM, SHA512withRSA	type of primitive (signature, encryption), parameters, mode of operation, execution environment (CPU architecture), NIST security levels, functionalities
Key	RSA-2048 pub-key	type of key (e.g., public/private), size, lifetime, status (e.g., active, compromised), type of storage (SW, HW)
Certificate	X.509 certificate	subject, issuer, validity, format, extension, public key, signature

Table 2.2 | Type of Data reported in CBOMs.

```
...
   {
         "type" "crypto-asset",
         "bom-ref" "oid1.3.18.0.2.32.104",
         "name" "tlsv12",
         "cryptoProperties" {
               "assetType" "protocol",
               "protocolProperties" {
                     "tlsCipherSuites"  [
                           "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519)",
                           "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519)",
                           "TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)",
                           "TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)"
                     ]
               }
         }
   }
...
   {
         "type" "crypto-asset",
         "bom-ref" "oid2.16.840.1.101.3.4.1.6",
         "name" "AES",
         "cryptoProperties" {
               "assetType" "algorithm",
               "algorithmProperties" {
                     "variant" "AES-128-GCM",
                     "primitive" "ae",
                     "mode" "gcm",
                     "implementationLevel" "softwarePlainRam",
                     "implementationPlatform" "x86_64",
                     "certificationLevel" "none",
                     "cryptoFunctions" ["keygen", "encrypt", "decrypt", "tag"]
               },
               "classicalSecurityLevel" 128,
               "nistQuantumSecurityLevel" 1
         }
   }
...
```

Figure 2.3 | Example of a CBOM.

A snippet of a CBOM constructed from the web server *nginx* and provided by IBM [IBM24] is shown in Figure 2.3. In this example, the protocol TLS v1.2 and the cryptographic primitive AES-128-GCM are listed as cryptographic assets of nginx.

Additionally, CBOMs are structured so that they allow to track dependencies of cryptographic components. Following from the previous example, the CBOM reports that TLS v1.2 and AES-128-GCM have been detected; Figure 2.4 shows how these assets depend on the others.

Several detailed examples on how a CBOM should be structured can be found in the official authoritative guide [OWA24].

However, it is important to note that while the CBOM format can store this information, it does not guarantee that all this data will be delivered by scanning tools that produce CBOMs. These tools often face challenges in mapping all dependencies and identifying specific elements such as IVs, nonces, and passwords. Another notable limitation of CBOMs is that they do not capture procedures concerning key management (e.g., how a key is generated, loaded, stored) and the existing fields focus more on cryptographic assets discovered in software and less in network traffic.

```
...
  {
       "ref" "TLS v1.2",
       "dependsOn" [
            "libcrypto.so"
       ],
       "dependencyType" "uses"
  },
  {
       "ref" "libcrypto.so",
       "dependsOn" [
            "AES-128-GCM",
            "SHA256", "
            HMAC-DRBG"
       ],
       "dependencyType" "uses"
  },
...
```

Figure 2.4 | Dependencies reported in a CBOM.

2.3.5 Tools for Creating a Cryptographic Inventory

Asset discovery, inventory analysis, and remediation of possible threats are three essential aspects for tools dealing with cryptographic assets. Discovery helps identifying all cryptographic assets ensuring that no weak algorithms and vulnerabilities are overlooked. The subsequent inventory analysis phase involves assessing these elements for weaknesses, compliance with current standards, and potential risks. Remediation addresses identified issues, fortifying the system against potential attacks. Note that to ensure optimal life-cycle management of assets, discovery, analysis and remediation steps are part of a continuous cycle where regular re-evaluation and updates are necessary to mitigate potential threats in a timely manner.

Keep in mind that the best effect will be achieved when using automatic tools for cryptographic discovery along with manual effort it is imperative to perform sanity checks on the output of the tools and to see if the output of such tools is in line with the strategy defined for the discovery process. Besides, tools cannot provide insights on all the security measures in place for data storage or key generation. For example, if a cryptographic inventory does not provide process information about key management then an expired cryptographic key might still be active and deployed. Even though the protocol in which this key is used is still considered secure, in practice the key's extended use increases the risk of compromise. Another example for tool limitation is the analysis of isolated systems like Hardware Security Modules (HSMs) or Trusted Execution Environments (TEEs) where no scanning is possible. Additionally, these tools cannot establish a connection between different cryptographic elements: for example the link between a digital certificate and the keypair associated with it.

It is not only important to use tools that create a cryptographic inventory, but it is equally important to manage an inventory so that action can be taken. To this end, tools that can digest such an inventory and keep it updated should be available. Once an informed view of the cryptographic assets is established, the necessary actions can be determined.

It is also important to note that the process of reporting cannot be fully automated. While tools can assist in creating and maintaining the cryptographic inventory by providing the necessary data and initial analysis, manual effort is essential to interpret the reports, understand the context, and decide on the appropriate actions.

There are several open-source and proprietary tools available to help getting started with cryptographic asset discovery. An incomplete overview of the tools used to carry out the NCCoE investigation is provided by the participants in the previously mentioned NCCoE publication [NCCoE23].

Integration of CBOMs

A notable example of integration of CBOM into open-source services can be found in Github In December 2023, Github announced that CodeQL can be leveraged to create CBOMs [Cha23]. CodeQL is a static code analysis engine that analyses code hosted on Github for security vulnerabilities. Static analysis tools are used to scan source code without executing it. Such tools are used in code development to monitor code quality and to locate possible security issues. CodeQL can beused to find cryptographic assets in software. For each cryptographic asset that CodeQL finds, it reports its exact location in the source code.
An open-source tool to convert the output of CodeQL to a valid CBOM, named CryptoBOM-forge can be found at [Res24].

2.4) Quantum Risk Assessment

After an organisation has a solid understanding of the cryptography that they are using in their (most important) systems, an essential next step is to assess the risk of quantum computers towards these systems. In this chapter, concrete guidance on how to perform a quantum risk *assessment* is presented. This chapter helps in quantifying the risks of different systems and prioritising which systems need to have migrated first. Note that the methodology is specifically meant for risks towards cryptography; other potential risks for organisations introduced by quantum computers are out of scope. This chapter is largely based on the content of the publication "Quantum Risico Methodologie voor Cryptografie" (EN Quantum Risk Methodology for Cryptography) by TNO in 2024 [dVBDvV24].
In this section, we assume that a cryptographic inventory has already been made, or that the information about the cryptographic algorithms necessary for performing this risk assessment can be obtained easily.
Concretely, the quantum risk consists of three components:

- The **quantum weakness** of the cryptography that is in use on a system/application level. This is judged based on the strenght of the known quantum attacks;
- The expected **impact** of a quantum attack on the system. This is based on insight into the consequences if the cryptography would be broken, taking into account the goal for which the cryptography is used;
- The estimated **time and effort** required to migrate to post-quantum cryptography. The estimations are primarily made based on known challenges in the migration and experience from previous cryptographic migrations.

In the next sections, concrete guidance to judge which attackers should be considered and each of these three components of the quantum risk will be presented. Finally, the last section combines these components into one risk score between 0 and 4, that can be used in a PQC migration plan or general risk management processes.

2.4.1 Realistic Attackers using Quantum Computers

Before performing a (quantum) risk assessment, an organisation needs to identify what attackers are realistically going to target them. For the quantum risk assessment, we assume that an attacker has an interest in attacking the organisation, and not specific systems of the organisation.
Currently, experts predict that there is a realistic threat of quantum computers in 10-20 years, where the predicted likelihood increases from 25% in ten years to over 60% in twenty years [MP23]. Since quantum computers are going to be extremely costly at the start, it is reasonable to expect that mainly state actors or highly motivated and capable attackers will use them to attack cryptographic infrastructures.

Their motivations will mainly be of political, military and economic nature, for example, aiming to cause disruption and to gather intelligence within other societies. These threats are therefore most relevant to organisations with a pre-existing threat from state actors, particularly from cyberpowers. Furthermore, organisations that provide or host critical infrastructure or that have long-lasting valuable secrets that need to be secure for 10 or more years, are in scope. When in doubt, the reader can always consult the national threat landscape of their national intelligence or cybersecurity organisations. In the 2023 yearly report of the Dutch intelligence services (AIVD), such examples of targets of nation states are given [AIVD23]. Amongst others, they explicitly warn governments, defence industry and prominent technology companies for the ongoing threat of espionage. Specifically on the threat of state actors, another document was published in 2022 by the AIVD, Military intelligence services (MIVD) and the National Coordinator for Security and Counterterrorism (NCTV) [NCTV22].

As quantum computing is expected to be largely made available via the cloud, the step from nation states to other motivated attackers expected to be quick. In this case, attackers with for example a monetary incentive will also be able to execute quantum attacks that might allow them to steal money or obtain commercially sensitive information. While (quantum) cloud-based attacks are a few years further in the future and will be expensive for an attacker, it means that eventually every organisation that is troubled with motivated attackers, it can be expected that they will face this threat within the decade of those facing state actors. This means that if they have malicious actors as threats, it will be but a matter of time before they too can exploit these vulnerabilities. Due to the exploit cost, mainly large multinationals, organisations who work on high-tech or innovative solutions, or other high-gain targets will be at risk.

2.4.2 Quantum Weakness

We divide the weakness of cryptographic algorithms used in an application in three different *quantum weakness scores*

0: The algorithm in use is quantum-safe and does not need to have migrated according to the current knowledge.

1: The algorithm is not (yet) in danger of being broken by a quantum computer but will need attention in the future. The most prominent example of this are symmetric-key algorithms and hash functions. There are known quantum attacks against some of these primitives in theory but these are not deemed feasible in the foreseeable future.

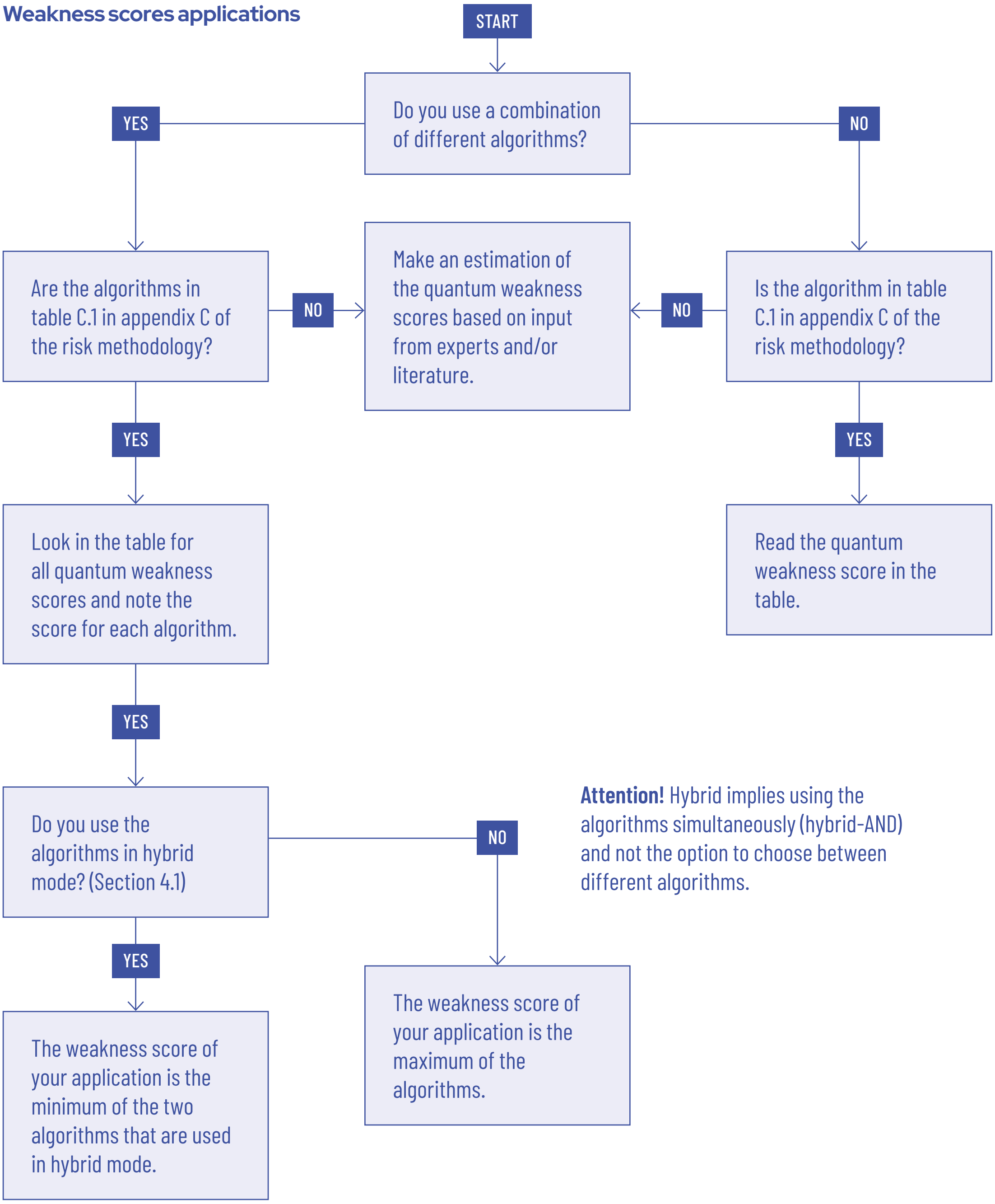
2: The algorithm is not safe against quantum computers and thus needs to be replaced by a quantum-safe alternative.

A list of many common cryptographic algorithms and their quantum weakness scores can be found in [dVBDvV24, Appendix (Bijlage) C].

Quantum Weakness on Application Level

In many applications in practice, cryptographic algorithms are combined to form one cryptographic solution. For example, TLS accommodates for choosing any of a list of cryptographic algorithms to protect a specific session and uses public-key encryption to set up a key for a symmetric-key algorithm. In these examples, the quantum weakness on the application level is in fact the highest weakness score of all of its algorithms. Intuitively, this can be explained by the fact that an attacker will simply choose the weakest cryptographic algorithm to attack the system. Only in the case where a hybrid-AND construction is used such that multiple cryptographic algorithms are used in a layered fashion, the system-level weakness score is the *minimum* of the weakness scores of the individual algorithms.

Weakness scores applications


START
Do you use a combination of different algorithms?
YES
NO
Are the algorithms in table C.1 in appendix C of the risk methodology?
NO
Make an estimation of the quantum weakness scores based on input from experts and/or literature.
NO
Is the algorithm in table C.1 in appendix C of the risk methodology?
YES
YES
Look in the table for all quantum weakness scores and note the score for each algorithm.
Read the quantum weakness score in the table.
YES
Do you use the algorithms in hybrid mode? (Section 4.1)
NO
YES
The weakness score of your application is the minimum of the two algorithms that are used in hybrid mode.
The weakness score of your application is the maximum of the algorithms.

Attention! Hybrid implies using the algorithms simultaneously (hybrid-AND) and not the option to choose between different algorithms.

Figure 2.5 | Flowchart for finding the quantum weakness of a system.

A flowchart to help organisations in finding the quantum weakness of a system can be found in Figure 2.5. Note that this flowchart judges combinations of algorithms used to protect one network connection (or similar). If one application uses cryptography to protect two endpoints, the flowchart needs to be followed for both endpoints separately.

2.4.3 Impact Analysis

The goal of the *impact score* is to measure how big the consequences are for an organisation in case the cryptography of a system is broken. In order to perform the impact analysis, it is important to identify whether it is realistic that an attacker could be targeting the organisation.
The expected impact is again divided into three levels (1, 2 and 3). Note that we now start at 1 instead of 0, since there will always be some form of impact if a system is compromised. Figure 2.6 can be used to judge the expected impact of the cryptography of a certain system being broken. For more intuition on the different levels or in case the flowchart does not apply to a system, the intuition behind each level is as follows

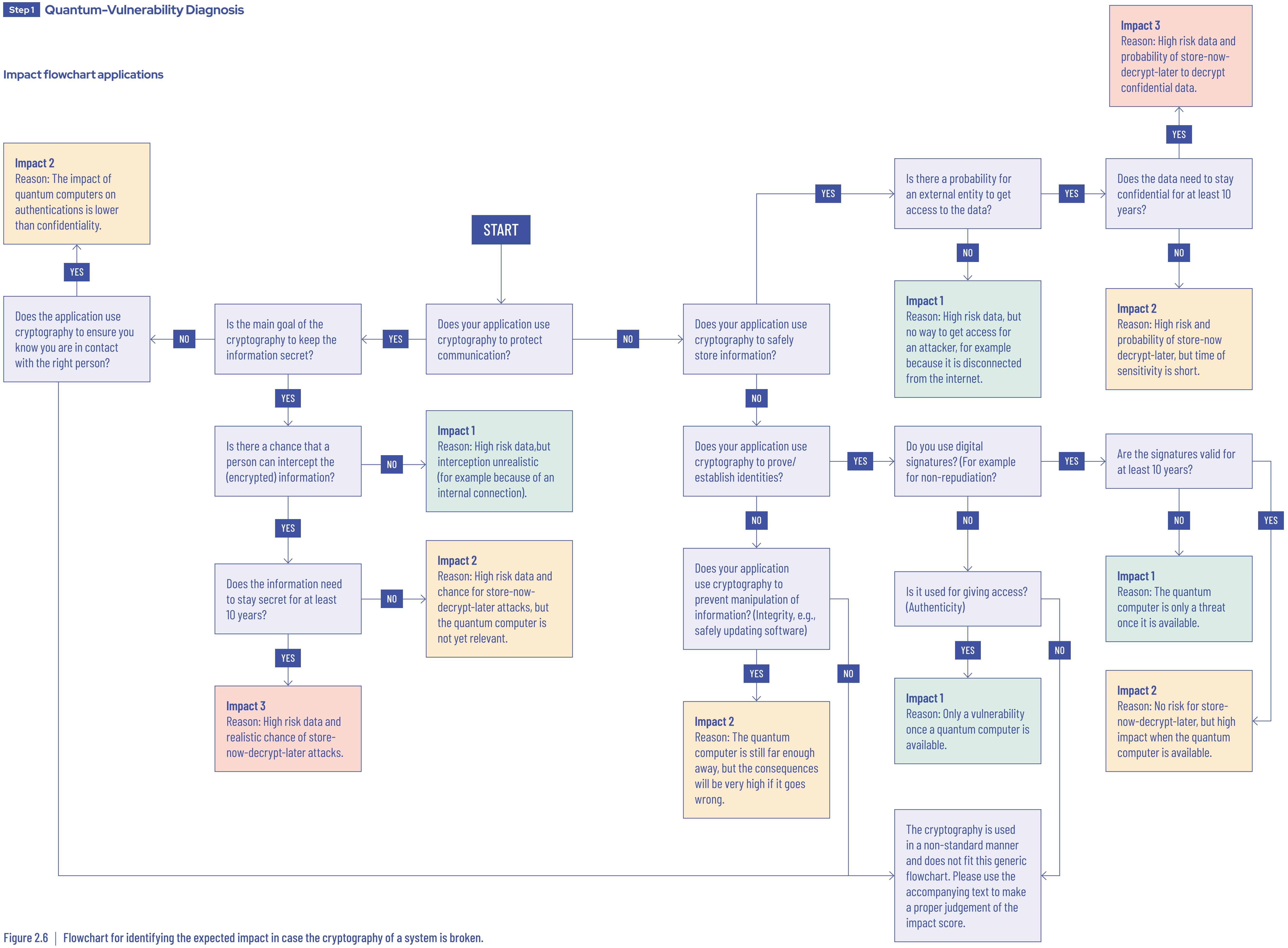
1: There is no significant impact that requires attention. This can for example be the case if the cryptography does not protect a sensitive system, because the threat is more than ten years away or if there is no realistic attacker known for the specific system or when other safety measures are taken.

2: In this case, there is a realistic attackerto cause impact, but not in the short term. An example can be sensitive data that can be intercepted but is not relevant anymore when it can realistically be decrypted. Another example is a system that has a high impact to the business, for instance verifying identities or securing the software updates that people install. In these cases, there is a high risk and likelihood of an attack to the system when a quantum computer is available. Hence it is essential to have migrated to post-quantum cryptography in time.

3: Finally, the highest impact score is given when the impact is already so high that it needs to be mitigated immediately. This is the case when there is a realistic attacker that can already intercept messages that are still sensitive when a relevant quantum computer is available. This is data, that is in this case compromised, still impacts the business or individuals significantly in 10-20 years. Examples are state secrets, intellectual property, confidential contracts or special personal information.

Note that this impact score is a snapshot of the current situation. The impact of a weakness will be different if sensitivity of the application or the timeline to a relevant quantum computer changes. Furthermore, it can change if the system is updated. Therefore, it is advised to repeat the risk assessment periodically as part of the regular risk-assessment process.

Impact flowchart applications



START

Does your application use cryptography to protect communication?

Is the main goal of the cryptography to keep the information secret?

Does the application use cryptography to ensure you know you are in contact with the right person?

Impact 2
Reason: The impact of quantum computers on authentications is lower than confidentiality.

Is there a chance that a person can intercept the (encrypted) information?

Impact 1
Reason: High risk data,but interception unrealistic (for example because of an internal connection).

Does the information need to stay secret for at least 10 years?

Impact 2
Reason: High risk data and chance for store-now-decrypt-later attacks, but the quantum computer is not yet relevant.

Impact 3
Reason: High risk data and realistic chance of store-now-decrypt-later attacks.

Does your application use cryptography to safely store information?

Is there a probability for an external entity to get access to the data?

Impact 1
Reason: High risk data, but no way to get access for an attacker, for example because it is disconnected from the internet.

Does the data need to stay confidential for at least 10 years?

Impact 3
Reason: High risk data and probability of store-now-decrypt-later to decrypt confidential data.

Impact 2
Reason: High risk and probability of store-now decrypt-later, but time of sensitivity is short.

Does your application use cryptography to prove/ establish identities?

Do you use digital signatures? (For example for non-repudiation)?

Are the signatures valid for at least 10 years?

Impact 1
Reason: The quantum computer is only a threat once it is available.

Impact 2
Reason: No risk for store-now-decrypt-later, but high impact when the quantum computer is available.

Is it used for giving access? (Authenticity)

Impact 1
Reason: Only a vulnerability once a quantum computer is available.

Does your application use cryptography to prevent manipulation of information? (Integrity, e.g., safely updating software)

Impact 2
Reason: The quantum computer is still far enough away, but the consequences will be very high if it goes wrong.

The cryptography is used in a non-standard manner and does not fit this generic flowchart. Please use the accompanying text to make a proper judgement of the impact score.

Figure 2.6 | Flowchart for identifying the expected impact in case the cryptography of a system is broken.

2.4.4 Migration Effort

Finally, it is important to estimate how much effort and time the migration to post-quantum cryptography is going to cost and how much unforeseen challenges can be expected. Note that this section only focusses on estimating the time it takes to migrate to PQC. In practice, other resources such as humans and money are also vital for a successful PQC migration. For guidance on estimating these resources, we refer to Chapter 3. The *migration effort score* is again divided in three levels

1: No major challenges are expected and the time to fully migrate a system to PQC is expected to take up to two years.

2: The migration is not trivial but no major hurdles are expected in the migration, the expected time to migrate is up to 8 years.

3: The migration is going to be difficult, and it is hard to predict what challenges will be encountered. This is for example if there are many dependencies on others, a lack of priority, a physically hard to reach system or other delaying factors. In this case, the migration to PQC will take more than 8 years.

The effort for migrating to PQC depends on many factors that vary heavily per organisation. Hence, there is no generic way of coming to a migration effort score and this is something that the organisation needs to judge itself. In the rest of this chapter, common factors will be explained that can help an organisation in judging the migration effort

Maturity of management organisation | Organisations that have proper life cycle management such as up-to-date inventories of their software, cryptography and certificates will have an easier time to find and migrate the cryptographic instances that need to have migrated.

External dependencies on standardisation and regulations | Sometimes, organisations cannot migrate themselves because they are restricted to certain regulations or forced to use a standardised algorithm. These processes can be lengthy and organisations have no influence on them. On the other hand, regulations can also speed up the adoption of PQC.

External dependencies on suppliers | Many organisations will be using soft- or hardware from external suppliers. This can speed up the migration if the supplier is already working on PQC solutions, in which case the organisation itself can focus on how to perform the eventual update smoothly. On the other hand, a supplier might not be working on PQC, for example because of a lack of priority, because the software is no longer maintained or the supplier does no longer exist. Also, compatibility between different systems managed by different organisations is going to be a major factor that slows down the PQC migration.

External hardware dependencies | Often, hardware will be used to speed up or manage cryptographic processes. For example, hardware security modules (HSM) are often used to create and manage cryptographic keys. The HSM needs to support the PQC algorithm first before another application can use the algorithm. Also, hardware acceleration is often used to speed up cryptographic operations. If the accelerator does not support the PQC algorithm, this can have significant impact on the performance of the system. In that case, new hardware needs to be installed which costs time, money or can even be impossible in certain OT (Operational Technology environments.

Limited hardware capabilities | Similar to hardware dependencies, the bandwidth, storage, speed and supported operations can also increase the effort needed to migrate to PQC. The PQC algorithms will have different requirements compared to the currently used algorithms. Low-end devices might have trouble accommodating for this. Notable examples are smartcards, IoT devices, OT systems and high-end systems that run many cryptographic operations such as corporate network devices.

Self-managed software/code | If an application or system is self-managed, the required expertise to migrate the system to PQC also needs to be in-house. If this is the case, the time to migrate can drop significantly. On the other hand, if an organisation does not have the expertise, it might be a major hurdle.

2.4.5 Quantum Risk Scores

As a final step, the three individual scores need to be combined into one quantum risk score between 0 and 4. The quantum risk score refers to the systems in the organisation. The quantum risk score can be found in Figure 2.7. A quantum weakness score of 0 will always lead to the lowest quantum risk score of 0 because the system is already adequately protected. The interpretation of the four levels is as follows

0: **Risk score 0 (No risk)** | All quantum threats are adequately mitigated.

1: **Risk score 1 (Low risk)** | There is a risk on the long term, but no priority is needed at the moment.

2: **Risk score 2 (Medium risk)** | Action is needed but the current cryptography is still secure on the short term or the migration is expected to be straightforward.

3: **Risk score 3 (High risk)** | Priority is needed on the short term because the expected impact is large and/or the migration to PQC is expected to take a long time.

4: **Risk score 4 (Acute risk)** | The system is already at risk, for example because because the expected migration effort in combination with how long the data should stay secure is longer than the expected time before a quantum computer will be able to break cryptography. In this case, there is a realistic threat that needs attention immediately, possibly from management in case of high business impact.

Depending on the PQC persona of an organisation, certain risks can or cannot be acceptable. For example, a regular adopter might be able to afford waiting longer with migrating a quantum risk 1 or 2 system. On the other hand, urgent adopters might already need to start prioritising systems with a quantum risk score of 1 or 2 onwards, because the expected damage is much higher in case the system is broken. In the end, the way organisations prioritise systems with different quantum risk scores depends on their overall risk management process, available resources and the general risk appetite of the organisation.

<table>
<tr><th>Weakness</th><th colspan="3">Impact</th><th colspan="3">Migration Effort</th><th>Risk</th></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>1</td><td>2</td><td>3</td><td>0</td></tr>
<tr><td>1</td><td colspan="3">1</td><td colspan="3">1</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">1</td><td colspan="3">2</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">1</td><td colspan="3">3</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">2</td><td colspan="3">1</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">2</td><td colspan="3">2</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">2</td><td colspan="3">3</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">3</td><td colspan="3">1</td><td>1</td></tr>
<tr><td>1</td><td colspan="3">3</td><td colspan="3">2</td><td>2</td></tr>
<tr><td>1</td><td colspan="3">3</td><td colspan="3">3</td><td>2</td></tr>
<tr><td>2</td><td colspan="3">1</td><td colspan="3">1</td><td>1</td></tr>
<tr><td>2</td><td colspan="3">1</td><td colspan="3">2</td><td>1</td></tr>
<tr><td>2</td><td colspan="3">1</td><td colspan="3">3</td><td>2</td></tr>
<tr><td>2</td><td colspan="3">2</td><td colspan="3">1</td><td>2</td></tr>
<tr><td>2</td><td colspan="3">2</td><td colspan="3">2</td><td>2</td></tr>
<tr><td>2</td><td colspan="3">2</td><td colspan="3">3</td><td>3</td></tr>
<tr><td>2</td><td colspan="3">3</td><td colspan="3">1</td><td>3</td></tr>
<tr><td>2</td><td colspan="3">3</td><td colspan="3">2</td><td>4</td></tr>
<tr><td>2</td><td colspan="3">3</td><td colspan="3">3</td><td>4</td></tr>
</table>

Figure 2.7 | Table from individual risk score to a final risk score per application.

Step 2

3 Migration Planning

Summary

This chapter provides a description of the action steps to help organisations with planning their post quantum migration. It is mainly intended for organisations that identify as urgent adopters and regular adopters who would like to act proactively.

In this chapterit is assumed that an organisation has already gone through the diagnosis step described in Chapter 2. Specifically, in order to decide which assets should be migrated first, the information described in Section 2.2.1 concerning the current security architecture of an organisation is required. Furthermore, the outcome of a quantum risk assessment is required to start planning when systems need to be migrated. Using this information, this chapter will guide you in determining two things.

The first part of this chapter is there to help determining when to migrate. The first NIST standards have been published in August 2024, and it is expected that in a few years, certified post-quantum cryptographic standards and libraries will be released. Some organisations can afford to wait for them to be available, while others have to start migrating today, potentially even to algorithms which are not yet standarised. This will influence a migration policy. The first section of this chapter provides all necessary information to decide which migration scenario corresponds to the organisation.

The second part of this chapter gathers advice on how to plan the migration. This is where which cryptographic assets need replacement is decided, what to replace them with and in which order they shoulde be replaced. This involves prioritising, identifying dependencies and anticipating some consequences of the migration, such as the necessity to temporarily isolate some data assets.

After carefully planning the migration, the subsequent chapter will provide guidance through the execution of the migration. Note that although this document describes the migration steps (diagnosing-planning-executing) sequentially, in practice an organisation should not wait to entirely complete one step before starting the next one. Organisations should start by identifying their most critical assets, planning a first migration phase for these critical parts and proceeding to this migration, while in parallel actively working on extending the diagnosis to a larger part of their infrastructure that will be migrated in a second phase.

3.1 When to Start Migrating?

Considering that systems may need to be migrated in the short term, it is now time to decide *when* to migrate. This is determined by three variables, namely the time X that the asset must remain secure, the migration time Y , and the time Z left until a quantum computer will be able to break public-key cryptography. A migration is executed in that time if $X + Y < Z$. This inequality is also known as Mosca's inequality, named after the researcher that introduced it. The closer $X + Y$ is to Z, the more urgent the migration is. Note that organisations can and should already start preparing for the migration by executing the no-regret moves.

In the quantum risk assessment of Section 2.4, in certain cases the impact score is directly influenced by the time an asset must remain secure. This is the case if the impact is level 3 because of the possibility of a store-now-decrypt-later attack. If this is so, it is advised to start migrating as soon as possible. Next to this, the migration effort score maps directly onto *Y*, the time needed to perform the migration. Here, the migration effort scores roughly map to the parameter *Y* in the following way:

Migration Effort Score	*Y*
1	0-2 years
2	5-8 years
3	>8 years

Table 3.1 | Mapping from Migration Effort to Years.

For this, one needs to consider the journey to industry-certified implementations of standardisation institutions post-quantum cryptography standards and its milestones. There are three suspected milestones in this journey, of which the first one, published NIST standards, was achieved in August 2024. This section aims to aid with the decision which moment should be chosen for which cryptographic asset.
Each asset should be migrated in a scenario with corresponding milestone *M*, as shown in Figure 3.1, so that the migration time *X* + *Y* + *M* is less than *Z*.

Estimating *M* | Naturally, it is difficult to determine when production-level and/or industry-certified PQC libraries are available for general use. This is especially true due to the fact that different PQC libraries will be aimed at optimising the algorithms for different use cases, such as smartcards or IoT devices. Hence, using experience of similar situations is a useful way of determining this timeframe.
Furthermore, end-users can have an influence on these timelines. This is the period when vendors should start developing production-level libraries. Contacting these vendors or making the desire for these libraries clear on the community feedback or online forums can influence how quick or slowly the libraries are published.

Estimating *Z* | Estimating when a quantum computer has the capabilities to break public-key cryptography is difficult and still being debated between experts. To provide an informed estimate, Michele Mosca conducts a yearly survey, asking a selection of experts in the field of quantum computing to provide their opinion on the probability that a quantum computer will break RSA-2048 in 5, 10, 15, 20 and 30 years. The outcome of the most recent survey [MP23] is reported in Figure 3.2. From this figure, a conservative estimate is that quantum computers will break public-key cryptography in 2040, while a less conservative one fears that it already happens in 2030.
Note that the time to actually perform the migration will vary per organisation or even per asset. This may be due to the fact that, for example, library documentation, commercial support and overall knowledge of PQC will most likely be more complete the later the migration starts. Hence, it is imperative that any system eventually migrates to either production-level or certified implementations of NIST PQC standards. Once again, the exact timing of migration will heavily depend on the risk appetite of the organisation.

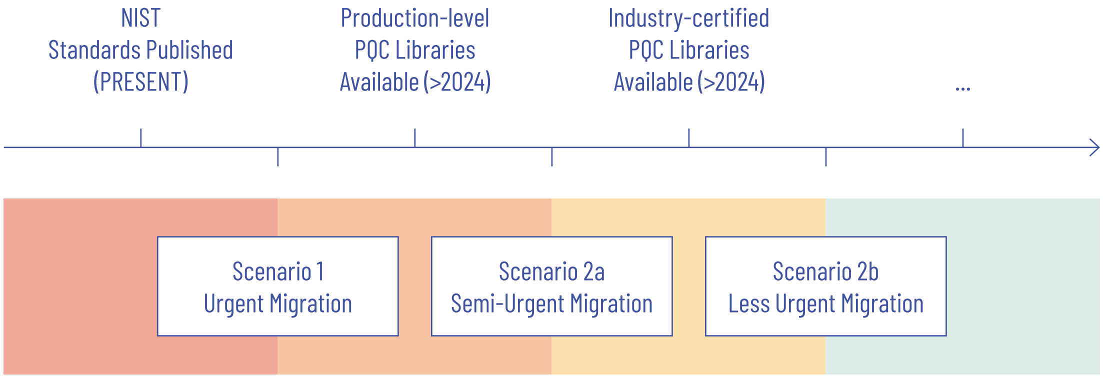


Figure 3.1 | Timeline of different migration scenarios.

Note on Certified Libraries

For some organisations it will be vital to migrate in Scenario 1, which will mean migrating to PQC standards without certified libraries being available. It should be mentioned that this brings an extra disadvantage because using uncertified libraries can lead to certification issues and using non-production-level code can lead to a slew of security problems. This disadvantage should be taken into account when choosing which Scenario to migrate from. It is important to note that the current most-used standard for cryptography, FIPS 140-2, already allows for hybrid schemes. This means that it is possible to obtain at least that certification using the hybrid approach. For more information on the hybrid approach, please refer to the 'Hybrid solutions' paragraph in Section 4.1.

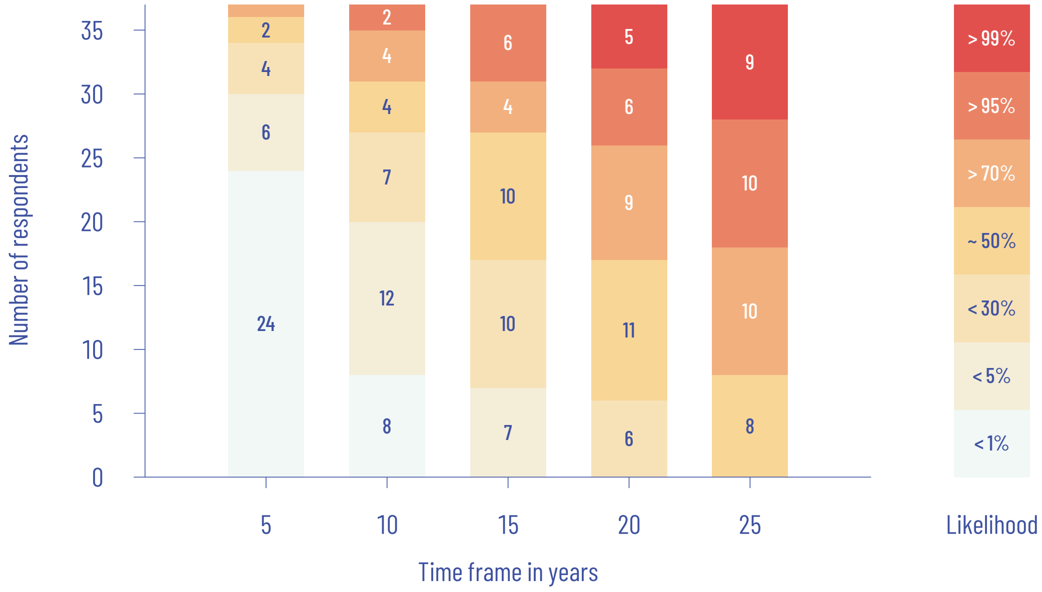


Figure 3.2 | Survey on probability of a quantum computer breaking RSA-2048 within *x* year from 2023 [MP23].

Determining the Migration Scenario

As part of the quantum risk assessment, an overall risk score per system was identified. Depending on the height of the risk a system faces and the risk appetite of the organisation towards the system, more or less priority to migrating the system should be given. Depending on the gap between the faced risk and the willingness to accept the risk, organisations can or cannot wait until all milestones are achieved, leading them to one of the three scenarios (urgent, semi-urgent or less urgent migration).

In Chapter 4, advice on how to migrate asymmetric primitives will be provided depending on a specific scenario. Note that in the rest of the document scenarios 2a, 2b are clumped together under the name Scenario 2. This is because, at a high-level, the advice for both is the same. Note that this advice may change once the milestones above are achieved.

General Strategy

As it is impossible to migrate everything at once, a general strategy is required. It is recommended to migrate outdated protocols to protocols that are currently recommended by the NCSC-NL first. This will test the asset management and the overall agility of both the cryptography and the organisation at a whole. Only once this is done is it recommended to begin the migration to PQC. This way, an organisation can already start modernising its migration process to smoothen the eventual transition.

3.2) Advice on Migration Planning

The second part of this chapter gathers advice on how to plan the migration. The main goal of this step is twofold.

1. For each cryptographic asset, decide if it needs to be replaced, and if so, identify what it should be replaced with;
2. Decide the order in which the different cryptographic assets should be migrated.

This section provides useful resources to help decide which cryptographic elements should be replaced and suggests solutions to replace them with (see Chapter 4). The prioritisation depends on the risk assessment established in the previous chapter, but should also take into account the dependencies and the consequences of the migration for a specific business.

3.2.1 Business Process Planning

As a considerable part of migration involves business processes, it is important that the planning phase focuses on this. First, a migration manager should be appointed, who will be responsible for the execution of the migration. This should be a person with thorough understanding of the organisation and access to all departments to guide the relevant employees on the necessary steps and timelines for the migration. Second, sufficient budget should be allocated to the necessary migration steps, such as time, finance and facilities. Lastly, during the process of migration, there will be moments when certain services and parts of the organisation will have to be isolated and shut down. The management of this "down time" should be carefully considered and planned beforehand to minimise the effect on the continuity of the organisation.
An appropriate planning takes into account the migration paths of other organisations to maintain interoperability as well. For this reason, it is wise to consider planning the migration together with a community of similar organisations. In some cases this might even be necessary because of cryptographic systems and assets between organisations being interrelated. Even if this is not the case, performing a migration planning together can still be beneficial because the workload of planning the migration can be divided. We refer the reader to the technical report [ETSI20a] written by ETSI for more advice on the business process planning.

3.2.2 PQC Maturity Assessment

For the migration to succeed it is important to identify the main issues that hinder the transition in an organisation. The growth model reported in [KJB24] helps to understand the aspects of the migration to focus on, and to understand the main technical and non-technical challenges. In the report, fifteen main migration challenges are listed and further elaborate:

1. Migrating legacy systems;
2. Lack of PQC standards;[1]
3. Lack of decision on the most suitable algorithms for different use-case;
4. Lack of testing and benchmarking;
5. Lack of PQC software and hardware certification and high-end implementations;
6. Lack of insights on the impact of quantum computing, and related risks and vulnerabilities;
7. Lack of urgency within a single organisation;
8. Lack of long-term vision on organisational benefits;
9. Lack of qualified personnel with PQC knowledge;
10. Lack of organisational urgency and planning;
11. Lack of urgency among stakeholders;
12. Lack of leadership among stakeholders;
13. Lack of collaboration among stakeholders;
14. Lack of policies and legal implications;
15. Technical complexity of the migration.

These challenges are not standalone and they influence each other. Tackling them can have a domino effect: the sooner an organisation starts taking action within their ecosystem, the easier it will be to solve the follow-up challenges. Conversely, attempting to address these issues in isolation will make the migration process significantly more difficult. As a result of the analysis in the report, collective actions and strong collaborations are highly advised as initial steps for migrating.
To guide in addressing these challenges, the growth model provided by the report can be consulted to obtain an overview of the migration trajectory.

The growth model is presented as an assessment matrix and clusters the fifteen challenges into eight main priority aspects:

- Collaboration;
- Awareness;
- Governance;
- Policies and Regulations;
- PQC availability;
- Hybrid approach;
- Strategies for cryptographic security;
- Knowledge on the PQC migration.

Each of these aspects is divided into five distinct growth stages. By identifying the aspects an organisation may need to work on, it is possible to gain a clear understanding of the progress and navigate the specific actions needed. This structured framework serves as a valuable assessment tool, allowing an organisation

[1] Research performed while NIST standards were not available.

to evaluate their current status within each aspect. The matrix is presented in Table 3.2. An online version of the assessment tool is under development and will be made publicly available in January 2025.
While the report primarily focuses on public-key infrastructures, its underlying principles and strategies are versatile and can be adapted to facilitate any organisation's transition to post-quantum cryptography.

3.2.3 Technical Planning

The technical part of the planning should focus on aspects such as which cryptography should be migrated, when it should be migrated and which methods should be used.

Dependency of Assets

An important goal of this planning is to identify the dependencies between the different cryptographic assets and decide the order of the migration. If an asset A depends on an asset B, decide whether A or B should be migrated first. Such dependencies should be clear from the inventory. To maintain interoperability between the assets during the migration, the post-quantum protocol can be made optional at first, until all the related assets have been migrated.

Cryptography Replacement

With the cryptographic inventory established and the dependency of cryptographic assets sorted out, the actual planning of replacing cryptographic assets can start. For each cryptographic asset it should first be decided whether it should be replaced, redesigned, retired or something else. This decision depends on different factors, such as importance of the asset to the organisation, consequences of misfunctioning of the asset, risk of the asset being attacked, but also available resources. Once it is decided that an asset needs to be replaced or redesigned, the next step is to decide which quantum-safe solution needs to be used. Chapter 4 suggests replacement solutions depending on the cryptographic asset and its use case. We advise to use a cryptographic solution which is crypto-agile, so that the implementation can quickly be updated once later standards or rules comes out. For more information on crypto-agility, see the 'Cryptographic Agility' paragraph in Section 4.4.
It is important that cryptographic assets are protected during migration as well. This can be done in several ways. The easiest way is by keeping the traditional cryptographic protection on the asset until after the asset is protected with the new quantum-safe solution. If this is not an option, asset isolation is the alternative.

Asset Isolation

In some cases, data/system isolation is the only way to completely protect an asset. This is particularly true for personal data and organisationally sensitive data handlers. There are different cases for when asset isolation is advised or even necessary. Firstly, data isolation brings protection against the so-called store-now-decrypt-later attacks. By physically separating this data from the network, the risk of such an attack can be taken away. This mainly holds for data in transit as these attacks are performed by listening in on a communication channel. Data at rest is less vulnerable to store-now-decrypt-later attacks.
Another situation when asset isolation is useful, is when it is not an option to keep asset protected during migration as mentioned in the previous paragraph. As migration is an involved process, it might not be possible to update all systems at the same time. Because of this, it may be necessary for some systems or data to remove their current cryptographic protection before the quantum-safe protection can be applied. Alternatively, it might be that it is currently too expensive to migrate certain assets, even though it is desirable to keep them protected. In either case, isolating the asset for the time that the asset is vulnerable makes sure that it keeps the required protection. After the required migration steps have taken place, the asset can then again be taken out of isolation.

However, it should be mentioned that asset isolation has a huge impact on functionality and availability of the data. As long as the asset is isolated, the asset cannot be used at all. This is an important aspect which should be taken into account when choosing to isolate an asset. In some scenarios asset isolation is not even an option because of this restriction.

Hardware Replacement

The migration may necessitate to replace hardware devices. In case of large-scale hardware replacement, the availability of the new product and the deployment time should be taken into account in the planning of the migration.

Testing

New solutions on both the hardware and software level will necessitate a phase of testing. The testing part is very important and should be anticipated. The tests should make sure that the new algorithms are compatible with the rest of the infrastructure and indeed provide the promised security.

3.3) Costs of the Migration

An essential component in planning the PQC migration is cost estimation and resource allocation. Comprehensive cost estimates should be taken into account when taking strategic PQC decisions and prioritising actions. For instance, the federal government of the US has estimated the total government-wide costs of the PQC migration between 2025 and 2035 to be 7.1 billion dollars [US24]. They have provided these cost estimates in order to prepare for the PQC migration, and require federal agencies to update their cost estimates annually.

Based on the Quantum Vulnarability Diagnosis, and in particular the cryptographic asset inventory, the scope and complexity of the PQC migration can be determined. The complexity is additionally influenced by the organisation's regulatory requirements and the PQC risk assessment. Subsequently, an organisation should estimate the manpower and the expertise required to execute the PQC migration, thereby taking into account which parts of the cryptographic infrastructure are directly under the organisation's control and which parts are managed by their vendors. Further, various tools and service are available to assist in the PQC migration. By estimating their costs, a well-informed decision on which tools and services to acquire can be made.

Furthermore, appliances might need to be replaced in case they can not support PQC or if the vendor is not planning to include PQC. Additionally, PQC algorithms often require more computational steps, for which the currently used cryptographic hardware might not be sufficient. If it turns out that the current hardware is not sufficient anymore, this also needs to be replaced.

An additional consideration with respect to the cost of the PQC migration is potential downtime. Ideally an organisation minimises its downtime and the impact on business operations, but unforeseen complications may occur. For the same reason, a backup must be in place and a robust procedure for recovering an organisation's communication infrastructure.

Finally, the PQC migration offers a great opportunity to bring an organisation's cryptographic policies and processes to a higher level. This may in fact be extremely desirable, taking into account that the current PQC migration is likely not going to be the last cryptographic migration. New cryptographic primitives are still being developed and standardised, offering the potential for future improvements. At the same time future cryptanalytic advancements may warrant adjustments or further cryptographic migrations. The costs of these future expenses should be taken into account, but they can be reduced by current investments in cryptographic agility.

	1. Collaboration	2. Awareness	3. Governance	4. Policies & Regulations	5. PQC availability	6. Hybrid approach	7. Strategies for cryptographic security	8. Knowledge on the PQC migration
Level 0	**1.0 Disengagement** The organisation is disengaged in the ecosystem. The organisation is disconnected and not actively involved.	**2.0 Unawareness** The organisation lacks awareness of the PQC migration. The organisation in unprepared and has not yet recognised the relevance and benefit of PQC.	**3.0 Governance vacuum** There is a lack of formal governance for migration in the ecosystem. There are no guidelines, rules or mechanism for decision-making, coordination and accountability.	**4.0 No formal policies & regulations** There is an absence of formal certification processes for PQC. There is a lack of regulations and policies for PQC migration.	**5.0 Limited knowledge on PQC** The organisation does not have knowledge of the key concepts related to the PQC migration. The organisation does not recognise the need for PQC.	**6.0 Limited knowledge on PQC** The organisation does not have knowledge of the key concepts related to the PQC migration. The organisation does not recognise the need for PQC.	**7.0 Reactive & ad hoc practices** The organisation has a reactive approach to security and risk management. Cryptographic algorithms and protocols are implemented on ad-hoc basis.	**8.0 Limited knowledge on PQC migration** The organisation has limited knowledge on the PQC migration. The organisation does not know what should be done. The organisation is not aware of the quantum threat and of the benefits of PQC.
Level 1	**1.1 Communicating & monitoring** The organisation recognises the importance of collaboration in the ecosystem. The organisation establishes communication channels in the ecosystem and monitors the PQC migration.	**2.1 Acknowledged awareness** There are emerging discussions on the PQC migration. The organisation recognises that change is necessary and acknowledges the potential impact of the quantum threat on the existing system.	**3.1 Recognition of assessment & planning** The organisation recognises the need for migration governance in the ecosystem. The organisation identifies shared objectives for the migration.	**4.1 Emerging insights & consideration** The organisation recognises the need for some level of policies and regulations.	**5.1 Basic understanding of PQC** The organisation has a basic understanding of the PQC migration. However, the organisation has not conducted a technical inventory assessment in the existing system.	**6.1 Basic understanding of PQC** The organisation has a basic understanding of the PQC migration. However, the organisation has not conducted a technical inventory assessment in the existing system.	**7.1 Defined policies & procedures** The organisation has defined cryptographic policies and guidelines outlining acceptable cryptographic algorithms and key management practices.	**8.1 Knowledge of the existing infrastructure** The organisation has conducted a cryptographic inventory assessment. The organisation has knowledge on the existing infrastructure and knows the vulnerable area and where PQC should be adopted.
Level 2	**1.2 Stakeholder identification** Organisation identifies potential directions for the PQC migration. The organisation develops plans to share expectations for the PQC migration with stakeholders	**2.2 Growing awareness** The organisation seeks information about PQC. There is a growing awareness of PQC. However, the organisation does not fully understand the scope of PQC.	**3.2 Shared governance principle** Organisations in the ecosystem engage in discussions on shared governance principles. Organisations set the foundational values and expectations for the PQC migration.	**4.2 Shared insights & discussions** The organisation engages in discussions and shares insights in the ecosystem on PQC guidelines and informal industry standards.	**5.2 Technical inventory assessment** The organisation assesses the existing infrastructure and identifies potential areas where PQC may be implemented. However, the organisation does not understand the full scope of PQC.	**6.2 Technical inventory assessment** The organisation assesses the existing infrastructure and identifies potential areas where PQC may be implemented. However, the organisation does not understand the full scope of PQC.	**7.2 Risk-based approach** The organisation has a risk-based approach to cryptographic security. Risk assessments are conducted to identify vulnerabilities and threats. The use of cryptographic algorithms is aligned with industry standards and compliance requirements.	**8.2 Knowledge of PQC** The organisation has knowledge on the limitations and the challenges of the different PQC algorithms. The organisation understands where the hybrid approach may be adopted and implemented in the existing systems.
Level 3	**1.3 Coordinated efforts** The organisation engages with the ecosystem to foster coordination for the PQC migration. Organisations work together to leverage a shared vision and collective goals.	**2.3 Informed awareness** The organisation explores different possibilities regarding the PQC migration. The organisation has a deeper understanding of PQC and identifies areas in the existing systems that need PQC.	**3.3 Governance structure** The organisation establishes a formal structure such as the creation of governing committees for the PQC migration. The organisation agrees on roles, responsibilities that facilitate decision-making.	**4.3 Gap analysis & preparation** The organisation identifies policy and regulation gaps regarding the PQC migration. The organisation evaluates the potential risks and consequence associated with the identified gaps in policies and regulations.	**5.3 Testing specification & use cases** The organisation conducts tests on PQC. The organisation identifies testing scenarios and use-cases of PQC. The organisation performs interoperability tests and validates functionality performance and resilience.	**6.3 Testing specification & use cases** The organisation conducts tests on PQC. The organisation identifies testing scenarios and use-cases of PQC. The organisation performs interoperability tests and validates functionality performance and resilience.	**7.3 Proactive approach** The organisation takes a proactive approach to cryptographic security. Advanced cryptographic controls are implemented to protect critical data assets. Cryptographic agility is emphasized into the organisation's security strategy.	**8.3 Knowledge of selection of PQC** The organisation has knowledge on the selection of different PQC algorithms. The organisation gains understanding and clarifies the knowledge needed for implementation and adoption. A roadmap, timeline, goals and resources are defined.
Level 4	**1.4 Collaborative actions** Organisations collaborate within the ecosystem to provide necessary support and resources for the PQC migration. Organisations actively take part in joint projects, initiatives and coordinate efforts to benefit the entire ecosystem	**2.4 Strategic awareness** The organisation aligns its awareness to its strategic goals for the PQC migration. The organisation makes plans to achieve a smooth PQC migration.	**3.4 Implementation & enforcement** The established governance structure and principles are put into practice. The organisation actively implements and enforces the governance mechanisms ensuring compliance, transparency and accountability.	**4.4 Voluntary guidelines** Voluntary measures and informal guidelines are introduced outlining criteria, procedures and requirements for the existing systems to become quantum-safe. These serve as recommendations and are not legally binding.	**5.4 Piloting & validation** The organisation implements a small scale solution and conducts a pilot deployment of PQC. The organisation monitors performance, gathers feedback. The organisation collaborates with stakeholders to assess usability and effectiveness.	**6.4 Piloting & validation** The organisation implements a small scale solution and conducts a pilot deployment of PQC with a hybrid approach. The organisation monitors performance, gathers feedback. The organisation collaborates with stakeholders to assess usability and effectiveness.	**7.4 Continued enhancement of cryptographic measures** The organisation improves its cryptographic security measures. There is an ongoing evaluation and adoption of new cryptographic algorithms and protocols. Cryptographic agility is emphasized into the organisation's security strategy.	**8.4 Knowledge of implementation of PQC** The organisation has a strategic plan to implement PQC in the existing systems. The organisation gains knowledge on implementations of PQC.
Level 5	**1.5 Collaborative actions & continuous dialogue** Organisations maintain continuous dialogue within the ecosystem. There is ongoing communication, reporting, feedback, and collaboration between leaderships to ensure the share vision and goals are cascaded.	**2.5 Foresighted awareness** The organisation looks ahead and stays up-to-date wit the latest developments in PQC. The organisation is aware of the evolution of PQC and strategically plans for future challenges.	**3.5 Continuous evaluation & adaptation** The organisation assesses the effectiveness of the governance framework in the ecosystem and makes necessary adjustments to meet its evolving needs. The established governance undergoes continuous evaluation and adaptation.	**4.5 Mandatory policies & regulations** Policies and regulations for PQC become mandatory by law. Regulatory bodies introduce legal mandates requiring PQC for standards, processes, and compliance requirements that all relevant organisations must adhere to.	**5.5 Scaled deployment** The organisation selects the PQC algorithms to implement and adopts them in the existing systems. A successful adoption leads to further scaling and integration of PQC.	**6.5 Scaled deployment** The organisation selects the PQC algorithms to implement with a hybrid approach and adopts them in the existing systems. A successful adoption leads to further scaling and integration of PQC with a hybrid approach.	**7.5 Mature & resilient cryptographic security** The organisation is highly responsive to cryptographic threats. Agile cryptographic security is a fundamental component of the organisation's security strategy. Cryptographic agility is scaled across the organisation allowing for a rapid adaption to emerging cryptographic standards.	**8.5 Knowledge of utilisation of PQC** A successful adoption leads to further scaling and integration of PQC. The organisation tracks performance, collects data and gathers feedback. The organisation shares knowledge and experience in line with industry best practices.

Table 3.2 | Growth Model Assessment Matrix.

Step 3

4) Execution

Summary

This chapter aims to give more information and guidelines on how to execute the migration. It will provide guidelines on migrating insecure cryptography and protocols. These guidelines provide both high-level and lower-level steps to successfully migrate to a quantum-safe environment. Many steps are conditional on when the organisation will actually perform the migration, which means it is recommended to first determine the migration scenario in the previous chapter. Furthermore, it is important to start working on the cryptographic agility of the assets already. The main recommendation for almost all protocols is to utilise a hybrid approach.

4.1) General Strategies

The final stage of the migration is the execution of the plan devised in the previous chapter. Ideally, at this point a complete overview of cryptographic assets is available, and a plan has been made outlining which PQC alternatives the vulnerable assets need to be migrated to. Alternatively, an organisation might opt to already start migrating high priority assets before the complete plan is finished and perform the final stage in parallel to the other stages. Be aware that IT environments are constantly changing. An asset inventory made two years ago will most likely not represent the current cryptographic landscape of an organisation. Therefore, it is important to continuously keep this asset inventory up-to-date .
The first section in this chapter gives some general strategies which can be applied in the PQC migration. The following two sections discuss in detail how to migrate cryptographic primitives and protocols.

⚠ **Warning** | The application of the migration plan should be performed with great care. Indeed, the replacement of certain cryptographic assets by others could introduce new vulnerabilities. An incorrect choice of replacement algorithm or an error in the new configuration could decrease the security level. In addition, the migration phase in itself increases the attack surface. Even if an organisation outsources this task, it is required to maintain a certain level of understanding of post-quantum cryptography internally, so as to understand the different trade-offs offered by each replacement solution. It is also important to acknowledge that post-quantum asymmetric cryptography is less mature than quantum-vulnerable asymmetric cryptography and still requires years of thorough cryptanalytical work to achieve the same level of confidence. Still, this should not be an argument to postpone the migration. Hybrid schemes allow for a security at least as good as the security level of the quantum-vulnerable algorithm used , which strictly reduces the threat of quantum computers.

Migration of Primitives vs. Protocols

Before discussing the migration of either primitives or protocols, there are important differences to be made clear. Cryptographic primitives generally do not live in isolation, but are used as a single piece in a larger protocol. This means that most organisations do not actually ever directly interact with purely the intimate details of cryptographic algorithms. Rather, they interact and use libraries that implement commonly used protocols that use cryptography, such as TLS. Various cryptographic choices can be made through these libraries, such as which primitives or key-sizes to use, but it is normally not the organisation's responsibility to implement their own cryptographic algorithms in libraries.

Generally, directly migrating primitives rather than protocols is reserved for the rare cases that an organisation is directly interacting with purely cryptographic libraries and potentially implementing their own protocols. On the other hand, for many organisations, updating a protocol that they do not implement themselves simply means updating the protocol version. For example, moving from TLS 1.2 to TLS 1.3.

The first part of Chapter 6 provides a list of the cryptographic primitives, their main characteristics and whether or not they provide quantum security. This chapter also presents the main post-quantum primitives.

Migration of Symmetric Cryptography

Theoretically, a quantum computer can attack symmetric-key cryptography, including hash functions, more efficiently than classical computers. In general, the resulting (theoretical) quantum advantage does not constitute a complete break of symmetric-key cryptography, but it may warrant the use of larger cryptographic keys. However, more detailed analyses have shown it to be unlikely that the above quantum advantage will be exploited for the purpose of breaking symmetric-key cryptography. Therefore, symmetric-key primitives are expected to remain secure against quantum attacks, even without increasing the key length. For this reason, we stress the importance of prioritising the migration of asymmetric-key cryptography. For more details, we refer to Section 4.2.3.

Migration of Asymmetric Cryptography Using Hybrid Solutions

A cryptographically relevant quantum computer will be able to break certain asymmetric-key, compromising all associated security guarantees. Encryption schemes and key exchange/encapsulation mechanisms, which protect the confidentiality of data, are vulnerable to store-now-decrypt-later attacks. To mitigate this threat, a timely migration to PQC is essential. Digital signature algorithms, used for authentication and integrity, do not suffer from store-now-decrypt-later vulnerabilities, making their migration to PQC potentially less urgent. Additionally, special attention is required for long-lived systems such as critical infrastructures, satellites, and operational technology. Updating the long-lived systems developed and deployed today may be difficult or even impossible.

Hybrid Solutions

Hybrid solutions denotes the use of both quantum-vulnerable and post-quantum cryptography together in parallel within one single protocol. To break the scheme, an adversary would need to break both the quantum-vulnerable and the post-quantum algorithm. Hence, the security of the complete scheme is at least as good as the security of each algorithm separately.

This aims at mitigating the security risks induced by the relative lack of maturity of the new postquantum algorithms, as well as having the added security of the post-quantum algorithm.

Next to this mathematical security, deploying quantum-vulnerable and post-quantum algorithms in hybrid also protects against implementation mistakes in the new implementations of PQC. Finally, hybrids are particularly interesting to use in environments where PQC is not yet allowed or trusted. Using PQC in combination with a trusted, quantum-vulnerable algorithm has the potential to use PQC while still being compliant with existing regulations.

Hybrid is particularly recommended for organisations that need to deploy quantum-safe cryptography before reference implementations of the new standardised algorithms become available, for instance if the data of the organisation is prone to store-now-decrypt-later attacks today already. The main drawback of this technique is that it can induce an overhead (in time and/or memory) as now two cryptographic algorithms need to be executed for a single encryption or signature. But as most post-quantum schemes already induce relatively more costs compared to quantum-vulnerable cryptography, this additional cost should be reasonable. In typical scenarios the hybrid solution is used only once to set up a (symmetric) keypair to encrypt the remainder of a connection. In these scenarios, the additional costs of the hybrid solution are low compared to entire connection.

⚠ **Warning** | When products claiming to use hybrid encryption or signatures are encountered, organisations need to make sure that this corresponds to the above description, that is, using quantum-vulnerable AND post-quantum algorithms at the same time for the encryption or signature. This is not to be mistaken with having a choice between using quantum-vulnerable OR post-quantum algorithm for encryption (see below). Furthermore, hybrid encryption is also often used to denote a combination of symmetric and asymmetric cryptography, where the asymmetric cryptography is typically used to set up a key for the symmetric algorithm. This is also not the hybrid AND strategy.

Downgrade Attacks

Some hybrid approaches face the risk of downgrade attacks. This happens when a system implements *hybrid OR* instead of *hybrid AND* explained above. Hybrid OR, or equivalently optional post-quantum describes a situations where both the quantum-vulnerable and the post-quantum algorithm are implemented on the server. However, to communicate with the server, a client can choose to use the quantum-vulnerable or the post-quantum protocol and is not forced to use both. Such a configuration is beneficial for backwards compatibility. This backwards compatibility is very convenient during the testing and early development phase to provide interoperability. Such solutions present an important risk an adversary can pretend not to support post-quantum protocols and hence force the server to communicate using the quantum-vulnerable algorithm. This is known as a *downgrade attack*. Even if the malicious actor cannot break the quantum-vulnerable primitive used, it can still perform store-now-decrypt-later attacks.

Therefore, it is generally recommended that internal systems use hybrid in the hybrid AND form described above. However, for externally facing systems this can be more cumbersome and hybrid OR might be the only option. Policies and strategies need to be formed for when and how such systems can use hybrid schemes correctly.

Migration of Asymmetric Cryptography Using Pre-shared Keys

Another way to make asymmetric cryptography quantum-safe is by using symmetric cryptography with pre-shared keys. This method aims to establish communication without any form of public-key cryptography. To use this method, pre-shared keys need to be established in a physical way, such as via USB. Because of this, establishing such keys is usually quite a cumbersome process and it in particular makes this solution scale poorly in many-to-many infrastructures. Moreover, since public-key cryptography is avoided, validating certificates is not possible. However, once such pre-shared keys are established, this is a very high-security and efficient approach.

It is therefore recommended to use the hybrid approach, unless the system satisfies *all* of the following requirements:

1. The system needs to be migrated from Scenario 1.
2. The system is within the full control of the organisation and is completely trusted.
3. The system will only communicate with equally trusted and fully controlled systems.
4. There is a practical way of sharing the secret keys between the communication systems.
5. The networks in which these communicating systems exist are very confidential and its layout does not frequently change.
6. Adding nodes to or removing nodes from these networks is not done frequently.

Examples of protocols for which using pre-shared keys is an option are TLS and IPSec.

4.2 〉 Recommended Cryptographic Primitives

Executing the PQC migration requires making very specific choices, one of which is choosing which post-quantum primitive to use in practice. This choice can be a challenging task and it requires expert and knowledge. This section presents a table of recommended cryptographic primitives (Table 4.1) and a table with the corresponding recommended parameter sets (Table 4.2). In addition, we provide explanations of the nuances and rationale behind these recommendations. It is important to note that these tables are not exhaustive. For instance, while SHA-2 and SHA-3 are recommended general-purpose hash families, they may not be suitable for all application scenarios. For example, password hashing typically requires special-purpose hash functions such as Argon2. In general, there is a broad spectrum of application scenarios that may necessitate cryptographic primitives beyond those discussed in this section. This section is intended to guide software developers and security architects, assuming a certain level of familiarity with cryptography. For a more comprehensive discussion of the recommended cryptographic primitives, see Chapter 6.
Additionally, there as some tools that can provide guidance in making an informed choice on the most suitable cryptographic primitive depending on specific use cases and security requirements. More information can be found in Section 6.4.

Functionality	Type	Recommended	Acceptable	Deprecated
Key Exchange/ Key Encapsulation	Asymmetric	ML-KEM[1]	FrodoKEM[1] Classic McEliece[1]	ECDH[3] RSA[3]
Digital Signature – Stateless	Asymmetric	ML-DSA[2] SLH-DSA	FN-DSA[2]	ECDSA[3] EdDSA[3] RSA[3]
Digital Signature – Stateful	Asymmetric	XMSS LMS HSS		
Hash Function	Hash	SHA-2 SHA-3	BLAKE2	MD5 SHA-1
Block Cipher	Symmetric	AES	Camellia	(T)DES IDEA Blowfish
Stream Cipher	Symmetric	AES-CTR ChaCha20		RC4
Encryption	Symmetric	AES-CTR ChaCha20		
Authenticated Encryption (with Associated Data)	Symmetric	AES-GCM(-SIV) AES-OCB ChaCha20-Poly1305		
Message Authentication Code	Symmetric	CMAC-AES HMAC-SHA-2 KMAC	CMAC-Camelia BLAKE2-MAC	CBC-MAC

[1] Recommended to be deployed in a hybrid combination with ECDH. [2] Recommended to be deployed in a hybrid combination with either ECDSA or EdDSA. [3] Secure against classical attacks and can be part of a hybrid scheme.

Table 4.1 | Cryptographic primitive recommendations.

Primitive	Recommended	Acceptable
ML-KEM[3]	ML-KEM-1024[1]	ML-KEM-768[1]
ML-DSA[3]	ML-DSA-87[2]	ML-DSA-65[2]

SLH-DSA	SLH-DSA-(SHA2/SHAKE)-256(s/f)
	SLH-DSA-(SHA2/SHAKE)-192(s/f)
		SLH-DSA-(SHA2/SHAKE)-128(s/f)

AES	AES-256	AES-128
SHA-3	SHA-3-256 SHA-3-384 SHA-3-512 (c)SHAKE256	SHA-3-224 (c)SHAKE128
SHA-2	SHA-256 SHA-384 SHA-512	SHA-224

[1] Recommended to be deployed in a hybrid combination with ECDH. [2] Recommended to be deployed in a hybrid combination with either ECDSA or EdDSA. [3] BSI, ANSSI, NLNCSA recommend the use of NIST level 5 or 3 parameter sets. NSA CNSA 2.0 requires level 5.

Table 4.2 | Recommended parameter instantiations of the cryptographic primitives.

4.2.1 Key Exchange/Encapsulation and Digital Signatures

Recently, NIST has finalised the standards for the lattice-based asymmetric primitives ML-KEM [NIST24a], the key encapsulation mechanism formerly known as CRYSTALS-Kyber, and ML-DSA [NIST24b],the digital signature algorithm formerly known as CRYSTALS-Dilithium. These primitives have undergone thorough scrutiny during NIST's PQC standardisation process and are therefore considered ready for practical deployment. We recommend that these primitives be deployed in a hybrid mode, combined with well-established elliptic curve-based primitives, to ensure that PQC implementation vulnerabilities and potential advances in lattice-based cryptanalysis do not immediately render the cryptography insecure. Both standards specify three parameter sets, corresponding to security levels 1 (or 2 in the case of ML-DSA) 3, and 5. We recommend initialising the primitives with the strongest parameter set, security level 5, when possible, and consider security level 3 an acceptable alternative (see Table 4.2). The ML-KEM standard specifies security level 3 as the default option; thus, our recommendations can be considered slightly more conservative.

The third PQC standard published by NIST is the hash-based digital signature algorithm SLHDSA formerly known as SPHINCS+. Since its security relies solely on the security of the underlying hash function, SLH-DSA is considered a slightly more conservative choice than its lattice-based counterpart ML-DSA. For this reason, it is not deemed necessary to deploy this scheme in a hybrid combination with elliptic curve primitives. For the same reason, we consider security level 1 an acceptable instantiation of SLH-DSA.

FN-DSA, formerly known as Falcon, presents an additional lattice-based digital signature algorithm. Together with ML-KEM, ML-DSA, and SLH-DSA, it has been selected for standardisation. However, in contrast to these other primitives, the FN-DSA standard has not yet been finalised. Thus, we currently recommend the usage of ML-DSA and SLH-DSA over FN-DSA.

Finally, we recognise that there may be scenarios in which a stronger level of conservatism is desired. For these scenarios, FrodoKEM and Classic McEliece provide key encapsulation functionality. At the cost of decreased overall efficiency, these primitives are built from more conservative assumptions and are accompanied with a more conservative security analysis. It is therefore less likely that the underlying assumptions will turn out to be invalid and that cryptanalytic attacks become feasible. However, FrodoKEM and Classic

McEliece have not yet been standardised. Until this is the case, we consider these primitives merely acceptable, although we strongly support ongoing initiatives aiming to standardise them. When instantiating these schemes, we recommend following the most recent parameters sets aiming for security level 5 or 3.

4.2.2 Stateful Digital Signature Algorithms

In addition to SLH-DSA, the primitives XMSS, LMS, and HSS also provide standardised hashbased digital signature algorithms. These primitives are even more efficient and may therefore be preferable to the previously mentioned digital signature algorithms. However, they come with one significant drawback they are *stateful*. Stateful signature schemes can only produce a fixed number of signatures and require careful state management. More precisely, after every usage of the private key, the state must be updated. Furthermore, if the state is lost, the scheme is insecure. For these reasons, stateful signature schemes are only applicable in specific scenarios that allow for such careful state management. However if deployed correctly, stateful signature schemes provide efficient and conservative digital signature functionality. NIST has published a comprehensive set of guidelines for deploying stateful signature schemes [NIST20a].

4.2.3 Symmetric-Key Cryptography

Theoretically, symmetric-key primitives can be attacked by Grover's quantum algorithm in quadratically fewer steps than a classical brute-force attack. This suggests a halving of the security level, which can be counteracted by doubling the key length. More concretely, this implies that a key length of 128 bits should be avoided, and 256 bit keys are advisable. However, a more detailed analysis of the Grover quantum attack shows that its costs are at least comparable to the costs of a classical attack [JNRV20]. The main reason is that, unlike the quantum attack, the classical attack can be parallelised. Therefore, it is likely that 128 bit symmetric-key primitives will remain secure far beyond the realisation of quantum computers capable of breaking asymmetric-key primitives.

In general, we recommend the use of 256 bit keys when possible and consider 128-bit keys an acceptable alternative. The key takeaway is that organisations should prioritise the migration of asymmetric-key primitives. In fact, we recommend that organisations only allocate resources to increasing symmetric key lengths if they have migrated all of their asymmetric primitives to post-quantum alternatives.

4.3 Migrating Protocols

This section discusses how to migrate protocols to a quantum-safe version. Different commonly used protocols are discussed, and for each protocol at least one solution to migrate to PQC is listed. For each of these solutions, action steps are listed for both system administrators, library developers and personnel responsible for security policies in the organisation. Note that this is still quite high-level, but already gives advice to some of the relevant parties.

It should be noted that only very common protocols are presented in this section, namely TLS, SSH, S/MIME, PGP, IPSec and X.509. Many of these aforementioned protocols are defined in a type of document called an RFC (Request for Comments). These are standardisation documents that are produced by the Internet Engineering Task Force (IETF). Draft standards are called Internet-Drafts.

TLS

Description | Ensures the confidentiality, authenticity and integrity of communication over the Internet [Res18].

Current Version | TLS 1.3 [Res18].

Standardisation Documents | RFC 8446 [Res18].

Common Usage | TLS is used in a variety of domains such as HTTPS and secure email.

To migrate TLS to PQC, there are two options using pre-shared keys (Option 1) and the hybrid approach (Option 2).

Note to System Administrators | For any scenario or option, it is recommended to use TLS 1.3 as long as the hardware supports it. Furthermore, ensure that either **AES-256-GCM** or **ChaCha20-Poly1305** are included in the chosen cipher suites for the Authenticated Encryption with Associated Data ciphers.

TLS Option 1 Pre-shared Keys

Necessary Policies | Whilst the policies may vary from use case to use case, a strict policy for sharing these symmetric keys must be established to prevent malicious actors from obtaining them and to prevent them from being accidentally shared to the wrong system. Furthermore, a policy that clearly defines which systems use TLS with pre-shared keys must also be established. Lastly, key management policies must be updated to reflect the introduction of these pre-shared keys.

Pre-shared keys should be at least 256-bit to prevent store-now-decrypt-later attacks. However, a lower bit key can also be acceptable taking into consideration how long the information needs to remain confidential, as previously discussed.

Lastly, a clear policy stating when and how to perform the shift from pre-shared keys to either a hybrid or fully post-quantum keys is required.

System Administrators | Naturally, the system administrator must configure TLS to utilise pre-shared keys. Furthermore, these keys need to be managed properly. For example, how they are generated, shared, stored and revoked securely. This information can be found in the TLS vendor's documentation and if the TLS implementation does not support pre shared keys, contact the TLS vendor.

Library Developers | A detailed technical overview of implementing pre-shared keys into TLS is defined in RFC 4279 [ET05] and RFC 5487 [IETF09]. Library developers should ensure that their TLS implementation conforms to these standards.

TLS Option 2 Hybrid Approach

An Internet-Draft indicating on how to perform hybrid key exchange is a helpful tool to understand how the hybrid solution can be implemented in TLS [IETF24].

Necessary Policies | A discussion with the system administrator and if necessary, cryptographic experts, about the allowed cipher suites that can be used to ensure quantum-safety. It may not be required to ensure that all systems are quantum-safe as per the previous explanations on store-now-decrypt-later attacks, so defining which systems would use this altered TLS is imperative.

This is especially important as the RFC is currently in draft and is bound to be updated, which means that the policies need to reflect these changes. Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | The system administrator must configure the TLS to utilise this hybrid approach. This information can be found in the TLS vendor's documentation and if the TLS implementation does not support this RFC, consider changing TLS vendor or contact the TLS vendor.

Library Developers | Library developers can implement this experimental feature based on the RFC. Naturally, more revisions of this draft will be published, so it is expected that implementations will change over time.

SSH

Description | Allows parties to perform secure remote network services.

Current Version | SSH-2 [LY06].

Standardisation Documents | RFC 8446 [LY06].

Common Usage | One of the most common usages is using SSH to remotely login and remote command execution.

Since the SSH protocol does not accept pre-shared keys, all scenarios should consider the hybrid approach. An Internet-Draft on hybrid key exchange shows how hybrid SSH can be implemented [KSFH+20].

Necessary Policies | A discussion with system administrator and, if necessary, cryptographic experts, about the allowed ciphers that can be used to ensure quantum-safety. It may not be required to ensure that all systems are quantum-safe so defining which systems would use this altered SSH is imperative. This is especially important as the RFC is currently in draft and is bound to be updated, which means that the policies need to reflect these changes.

Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | The system administrator must configure SSH to utilise this hybrid approach. This information can be found in the SSH vendor's documentation and if the TLS implementation does not support this RFC, consider changing SSH vendor or contact the SSH vendor.

Library Developers | Library developers can implement this feature based on the RFC. Naturally, more revisions of this draft will be published, so it is expected that implementations will change over time.

S/MIME

Description | S/MIME provides confidentiality and authentication to MIME data (audio, pictures...).

Current Version | S/MIMEv4 [Hou02].

Standardisation Documents | RFC 8551 [SRT19] and RFC 3369 [Hou02].

Common Usage | S/MIME is frequently used in secure email communication.

At this moment in time, there is little research on post-quantum S/MIME. OpenQuantumSafe offers a fork of OpenSSL that includes a quantum-safe S/MIME that either uses a hybrid approach or only uses post-quantum primitives [OQS S/MIME24]. However, they state that their library is not meant for production environments which limits real-world usage.

Since this protocol does not accept pre-shared keys, all scenarios should consider the hybrid approach.

Necessary Policies | Probably the ideal policy to implement is to not use email to exchange information which needs to be kept confidential longer than the start of the decryption phase of store-now-then-decrypt-later attacks. Any exchange of such information should be flagged as a security incident. If the vendor implements a production-ready quantum-safe version of S/MIME, then a policy should be implemented that indicates the correct usage and transitioning to this new version.

Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | If the vendor implements a production-ready quantum-safe version of S/MIME, then the system administrator should configure this new version of S/MIME as per the established policy. Contacting the current S/MIME vendor to inquire about quantum-safety is also an option.

Library Developers | The aforementioned OpenQuantumSafe library can be used as a basis for altering the S/MIME library to be quantum-safe. This should be explicitly labelled as an experimental feature and the developer should continue to monitor for new developments in this area.

PGP

Description | PGP provides confidentiality and authentication to data and services for key and certificate management.

Current Version | OpenPGP [IETF07] and GnuPGP [MJ21].

Standardisation Documents | RFC 4880 [IETF07].

Common Usage | PGP is frequently used in secure email communication.

System Administrators | Any exchange of such information should be flagged as a security incident.

Contacting the current PGP vendor to inquire about quantum-safety is also an option and the organisation should continue to look for new developments in this area.

Library Developers | Monitoring any RFC drafts and scientific literature in this area is imperative so that PGP can begin to be migrated to a quantum-safe version.

IPSec

Description | IPSec encrypts and authenticates IP packets between communicating parties.

Current Version | IPSec-v3 [FK11].

Standardisation Documents | RFC 6071 [FK11].

Common Usage | IPSec is frequently used in VPNs.

To migrate IPSec to quantum-safe, there are two options using pre-shared keys (Option 1) and the hybrid approach (Option 2).

IPSec Option 1 Pre-shared Keys

Necessary Policies | Whilst the policies may vary from use case to use case, a strict policy for sharing these symmetric keys must be established. Furthermore, a policy that clearly defines which systems that use IPSec with pre-shared keys must also be established. Lastly, key management policies must be updated to reflect the introduction of these pre-shared keys.

It is important that the parties holding the symmetric pre-shared keys conform to the requirements that the keys must be at least 256 bits long to avoid store-now-decrypt-later attacks. However, a lower bit key can also be acceptable taking into consideration how long the information needs to remain confidential, as previously discussed. Lastly, it is important that there is a clear policy that states when and how to perform the shift from pre-shared keys to either a hybrid or fully post-quantum.

System Administrators | Naturally, the system administrator must configure IPSec to utilise pre-shared keys. This information can be found in the IPSec vendor's documentation and if the IPSec implementation does not support pre shared keys, consider changing IPSec vendor (at least for the systems that require pre-shared keys) or contact the IPSec vendor.

Library Developers | A detailed technical overview of this process is defined in RFC 7296 [KHNE+14]. Library developers should ensure that their IPSec implementation conforms to these standards. There is also an Internet-DraFt that can be useful for developers to utilise pre-shared keys to achieve quantum-safety [FKMS20].

IPSec Option 2 Hybrid Approach

A helpful technical resource to achieve quantum-safety in IPSec is ETSI TR 103 617 [ETSI18].

Necessary Policies | A discussion with the system administrator and if necessary, cryptographic experts, about the allowed cipher suites that can be used to ensure quantum-safety. It may not be required to ensure that all systems are quantum-safe as per the previous explanations on store-now-decrypt-later attacks, so defining which systems would use this altered IPSec is imperative. This is especially important as the RFC is currently in draft and is bound to be updated, which means that the policies need to reflect these changes. Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum.

System Administrators | The system administrator must configure IPSec to utilise this hybrid approach. This information can be found in the IPSec vendor's documentation and if the IPSec implementation does not support this hybrid approach, consider changing IPSec vendor (at least for the systems that require a hybrid system) or contact the IPSec vendor.

Library Developers | Library developers can implement this feature based on the ETSI technical report [ETSI18]. Naturally, more revisions of this draft will be published, so it is expected that implementations will change over time.

X.509

Description | X.509 proves ownership of a public-key.

Current Version | X.509v3 [ITU19].

Standardisation Documents | RFC 5280 and ITU-T X.509 [ITU19].

Common Usage | X.509 is frequently used to authenticate websites in HTTPS.

Since the X.509 protocol does not accept pre-shared keys, all scenarios should consider the hybrid approach. The ITU-T has already standardised a variant of hybrid (multiple algorithms) certificates in Section 9.8 of [ITU19]. It is based on the expired Internet-Draft by Truskovsky et al. [TGFK+18]. In the literature, these certificates are often referred to as catalyst certificates. Additionally, IETF is developing new Internet Drafts [OGPK+24b; OGPK+24a] that provide an alternative form of hybrid certificates, called composite certificates. Naturally, more root CAs and CAs will begin to offer post-quantum certificates, so it is important to keep up-to-date with the market.

Necessary Policies | It may not be required to ensure that all certificates are compatible with the hybrid solution as per the previous explanations on store-now-decrypt-later attacks, so defining which systems would use this altered X.509 certificate is imperative. Furthermore, it must be noted that cryptographic and protocol libraries must then be compatible with the new certificates.

Lastly, it is important that there is a clear policy that states when and how to perform the shift from the hybrid approach to fully post-quantum. To achieve all this, communication and planning with the CA or root CA is essential.

System Administrators The system administrator must configure X.509 certificates to be compatible with the hybrid approach.

Library Developers | Library developers can implement this experimental feature based on the RFCs and the ITU-T standard. Naturally, more revisions of the drafts will be published, so it is expected that implementations will change over time.

4.4) Cryptographic Agility

Cryptographic agility is a form of agility that helps to adapt to risks surrounding the use of cryptography with minimal effort. Concretely, cryptographic agility refers to the practice of structuring technology, processes and policies such that cryptography used at an organisation can be configured in an efficient manner. This means that the cryptography can be updated, changed or completely replaced with minimal effort and minimal consequences such as downtime for the organisation. Cryptographic agility can help at different levels of cryptography; it can help to smoothen the revocation of cryptographic keys, update the parameters, replace one cryptographic algorithm by another or replace an implementation of a cryptographic algorithm.

Cryptographic agility is not something that can be bought but requires alignment on different levels in an organisation. Technical solutions exist that allow, for example, to automatically detect issues with cryptography or configure/ replace the implementation of a cryptographic algorithm. Next to this, cryptographic agility should also be integrated in business processes as well company policies in order to ensure that the technical cryptographic agility solution can be used properly. For example, cryptographic agility can be integrated in change management or procurement processes and integrated in cryptographic policies to mandate certain measures across an organisation.

The PQC algorithms that are currently (being) standardised are still relatively untested in practice, and thus it is likely that their settings, parameters or even the entire algorithms need to be updated in the future. With cryptographic agility in place, this can be done with minimal resources and limited disruptions. Especially when choosing to partially migrate certain assets before actual standards and validated implementations are available, an organisation needs to be prepared to easily switch the cryptographic algorithms once the relevant standards are available or a new implementation is recommended. This is different from currently used, quantum vulnerable cryptography where standards and good parameter choices are well established and changes happen less often.

Not only does cryptographic agility help with performing a smooth migration to PQC, it also helps with managing cryptography in general. Therefore, working towards a more cryptographic agile organisation is considered a no-regret move as it already helps now in identifying potential vulnerabilities earlier and reduced response times in case of an incident.

Nevertheless, cryptographic agility remains a somewhat abstract concept in practice. Discussing specific modalities or *forms* of cryptographic agility can help to make the goal more explicit. In this chapter, we will first provide guidance on how cryptographic agility be incorporated in technology, processes and policies. After that, we describe different forms of cryptographic agility and common challenges to achieve them. Finally, we discuss considerations when choosing an applicable cryptographic agility strategy.

Technical Measures for Cryptographic Agility

At a technical level, various measures can be implemented to ensure smooth transitions between cryptographic algorithms, parameters or implementations. A starting point for cryptographic agility is again knowing what and where cryptography is used in an organisation. Maintaining an up-to-date cryptographic inventory helps a lot with monitoring, identifying and updating vulnerable cryptography quickly. In Section 2.3, technical solutions are presented that can help with maintaining such an inventory.

Furthermore, a major agility challenge in managing cryptography are compatibility issues. This can for example occur if a new algorithm is adopted at one client but not yet on the other side. Maintaining a central cryptographic inventory makes it easier to monitor that the update is performed throughout the organisation simultaneously. Another part of cryptography management involves management of cryptographic keys and certificates. Tooling exists that enables to (partially) automatecreation, distribution and deprecation of cryptographic keys and certificates.

The next phase where cryptographic agility can be accounted for is during the development of systems using cryptography. In order to easily replace one cryptographic algorithm with another, calls to cryptographic functions insource code can be abstracted as much as possible. Furthermore, Continuous Integration/ Continuous (CI/CD) pipelines can be leveraged to test the cryptographic functionalities. This way, risks of incorrect usage of cryptography or compatibility issues can be spotted early on. Furthermore, this information can increase the performance of other tools for asset discovery as well.

Systems using cryptography can be built to support multiple algorithms simultaneously and letting other systems choose which algorithm to use for each connection. This can help the overall system be more agile and (backwards) compatible. On the other hand, this can also introduce new vulnerabilities such as downgrade attacks [NCSC-NL24].

Finally, cryptographic agility can be improved by taking into account the hardware requirements of (future) cryptographic algorithms. PQC will demand more capacity in terms of storage, bandwidth, etc. Therefore, it is important to assess whether the current hardware is suitable to run PQC in the future. If this is not the case, it is important to start thinking about alternative ways to either upgrade or replace the hardware. More information on the specific requirements for various PQC alternatives, we refer to Chapter 6.

Cryptographic agility in Processes

Next to technical solutions, cryptographic agility can and should also be enforced by including it in existing processes. Depending on the level of maturity of a system, organisational measures can also be easier to adopt compared to technical solutions, especially for systems that are already in use. By explicitly documenting cryptographic agility in processes, blind spots and bottlenecks in the process to update cryptography can be spotted more easily. Furthermore, processes increase alignment among involved stakeholders (both internally and externally) and can be preserved in case people leave. Ultimately, this leads to reduced errors in updates to cryptography and therefore reduced resources such as time and money required. Finally, by documenting the steps of cryptographic agility clearly while performing the process, a form of auditability is obtained which is also desirable for cryptographic agility.

To integrate cryptographic agility into processes, first the scope of the agility needs to be described. For example, what cryptographic agility form it is meant to achieve and when the process should start and end. This will also help identifying to which other processes it relates.

Common processes in which cryptographic agility can be taken into account are processes related to procurement, change management, development and releasing of software andincident response management. Cryptographic agility shouldbe taken into accountin procurement processes related to the purchasing of new soft- and hardware components. Cryptographic agility should be taken into account to ensure that the component can be updated appropriately in the future. Also, properly reviewing and testing the (claimed) agility features of a productis an important step for cryptographic agility. For hardware, it should either be capable of supporting different algorithms or parameters already, or be easily updateable in the future. Note that incorporating agility from the start of the lifecycle of a system is typically much easier than implementing it into existing systems. Therefore, these processes are particularly useful to include cryptographic agility. This also closely corresponds to cryptographic policies, which can mandate a certain level of agility for new products.

Next, processes related to development and releasing of software can increase cryptographic agility through testing. For example, the process should describe how and when cryptography can be tested to prevent compatibility issues or other vulnerabilities. Also, in case an update to cryptography needs to be performed, it should be described how this can be arranged smoothly as part of a software release.

Change management processes describe how organisations efficiently implement changes in the organisation. Such aprocess can for example describe why a change needs to happen, howit should be implemented and how the organisation can adaptto the change. For cryptographic agility, itisimportant to describe how an update or replacement ofcryptography needs be organised. For example, this can describe whoisresponsible for whatcryptography and how it should be ensured that the entire organisation makes the same changes to cryptography at the same time. People typically involvedin such a process are management or policy makers who needto approve a change to the cryptography or software developers/security architects who actually need to installor perform the update.

Finally, incident response processes describe how an organisation should response in case of an incident. For example, a process could describe what steps need to be taken in case a cryptographic key is compromised. Since response time is typically amajor consideration, describing steps related to cryptographicagility can helpto streamline the overall process. For example, continuously monitoring all cryptography in use at an organisation as part of a bigger risk assessment procedure will spot risks early on.Also in case an incident occurs, the process can help to identify whoisresponsible for what decisions and, for example, how acryptographic key should be deprecated quickly.

Cryptographic Agility in Policies

Finally, cryptographic agility should also be incorporated in policies surrounding cryptographic management. For a more thorough discussion on cryptographic policies, we refer to Section 2.3.1. A logical way to include cryptographic agility is by mandating technical and procedural measures for cryptographic agility, which is particularly applicable to new systems. Furthermore, a cryptographic policy could mandate updating a cryptographic inventory periodically and make persons responsible for cryptography management. For example, the policy could specify who is responsible for monitoring the security of the cryptography in use, or who needs to approve or perform an update in case this is desired. Furthermore, a cryptographic policy could specify how and when the processes in which cryptographic agility was included should be tested, to ensure they function correctly. Also in policies surrounding procurement, cryptographic agility can be taken into account.For example, vendors could be mandated to switch to new PQC algorithms within acertain timeframe after they are standardised.

Finally, a typical bottleneck in updating or replacing cryptography is that a cryptographic policy only allows for one algorithm or parameter set. Therefore when a migration to a new algorithm or parameter set needs to be performed, first the policy needs to be updated. A cryptographic policy should accommodate for this by allowing more options. On the other hand, organisations should be careful that their cryptographic policy does not contain outdated, obsolete choices for algorithms or parameters that are not secure anymore.

4.4.1 Forms of Cryptographic Agility

Based on the results of a cryptography workshop in 2019 [OPAB+19], the Dutch National Cyber Security Centre (NCSC) presented their vision on the different forms of cryptographic agility. Why organisations want cryptographic agility depends on their context. Carefully looking at what is required in which context helps to get a better grasp of what actually needs to be in place to achieve an adequate level of cryptographic agility with respect to the desired goals. In the remainder of this section, the different forms of crpytographic agility will be explained and common challenges that need to be overcome to reach them will be explained. For further discussion on the different ways to look at cryptographic agility, we refer to [ASWH+23].

Migration Agility

This is arguably the most well-known form of cryptographic agility. Its goal is to be able to replace one cryptographic algorithm with another. Therefore, this will be the main form of cryptographic agility that is required to migrate from quantum-valnerable cryptography to postquantum cryptography. Having this form of cryptographic agility is important *before*, *during* and *after* the migration to PQC has been performed as current and new algorithms will always need to be updated as they over time.

It is important to ensure that migration agility is implemented for every usage of a the algorithm for the service or application. Not updating the algorithm or its parameters everywhere can cause incompatibility issues when one side of the communication uses the new configuration while the other side still uses the old configuration. This is especially difficult if different instances of the algorithm are managed by different (external) entities. Next to that, not verifying that the algorithms has been updated throughout the organisation can introduce vulnerabilities because an attacker will simply attack the part where the old configuration is still in use.

Finally, hardware compatibility can be an obstacle for migration agility, since the hardware will for example need to be able to support larger keys or ciphertexts. Furthermore, current hardware acceleration could be incompatible with the new algorithm, making it much slower.

Measures to increase this form of cryptographic agility and mitigate the associated risks are implemented cryptographic asset management, abstracting the code responsible for the cryptographic operations so that it only needs to be changed in one location and having a proper view on and line of communication with internal and external dependencies. Furthermore, supporting multiple algorithms or parameter sets in an "OR" fashion can help remediating these (temporary) compatibility issues. However, this can also introduce the risk of downgrade attacks, when an attacker deliberately chooses a weaker algorithm to attack [NCSC-NL24]. Therefore, the supported algorithms should be monitored and removed once no longer necessary for compatibility or no longer secure.

Compliance Agility

This form of agility refers to cryptographic infrastructure that can easily be reconfigured to address different (regional) regulations simultaneously. In that case, there will multiple "versions" of the same system, each with a different cryptographic configuration. It is crucial to have a good inventory of what those configurations look like and where they are being used. In case this form of agility is desired to adapt the cryptography to changing regulations, it is similar in nature to migration agility with the added requirement that there is some form of monitoring in place to quickly recognise when a change in regulation is applicable to a certain piece of cryptography. For example, a country might mandate the usage of a new set of parameters for confidential information. Furthermore, where migration agility merely updates a system, with compliance agility different versions of the same system, adhering to different regulations, need to be functioning at the same time.

Implementation Agility

On an application level, instead of updating the cryptographic algorithm, the goal is to be able to replace the entire implementation of an algorithm. This can for example be the case if a new version of the implementation is released. Similar risks as for migration agility also hold for implementation agility. For example, compatibility- and dependency issues are also a challenge for this form of agility. Next to that, changing implementations typically requires going through more complex processes in organisations. For example, a company might have policies and/or continuous integration/ continuous delivery (CI/CD) solutions in place to test the software before it can be released. It is important to be aware of these processes and take their duration into account for the migration time. On the other hand, CI/CD solutions can also be a great opportunity to integrate automated testing of cryptographic implementations for known vulnerabilities or other errors.

Platform Agility

This form of agility refers to cryptographic algorithms seamlessly integrating with different platform types. This form of agility is mainly of interest for organisations actually supplying cryptographic implementations to customers. It entails that the same cryptographic algorithms should be able to run on many different devices, regardless of the hard- and software that it is being used on. Especially when running cryptography on certain devices, issues can arise when a new cryptographic algorithm does not fit on the existing hardware, and this hardware is difficult to replace. Also, some quantum-safe algorithms require more complex operations that can be hard to implement and run on these devices. It is advised to keep these considerations in mind.

Other Forms of Agility

Four other forms of cryptographic agility were identifiedin [OPAB+19] that are interesting but most likely note relevant for a majority of organisations. This can be because they are too advanced, specific or risky.
We only recommend to practice these forms of cryptographic agility if an organisation completely understands the cryptographic systems thatthey are building and really need these formsof agility. They are security strength agility, retirement agility, composability agility and context agility.

- Security strength agility refers to systems dynamically changing the security parameters of the cryptography based on the overall system configuration. This can save a lot of effort for organisations who continuously deploy their systemsin many different contexts with different demands. On the other hand, for (the majority of) organisations for which this is not the case, this form of agility might not be worth striving for.

- Composability agility refers to build cryptography in such a way that it can easily be composed with other cryptographic building blocks. This form of agility is particularly useful in the context of the PQC migration, where hybrid-AND compositions of cryptography are expected to be used as a temporary solution. However, we expect mainly the cryptographic experts who actually build the cryptography to be using this form of agility.
- Retirement agility refers to systems automatically retiring obsolete or insecure cryptographic algorithms.
- Finally, context agility refers to cryptographic systems that automatically derive from the context which algorithm and security strength should be used. For example, picking a stronger algorithm (version) based on the classification of the data to be encrypted. While this is a useful formofagility, there is arisk of picking insufficiently secure parameters on accident and therefore insufficient protection. For most organisations whodo not haveto upgrade security strength often anyways,it ismore safeto let humans make these decisions manually.

4.4.2 Choosing a Suitable Cryptographic Agility Strategy

While technical solutions, processes and policies are all important to help make a system more crypto-agile, incorporating cryptographic agility in other processes is expected to be easier for many organisations compared to technical- and policy solutions. On the other hand, technical solutions can be a very effective way to increase the speed of a cryptographic change while policies can be a good catalyst to enforce cryptographic agility.

Deciding on what measures are appropriate and how much cryptographic agility is required for a certain system or supply chain can be a challenging task. Nevertheless, it is possible to reason about the required speed of a cryptographic change based on the risk surface of an application, the persona of an organisation and the form of cryptographic agility that is desired.

For older systems that are already in use, technical solutions like abstracting calls to cryptography in code are hard to include in hindsight. For applications or products that are not yet used in production, we heavily recommend to investigate possibilities for including cryptographic agility solution into the design of the product or application. This can also be promoted by including these aspects into processes surrounding the purchasing of new systems. Note that the possibilities for including technical cryptographic agility solutions are also limited by overall maturity of the organisation itself. For example, automatically updating the parameters of a certain cryptographic algorithm can only be done if there is a proper, up-to-date cryptographic inventory available for the organisation.

However, for many forms of cryptographic agility and many organisations, some delay in changing or updating cryptography is perfectly fine, as long as the duration is guaranteed to a large extend. For example, an organisation requiring *compliance agility* in their product for release in another country does not need to be able to swap the cryptography within minutes. In fact, a product release could take weeks and thus being able to swap to new cryptography within a matter of weeks could be sufficient as long as the organisation is confident enough that there will not be any significant delays.

On the other hand, an organisation who wishes for migration agility to respond to newfound vulnerabilities in their cryptography to protect the personal data that they are handling needs to be able to respond much quicker and have more certainty of the delays.

All-in-all, evaluating the technical, process, and policy aspects of cryptographic agility and testing them will help in estimating whether its duration is acceptable or not. If the delay in a change to cryptography is unacceptable given the risk appetite and desired form of agility, an organisation does need to further investigate possibilities for improving the efficiency of the process.

5 Recent Developments

Summary

In this chapter, we review recent developments and ongoing efforts in the post-quantum migration process. We begin by discussing the current status of various standardisation initiatives, with a focus on the NIST standardisation process, which is the most advanced and comprehensive. We also examine legislation that mandates PQC migration, along with more flexible guidelines and recommendations provided to different agencies. The chapter concludes with insights and lessons learnt from previous migration efforts.

5.1 State of Different Standardisation Initiatives

Since the realisation that quantum computers threaten currently deployed cryptographic systems, there have been many efforts to mitigate this threat. Most of these efforts are consolidated through standardisation processes that enable us to specify algorithms capable of defending against quantum threats, test their security and efficiency, and provide guidelines on how these algorithms should be implemented and integrated into larger IT systems. This section provides an overview of different post-quantum standardisation initiatives. A short overview of post-quantum cryptography is presented in Section 6.3.1.

As the impact of a large-scale quantum computer on a symmetric cryptosystem is considered minor [NIST16c] (doubling the size of the keys should provide the same security as without quantum computers), we focus primarily on asymmetric cryptosystems, namely, Public-Key Encryption (PKE)/Key Encapsulation Mechanisms (KEM), and Digital Signature Algorithms (DSA). In the following subsection, we then summarise the NIST standardisation process, the largest standardisation effort on which most of the international cryptographic bodies rely, and provide some basic information about the current state of the process. We finish the section by providing basic information about other completed, ongoing, and in-preparation standardisation processes and related efforts.

5.1.1 NIST PQC Standardisation

In 2016, the National Institute of Standards and Technology (NIST) started the standardisation of Public-Key Encryption schemes (PKE)/Key Encapsulation Mechanisms (KEMs), and Digital Signatures aAlgorithms (DSA). After three major phases, which included public reviews and evaluation, in July 2022, NIST selected the following candidates to be standardised: a key encapsulation mechanism known as CRYSTALS-Kyber (now renamed to ML-KEM) and three digital signature algorithms, namely, CRYSTALS-Dilithium (renamed to ML-DSA), Falcon (renamed to FN-DSA) and SPHINCS+ (renamed to SLH-DSA). The first standards were released as Federal Information Processing Standards (FIPS) in August 2024 [NIST24a; NIST24b; NIST24c].

Name	Function	Hardness assumption	Standards
ML-KEM	PKE/KEM	structured lattices	[NIST24a]
ML-DSA	DSA	structured lattices	[NIST24b]
Falcon (FN-DSA)	DSA	structured lattices	not ready yet
SLH-DSA	DSA	stateless hash-based	[NIST24c]

Table 5.1 | Overview of algorithms selected by NIST for standardisation.

Four additional KEMs advanced to the fourth and final round with the intent to standardise one of them. As of May 2024, there are still 3 KEMs competing in this final round, namely Classic McEliece, Bike and HQC, all of them based on error-correcting codes. In order to diversify the hardness assumptions at the core of post-quantum cryptographic schemes, NIST opened an additional call specific for digital signatures, whose second-round candidates were revealed in October 2024. The following timeline represents the timeframe of the four rounds and the additional call in the NIST standardisation process, where the start of each call roughly corresponds to the time when the candidates were announced by NIST.

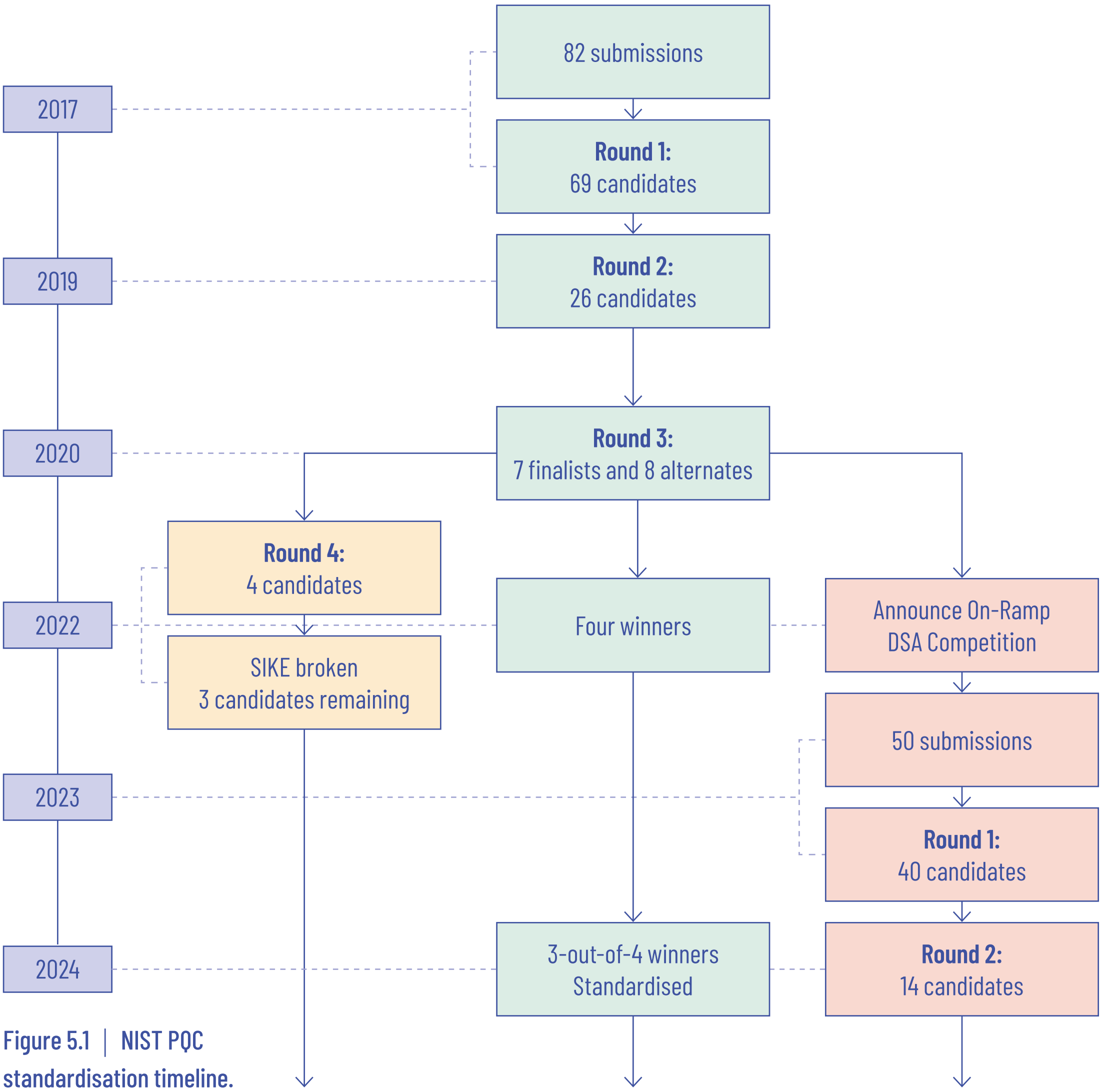


Figure 5.1 | NIST PQC standardisation timeline.

Standardisation of Stateful Hash-Based Digital Signatures | Ahead of the main PQC standardisation process described in this section, two post-quantum digital signatures had already been standardised by NIST in 2020 [NIST20a]. Their main particularity is that they require the signer to keep state of some one-time secret data which are not to be reused. Note that SLH-DSA [NIST24c] is *stateless*. For more details, please, refer to the end of this subsection where more details on stateful hash-based signature schemes are given.

Evaluation Criteria

The most important criterion for evaluating cryptographic schemes was the security. More precisely, the candidates were required to provably achieve strong security properties known as *IND-CCA2* (semantic security with respect to adaptative chosen ciphertext attacks) for key encapsulation mechanisms, and *EUF-CMA* (existential unforgeability with respect to adaptative chosen message attacks) for digital signatures. Beyond theoretical security, the candidates also needed to achieve some practical security with respect to known attacks. To this end, NIST provided 5 security strength categories which served as a new metric to compare the security of the cryptographic schemes. Each category was defined to provide similar security as well-analysed symmetric cryptographic schemes such as AES and collision-resistant hash functions. Eventually, the submissions mostly concentrated on levels 1, 3 and 5 which corresponded to AES-128, AES-192 and AES-256, respectively.

Beyond security, the candidates should also offer very good performances in terms of time and memory requirements to perform, comparable or even better than the quantum-vulnerable schemes, in order to facilitate their adoption.

The Standardisation Processes

Here we give a summary of the different phases of the selection of the standards.

Selection of the First Standards | The first round in which all the candidates that met both the submission requirements and the minimum acceptability criteria were evaluated. After feedback from the cryptographic community and following the above-mentioned evaluation criteria, NIST then chose candidates that continued to the second round. The second and third rounds were devoted to more thorough analysis and further experimental verification that eventually resulted in the candidates chosen for standardisation. More details about the first three rounds can be found in the NIST summaries of the rounds provided in [NIST19b], [NIST20b] and [NIST22].

The fourth round | After three rounds, one key encapsulation mechanism (ML-KEM [NIST24a]), as well as three digital signatures (ML-DSA [NIST24b], FN-DSA and SLH-DSA [NIST24c]) were considered mature enough and selected for standardisation.[1] However, three of those schemes are based on similar computational assumptions related to structured Euclidean lattices. In order to introduce more diversity in post-quantum standards, NIST also wants to select algorithms based on different hardness assumptions and four key encapsulation mechanisms moved forward into an extra fourth round, namely BIKE, Classic McEliece and HQC which are code-based, and SIKE, which is isogeny-based. Nevertheless, the latter suffered from a series of devastating attacks in the summer of 2023, starting with [CD23], and SIKE is not considered for standardisation anymore. The fourth round then consists in the three aforementioned code-based KEMs, at least one of them should be standardised by 2025.

Additional Call for Digital Signatures | In addition to the fourth round, NIST called for an additional round for digital signatures with a goal of introducing more general-purpose signature schemes that are not based on structured lattices as well as signature schemes that have short signatures and fast verification, which are relevant for certain applications. Even though the primary goal is to diversify signature schemes by intro-

[1] As of October 2024, the standard for FN-DSA has not yet been released.

ducing more variety in the underlying assumption of digital signatures, NIST stated that submissions that are based on structured lattices would still be considered if they significantly outperform ML-DSA and FN-DSA in pertinent applications and provide additional relevant security properties.

NIST SP 800-208 [NIST20a] LMS and XMSS(MT) stateful hash-based signature schemes | In October 2020, NIST opted to standardise two existing post-quantum signature schemes in NIST SP 800-208 LMS already standardised in IRTF RFC 8554 and XMSS already standardised in IRTF RFC 8391 [NIST20a; IETF19; IETF18]. These are the first two post-quantum schemes to have been standardised by NIST, ahead of the main PQC standardisation process described above. Their security is based on the hardness of finding hash function preimages, making them a conservative option for post-quantum security. They have been standardised for specific applications that 1) are long-lived, 2) can not wait for the main standardisation process and 3) are impractical to update in the field.
In contrast to SLH-DSA, these two schemes are stateful and require strict operational procedures to avoid reuse of state, as state reuse may directly facilitate forgeries. Therefore, NIST has specified in SP 800-208 that key material must be generated within a certified cryptographic module and is never allowed to be exported. Wiggers et al. have drafted a document to provide guidance for operational and technical aspects in state and backup management for LMS and XMSS(MT) [WBKG+24]. This includes solutions within the strict requirements set by NIST, as well as outside.

5.1.2 Other Standardisation Efforts

Apart from the NIST standardisation process, there were other standardisation efforts that eventually resulted or will result in new cryptographic standards. Most of these, however, were a lot smaller in scope and some of them were focused only on specific domains. Here we list some of the recently finished and ongoing post-quantum standardisation processes and comment on processes in preparation. For some of these, we just mention their existence but do not go into further details due to a lack of fairly accessible documentation.

International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) | ISO (International Organisation for Standardisation) and IEC (International Electrotechnical Commission) are non-governmental, international organisations which develop standards across virtually all industries. In particular, they created a joint technical committee (JTC 1) entitled Information Technology to specifically target information and communications technology standards. In preparation for the post-quantum migration, they conjointly released a document describing the need for post-quantum migration and mathematical problems that are presumed to underline future post-quantum standards. As part of ISO/IEC 14888 series, they have already standardised stateful hash-based signatures in ISO 14888-4 [ISO24], including LMS, XMSS, HSS, and XMSS-MT. Moreover, ISO/IEC JTC1 is developing a PQC amendment to ISO/IEC 18033-2 [ISO06]. This has not officially been released yet, but beyond NIST standards, it is expected that ISO/IEC also standardise the key encapsulation mechanisms FrodoKEM [ABDL+21] and Classic McEliece [ABCC+20], which are considered to be more conservative than their structured lattice-based analogue ML-KEM.
Beside their standardisation effort, ISO works closely with other international organisations such as the International Accreditation Forum (IAF) which provide certifications that some products are compliant with ISO standards through careful audits. This increases the confidence customers can have in products and services, and for some industries such certifications are even contractual requirements. As a result, ISO standards can be considered even more important than NIST standards in industrial environments.

Internet Engineering Task Force (IETF) | The Internet Engineering Task Force (IETF) is a globally recognised organisation specifically responsible for the development of standards for the Internet through so-called Requests For Comments (RFCs). The particularity of IETF is that it is a completely open process with public mailing lists and meetings. Although the status of post-quantum cryptography at the IETF is still at the level of internet-drafts (no RFC has been released yet), it is very active and in particular a specific working group called *Post-Quantum Use In Protocols* (PQUIP)[2] has been established on an experimental basis by the Internet Engineering Steering Group (IESG) to coordinate the development of the PQC standards. IESG intends to review it by 2025, when the first RFCs are expected to be officially released. To this aim, PQUIP is working closely with the Cryptographic Forum Research Group (CFRG),[3] which release RFCs describing the different cryptographic standards, as well as with more specific working groups such as LAMPS,[4] focusing on secure email communication, IPSECME,[5] involved in integrating post-quantum cryptography into the IPsec suite of protocols widely used in VPNs, COSE,[6] dedicated at developing standards for securing data objects using *Concise Binary Object Representation* (CBOR), or the TLS[7] and ACME[8] working groups respectively in charge of standardising the Transport Layer Security protocol, and specifying conventions for automated certificate managements. The status of post-quantum integration can be found on https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc.

Beyond that, the PQUIP working group is involved in a guide providing an overview to engineers of the post-quantum landscape (from threats to algorithms). The current draft of this document is available at https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/. It can be read as a complement to this handbook, but is not a replacement. For example, the PQUIP document does not provide a clear timeline on when to start the actual migration, which we do in Chapter 2, and our Section 4.4 on cryptographic agility is more complete.

European Telecommunications Standards Institute (ETSI) | ETSI is an independent, non-profit standards organisation based in Europe. It is recognised by the European Union as one of the main standardisation bodies for telecommunications. Regarding post-quantum cryptography, ETSI is primarily focused on supporting implementations of algorithms standardised by NIST rather than standardising the algorithms themselves. In July 2020, ETSI published a guideline for post-quantum migration [ETSI20a]. More recent reports by their technical committee CYBER focus on concrete advice on the use of quantum-safe hybrid key exchange [ETSI20b] and provide technical descriptions of public-key encryption/key encapsulation mechanisms [ETSI21a], and digital signatures [ETSI21b] submitted to the third round of NIST standardisation process.

Korean Post-Quantum Cryptography (KpqC) | The first round of a competition by the Korean post-quantum cryptography research centre started in November 2022. After a year of evaluation, the team announced four public-key encryption/key encapsulation mechanisms and four digital signatures that will proceed to the next round, where their security and efficiency will be further assessed. Among the four digital signatures that are being evaluated in the second round, there are two lattice-based schemes, one scheme based on multivariate polynomials and one symmetric-based scheme. Among the four key encapsulation/encryption mechanisms that are in the second round, there is two lattice-based and two code-based candidates.[9] The exact timeline for the standardisation process is not clear yet but the South Korean government plans to transform its national cryptography systems to post-quantum cryptography by 2035.

[2] https://datatracker.ietf.org/wg/pquip/about/
[3] https://datatracker.ietf.org/rg/cfrg/about/
[4] https://datatracker.ietf.org/wg/lamps/about/
[5] https://datatracker.ietf.org/group/ipsecme/about/
[6] https://datatracker.ietf.org/wg/cose/about/
[7] https://datatracker.ietf.org/group/tls/about/
[8] https://datatracker.ietf.org/wg/acme/about/
[9] Interestingly, two third-round signatures from KpqC, namely, AIMer and HAETAE, are also submitted to the NIST additional call for signatures.

Chinese Association for Cryptologic Research (CACR) | In 2018, CACR started a competition for symmetric and asymmetric cryptographic algorithms. After two rounds, CACR announced the winners of the competition in January 2020. Multiple algorithms are selected as the first, second, and third rank candidates. The outcome of this competition is slightly different from the NIST standardisation process as CACR is not a standardisation body but rather a research organisation. The goal of this competition thus was not to standardise new schemes but rather to encourage new designs of post-quantum schemes that may be standardised in the future.

Domain Specific Standards | In October 2010, the American National Standards Institute (ANSI) standardised a scheme based on a structured lattice problem with the intention to use it primarily for the US financial industry. The initially standardised scheme was later improved, by replacing its weak parameters and thus reaching the desired security level, and the standard was updated in February 2017. The details of it can be found in [ANSI10]. In February 2024, the Global System for Mobile Communications Association (GSMA) announced [GSMA24] that provides guidelines for post-quantum migration for different use cases in mobile communications.

5.2) Post-Quantum Cryptography and Legislation

Standardised cryptographic algorithms are much more likely to be deployed in practice. In fact, it is in general recommended to deploy only standardised algorithms. However, (cryptographic) standards are not inherently mandatory and, unless additional regulations are in place, organisations may choose to disregard them. By contrast, appropriate legislation creates a strong incentive for organisations to commence the migration to post-quantum cryptography. They establish legal obligations and allow organisations to be held accountable for their cryptographic decisions.

The importance of regulating cyber security measures, and thus the deployment of cryptography, has been clearly demonstrated. For one reason, migrating cryptography is a time-consuming and expensive undertaking, whose benefits may not show immediately, especially since the quantum threat will only manifest in the future. Therefore, organisations may prioritise short-term profits over long-term cyber risk mitigation. Investing in post-quantum cryptography could even put an organisation in a competitive disadvantage. Regulating the appropriate deployment of cryptography ensures a level playing field, forcing all organisations to deploy the same or similar measures. Moreover, legislation aims to protect smaller organisations that do not have the in-house knowledge on the latest cryptographic threats.

The importance of legislation is further emphasized by the fact that cryptography oftentimes protects public goods, such as national security, public safety and privacy. In these situations, the market may not create sufficient incentives for deploying appropriate cryptographic measures. Additionally, legislation enables a consistent deployment of standards; without legislation organisations may make inconsistent choices, limiting interoperability and auditability.

This section provides some examples of legislation prescribing the use of cryptography. These examples demonstrate how the use of post-quantum cryptography will be mandated more and more. This overview is far from complete and we advise organisations to inventory the relevant regulatory bodies and legislations in their region and sector. In general, legislation mandates the deployment of standardised, and well-understood, cryptographic algorithms. For instance, referring to FIPS or ISO standards. Since PQC standards are still young or even under development, this explains why legislation explicitly requiring the use of post-quantum cryptography is still scarce. However, it is expected that while more standards are being finalised, legislation will soon follow and start to deprecate the older cryptographic standards not capable of protecting against quantum adversaries. For this reason, it is important to keep track of the legislative developments.

5.2.1 ISO/IEC 27000-Series

The ISO/IEC 27000-series is perhaps the best known set of international cyber security standards, aiming to ensure robust information security management processes. This set of standards is adopted globally in many different sectors and formally by multiple governments and organisations. Adhering to the ISO/IEC 27000-series is not inherently mandatory, but it is widely regarded as a best practice. Moreover, in some sectors regulatory bodies may require compliance with these standards. These standards do not provide technical cryptographic requirements, but they do specify the need for cryptographic policies and controls, and the deployment of appropriate cryptographic techniques based on a risk assessment. More detailed guidelines and specifications with respect to cryptography can be found in other ISO/IEC standards and guidelines. For instance, ISO/IEC 18033 specifies a set of standardised primitives that can be used within these cryptographic policies. Currently, this standard does not yet provide post-quantum public-key primitives. However, the working group ISO/IEC JTC 1 SC27 WG2 is currently developing a post-quantum amendment to ISO/IEC 18033.

5.2.2 Network and Information Systems (NIS) Directive

The Network and Information Systems (NIS) directive [EU16a] provides legislation aiming to achieve a high level of cyber security in the European Union member states. In 2018, it came into force and, in 2023, it was replaced by its successor the NIS2 directive [EU22a]. NIS2 specifies 18 sectors and all mid-size to large EU companies in these sectors must comply with this legislation. The scope of NIS2 directive reaches far beyond cryptography, and it does not provide detailed or specific requirements on the use of cryptography. However, NIS2 does specify the obligation to deploy proportional cryptographic measures, taking into account both an organisation's exposure to risks and the state-of-the-art in cryptography.

5.2.3 General Data Protection Regulation (GDPR)

The GDPR [EU16b] is a comprehensive legislation mandating the protection privacy and personal information of EU citizens. The Data Protection Authorities in the different EU member states are responsible for monitoring GDPR compliance. Failing to comply with the GDPR may result in significant fines. Since the GDPR came into force in 2018, various fines have already been imposed. The GDPR does not prescribe the use of specific cryptographic algorithms, but it does imply the use of cryptography while "taking into account the state of the art" (Article 32).

5.2.4 Federal Information Security Modernization Act (FISMA)

The Federal Information Security Modernization Act (FISMA) [Uni02] mandates United States federal agencies, and their contractors, to deploy a range of cyber security measures. FISMA delegates the specification of cryptographic algorithms to the US National Institute for Standards and Technology (NIST). More precisely, to comply with FISMA, cryptography standardised by NIST, in Federal Information Processing Standards (FIPS), must be used. FIPS standards already cover a wide range of cryptographic algorithms, and recently new PQC FIPS standards have been added as a result of the NIST PQC competition. Separate higher level FIPS standards subsequently specify which cryptographic algorithms are approved, referring to the corresponding FIPS-standards of these algorithms. The above clearly displays the modular nature of this US legislation.

5.2.5 United States White House Memorandum

Already in 2022, the US White House issued a memorandum [US22] describing the administration's policy with respect to quantum computing, focussing both on the risks and the opportunities of quantum technology. This memorandum defines concrete actions for US government agencies to ensure a timely mitigation of the quantum threat. For instance, it describes the establishment of different (industry) working groups and new PQC migration projects. Hence, while it does not mandate the deployment of specific cryptographic algorithms, this memorandum does require many US organisations to commence the PQC migration. In July 2024, the White House Office of Management and Budget (OMB) released a strategy for transitioning federal information systems to PQC, in line with the memorandum. Within a year of NIST adopting the first PQC standards (approximately one year from the present moment), the OMB will issue guidance, in coordination with Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), NIST, and the Office of the National Cyber Director (ONCD), instructing agencies to develop a PQC migration plan and prioritise it.

5.2.6 Commercial National Security Algorithm Suite (CNSA)

In the Commercial National Security Algorithm Suite (CNSA) [NSA21a], the United States National Security Agency (NSA) requires a specific set of cryptographic algorithms to be used for protecting US national security systems (NSS). These requirements refer to NIST's FIPS standards. In 2022, the CNSA 2.0 was published, notifying NSS owners, operators and vendors about the future cryptographic requirements. In particular, CNSA 2.0 specifies four quantum-resistant public-key algorithms - CRYSTALS-Kyber, CRYSTALS-Dilithiumn, (now standardised as ML-KEM and ML-DSA), XMSS and LSS - and announces that their deployment will be mandatory. More precisely, CNSA 2.0 defines a transition period. Depending on the cryptographic application, either in 2030 or in 2033 compliance with CNSA 2.0, and thus the deployment of PQC, will be mandatory. Until then, CNSA 2.0 compliance will first be optional and later become preferred.

5.2.7 Sector Specific Legislation

In addition to generic regulatory framework, many sectors have specific legislation tailored to their requirements. For instance, the Digital Operational Resilience Act (DORA) [EU22b] aims to achieve a high level of operational resilience in financial sector of the European Union. DORA requires financial institutes to deploy "leading practices and standards" in cryptography, and thus it will soon (implicitly) require the use of post-quantum cryptography. In the US, the Health Insurance Portability and Accountability Act (HIPAA) [US96] mandates the health care industry to safeguard patient records, for instance by deploying appropriate cryptographic techniques. As a final example, the European Electronic Communications Code (EECC) [EU18] regulates electronic communication networks in the EU and, for instance, requires the use of strong cryptography to minimise the impact of security incidents.

5.3) International PQC Guidelines and Advice

Less legally binding, some international organisations have also provided some guidelines for a successful deployment of post-quantum cryptography.

5.3.1 European Commission

On 11 April 2024, the European Commission issued a comprehensive set of recommendations [EU24] to its member states regarding the transition to post-quantum cryptography. Although these are only recommendations, they make explicit reference to the NIS2 directive (see Section 5.2.2), underscoring the crucial role of post-quantum cryptography in achieving a high level of cyber security across the EU. The recommendation encourages member states to coordinate their efforts in migrating to PQC and to work together to develop a detailed, unified roadmap.

The Commission has not yet endorsed specific post-quantum algorithms but is advocating for the development of standards at the European Union level, alongside a thorough analysis of these algorithms. For the practical transition phase, it recommends adopting hybrid cryptographic solutions, which combine post-quantum algorithms with those currently in use. Additionally, the Commission has not ruled out Quantum Key Distribution (QKD) as a possible solution, even though many member states' security agencies deem QKD insufficiently mature and advise against its adoption.

5.3.2 Germany, France and The Netherlands

Several EU member states have provided specific guidelines on the transition to post-quantum cryptography through their different national cybersecurity agencies. In particular, while Germany [BSI24b], France [ANSSI23] and The Netherlands [NCSC-NL23; Fiche24] each have their nuances, they generally agree with the recommendations of the European Commission and support the use of hybrid cryptographic solutions. The situation is easier for digital signatures than for key encapsulation, since it is enough to provide signatures with two different algorithms and accept the signature if and only if they are both valid. Nevertheless, contrary to the EU Commission, they all have reservations about the maturity of QKD as a viable solution at this stage to mitigate the quantum threat.

Specific Algorithms | All three agencies present security as the main criterion for selecting post-quantum algorithms. In particular, even though they will consider those standardised by NIST (ML-KEM [NIST24a], ML-DSA [NIST24b] and SLH-DSA [NIST24c]), they give warnings about the difficulty to securely implement FN-DSA such that it provides a protection against side-channel attacks and therefore do not recommend using this algorithm. Additionally, they advocate for two other KEMs: *FrodoKEM* [ABDL+21] and *Classic McEliece* [ABCC+20]. Indeed, the former can be regarded as a variant of ML-KEM, which does not rely on an algebraic structure, and the latter is a direct adaptation of an original cryptosystem by McEliece [McE78] which makes it the oldest cryptosystem currently unbroken. These characteristics make these two algorithms more conservative than the NIST standards and the respective agencies are very confident in their security.

Conservative Sets of Parameters | When deploying post-quantum cryptography, all agencies agree that only the most conservative parameters which have been standardised by an external organisation should be used. In particular, they advocate for using the parameters which belong to security categories 3 and 5 for the NIST standards, and encourage waiting for the future ISO/IEC and IETF standards regarding FrodoKEM and Classic McEliece. This security concern also aligns with NIST that considers that the parameters corresponding to security category 3 should be used by default for ML-KEM [NIST24a, Section 8].

Adaptability and Crypto-Agility | All three agencies stress that the PQC migration roadmaps should remain adaptable to novel (technological) developments. In particular, the Dutch fiche [Fiche24] emphasizes the importance of investing in research and innovation and all three agencies insist on the development of crypto-agility to ease the transition from a particular cryptographic algorithm to another.

Timeline | A specificity of the report from ANSSI is that it also gives a timeline for the deployment of quantum-resistant cryptography:

- **Step 1 (Up to 2025)** The most critical organisations, which correspond to what we refer to as *urgent adopters* in Chapter 2, should start their migration by enhancing their cryptoagility. Post-quantum cryptography is still optional, but when used it should be used inside a hybrid system with cryptographic algorithms already deployed.
- **Step 2 (From 2025 to 2030)** Post-quantum security must be seen as a major priority by industries, which should define a clear migration strategy of their transition, starting from creating an inventory of their cryptographic assets (see Section 2.2.1). However, novel post-quantum cryptography should be deployed in a hybrid combination with another more established but quantum-vulnerable cryptosystem. ANSSI will start to provide certifications that products comply with these guidelines.
- **Step 3 (Starting from 2030)** ANSSI expects that by 2030, post-quantum algorithms will be more reliable and that their security will be better understood. In particular, if this is the case, it will be possible to use post-quantum cryptography as a standalone replacement to current cryptography, which will make them more efficient than with hybridisation.

Implementation | Beyond its recommendations, Germany's BSI also provides *Botan*, an Open Source Cryptographic Library written in C++ and available on Github.[10] Botan provides a wide range of cryptographic algorithms and protocols, supporting both quantum-vulnerable and post-quantum cryptography, and respecting their guidelines.

5.3.3 The United Kingdom

The UK National Cyber Security Centre (UK-NCSC) is a cybersecurity agency of the United Kingdom, and it acts as part of a larger intelligence and security organisation known as GCHQ (Government Communications Headquarters). In their white paper from 2020 [NCSC-UK20a], UK-NCSC recognises large-scale quantum computers as a threat to long-term cryptographic security, especially in the context of "harvest now, decrypt later" attacks that would enable a malicious party to decrypt a sensitive data in the future, when large-scale quantum computers might be developed. As BSI and ANSSI, they advise migration to quantum-safe algorithms as soon as feasible (as stressed out in their reports on cyber security strategies [NCSC-UK22]), but they discourage migration to algorithms that have not been standardised.

On Standards | In their white paper from 2023, [NCSC-UK23], UK-NCSC aligns with NIST standardisation and recommends using ML-KEM as a general purpose PKE/KEM and ML-DSA as a general purpose digital signature algorithm. For specific use cases, such as signing firmware and software, where the speed is not a major concern, they recommended using SLH-DSA (SPHINCS+) also standardised by NIST or stateful hash-based signatures Leighton-Micali Signatures (LMS) and eXtended Merkle Signature Scheme (XMSS). The latter two are recommended to use only when it is possible to manage state in a trusted manner for the lifetime of the signing key.

[10] https://github.com/randombit/botan

On Hybrids | In the first whitepaper from 2020, UK-NCSC implicitly supported hybrid constructions, namely, schemes that combine previously used algorithms with the post-quantum one, as these would enable a smoother transition to quantum-safe cryptography. Nevertheless, UK-NCSC highlights that using hybrid schemes is not an ideal solution due to the costs of their implementation, complexity, and lack of efficiency. Their stands are, therefore, that hybrid schemes should be used only when their application is necessary, more precisely, when the algorithm being replaced is part of a larger and very complex system, when a system requires a high level of security (for example, protects sensitive data) and when it is hard to remove traditional public-key algorithms. But, even in these cases, the organisations should eventually aim for fully post-quantum algorithms since hybrid schemes would provide no additional protection from a large-scale quantum computer and it would only introduce an overhead in implementation.

On QKD | In both the white paper from 2023 and their blog post from the same year, UK-NCSC expresses their opinion that using quantum-key distribution (QKD)[11] for key establishment is not the most efficient and secure measure to take as it requires hardware that is still under development. Hence, UK-NCSC does not encourage using QKD for sensitive data protection.

On Protocols and Services Migration | UK-NCSC remarks that, as part of the transition to the new post-quantum algorithms, protocols and services relying on these protocols will need to be re-engineered to accommodate for higher demands imposed by the deployed algorithms. UK-NCSC foresees that the major challenges in the PQC transition will be legacy that is hard to upgrade, sector-specific protocols and protocols running on devices with constrained resources. They remark, however, that for many use cases, the transition could be done "silently" through software updates and they encourage this approach when it is possible to have it.

5.4) Lessons Learnt from Executed PQC Migrations

Some organisations and maintainers of well-known software have already initiated a migration to post-quantum cryptography. In this section we give an overview of real-world experiences, describing the challenges that were faced and the lessons which have been learnt.

5.4.1 Google's Post-Quantum Migrations

Google has been a pioneer in integrating post-quantum cryptography into its internal infrastructure. Their migration process began even before NIST announced the initial algorithms for standardisation. As a result, their experiment serves as a significant example of a successful migration to post-quantum cryptography.
Google's internal communications are secured using a custom protocol known as ALTS (Application Layer Transport Security) [Google17]. ALTS is a mutual authentication and transport encryption system similar to mTLS (mutual Transport Layer Security) that is fully developed by Google to meet their specific needs. To upgrade ALTS to a post-quantum version, Google opted for *hybrid encryption* to mitigate security risks in case of any issues. Based on prior experiments, they chose NTRU-HRSS [HRSS17] as their primary post-quantum encryption scheme, with plans to switch to ML-KEM once standards are finalised. This should not offer a significant challenge since they aimed to remain as *agile* as possible. For more details, see [Google22b].
The migration to post-quantum ALTS was discussed at Real World Crypto 2023 [KPMS23], and was facilitated by Google's complete control over both server and client implementations of the protocol. However, incorporating the post-quantum layer presented several challenges. In particular, the use of ephemeral public

[11] Quantum-key distribution (QKD) uses properties of quantum mechanics instead of computationally hard mathematical problems to guarantee security.

keys in the ALTS protocol required generating fresh keys for each sessions, which is costly, especially if the server had not yet migrated. Therefore, they considered caching the public key to mitigate this issue. Unfortunately, this approach caused problems with key sizes, resulting in unexpected stack overflows on certain architectures. To address this, they moved the key to the heap, but this introduced latency issues not foreseen during initial benchmarks. Indeed, these latency problems arose from allocation time when thousands of post-quantum sessions were initiated, requireing protocol updates.

In summary, Google's experience highlights that migrating to post-quantum cryptography is a lengthy process requiring extensive testing in various scenarios due to unexpected issues.

5.4.2 Post-Quantum TLS at Google and Cloudflare

The TLS (*Transport Layer security*) protocol is one of the cornerstone protocols of the world-wide web, securing practically every connection between computers over the internet. Typically, TLS serves two purposes; authentication and encryption. Authentication is used to ensure that a user can verify they are talking to the right server by means of a digital signature in the form of a certificate. Encryption is used to ensure that the information sent from client to server and vice versa remains confidential. For this, the protocol first sets up a symmetric key in a secure manner using a key exchange protocol based on asymmetric cryptography after which symmetric cryptography is used to encrypt the remainder of the conversation.

TLS 1.3 [Res18] is the latest version of the TLS protocol, released in August 2018, coming with many security and performance improvements compared to version 1.2. However, TLS 1.3 was created without specific attention for PQC and integrating post-quantum algorithms raises certain challenges that need to be overcome. This is especially true when one wants to consider both confidentiality (by modifying the key exchange), and authentication (by using quantum-safe digital signatures), but they can be dealt with separately.

Early experiments with designing quantum safe variants of the TLS 1.3 key exchange mechanism include the CRPQ2 (*Combined Elliptic-Curve and Post-Quantum*) project, led conjointly by Google and Cloudflare in 2019 [VK19]. More precisely, they considered a *hybrid* key exchange using X25519 together with either the lattice-based NTRU-HRSS [HRSS17], or with SIKE [JACC+21] for the variant CRPQ2b. Note that SIKE is known not to be secure anymore, however since they were using a hybrid key exchange, the CRPQ2b did not yield security losses compared to the current deployment of TLS 1.3. Since then, NTRU-HRSS has been replaced by the draft of ML-KEM (see [OBr23; AVW23]). In this experiment, Cloudflare implemented the server side, while Google added support for hybrid KEMs in their own browser Chrome.[12] Since lattice-based KEMs are in general extremely fast, the computational overhead of using quantum-safe algorithms was almost not noticeable. However, some messages in the TLS protocol, namely the ClientHello and the ServerHello, also include the public keys as well as the ciphertext, which may collectively exceed the Maximum Transmission Unit (MTU), i.e., the maximum packet size which can be sent across the network, which is generally set to 1400 bytes. In this situation, the handshake messages necessitate to be divided over multiple TCP packets, increasing the risk of packet loss and potentially introducing latency issues when packets require retransmission. The TLS standard allows for the packets to be split this way, however, since this was extremely rare in a pre-quantum world, many clients and servers are not properly implemented and ignore subsequent packets, yielding unexpected abortion of the protocol. In particular, extensive tests are still needed to track those bad implementations and make sure vendors fix them. The IETF is currently working on a standardisation of hybrid key exchanges in TLS 1.3 [IETF24].

This issue with the sizes can be even more problematic when taking quantum-safe authentication into account. In general, many signatures and public keys are included into a single handshake. Even though the TLS 1.3 standard allows for a certificate chain of 16 MB, in practice many devices would reject much shorter chains. In this situation, Cloudflare argues that the adoption of quantum-safe authentication would be made easier if 6 signatures, as well as 2 public keys, would fit in 9kB [Wes21].

[12] Mozilla added support for hybrid KEMs in the version 123 of Firefox in early 2024.

In order to mitigate this, other solutions are also explored. For example, it has been suggested to remove intermediate certificates [KSFH+20], or even to replace some signatures by key exchange mechanisms [SSW20] to get a new variant known as KEMTLS. However, all those proposals require changing the protocol, which would take many years to be adopted, and no consensus has been reached as of August 2024. The interested reader can find more information about this KEMTLS variant and Cloudflare experiments with it in [CW21].

5.4.3 Post-Quantum TLS at Meta

Meta has also been active in the post-quantum cryptography migration, having contributed to the BIKE [ABBB+21] and Classic McEliece [ABCC+20] submissions to NIST. Similar to Google, they first opted to migrate their internal communication traffic noticing that their control of all endpoints as well as the susceptibility to store-now-decrypt later-attacks were the primary reasons why this is a suitable first test [LTAN+24] . Concretely, they opted for a hybrid approach, using Kyber (now standardised as ML-KEM) in hybrid with an elliptic-curve key exchange (X25519).

They implemented hybrid key exchange in their own, open-source TLS library called Fizz [Meta24]. For PQC, they used the open-source liboqs [SM16] library, which implements the Kyber mechanism. Their original plan was to set ML-KEM-768 (corresponding to NIST level 3) as the default choice for key exchange. However, after experiencing similar issues with the ClientHello not fitting in one packet and looking into various workarounds, they defaulted back to the smaller parameter set of ML-KEM-512, which corresponds to security category 1.

Furthermore, they encountered crashes in liboqs after rolling out hybrid key exchange to their internal communication. The crash was caused by multithreading, highlighting the need to properly test implementations as well before relying on them.

5.4.4 Post-quantum Cryptography in Messaging Applications

Signal | The Signal Protocol [Mar13; MP16] is a cryptographic protocol which provides end-to-end encryption for voice and instant text messages. It was developed since 2013 for the Signal messaging application, and has since been incorporated into many other secure messaging applications such as WhatsApp [Wha16] and Google Messages for Android [Google22a]. In particular, it is one of the most widely adopted instant messaging protocol in the world, used everyday by billions of people [Mil24]. Its security relies, among other things, on a key exchange protocol known as X3DH (triple DiffieHellman) [MP16]. In September 2023, Signal announced that a post-quantum variant known as PQXDH [Signal24b] had been incorporated into the Signal Messaging Application [Signal24a]. This quantum-safe variant adds support for a hybrid key exchange mechanism. In the documentation, the choice of the algorithm is let free to the implementer, although Signal mentioned that they used ML-KEM themselves. Since they controlled all endpoints of the protocol for their messaging application, they did not face any specific implementation challenges. However, soon after the release of this protocol, it has undergone formal verification (see [BJKS24]) which put forth new attacks on the hybrid key exchange on early versions of PQXDH. This resulted in modifications of the protocol.

iMessage | iMessage is the main instant messaging application developed by Apple, and exclusively deployed on their platforms. It is similar to the aforementioned Signal protocol, but uses different design for the key exchange phase, which offers different challenges. In February 2024, Apple enhanced iMessage with the introduction of the PQ3 protocol, enabling post-quantum security via the ML-KEM algorithm [Jac24; Apple24]. This protocol has also recently been formally verified [BLS24].

5.4.5 Wrapping-Up Lessons Learnt

These real-world examples demonstrate that hybrid key exchanges are viable solutions, making it theoretically easy to achieve post-quantum confidentiality. However, implementing this in practice presents many challenges that need to be overcome. The larger size of public keys can increase computation time due to the memory allocation, or even cause memory issues on constrained environments. Extensive testing on different architectures is necessary to identify these issues before the post-quantum variants can be used in production. This process is simpler when all endpoints are controlled by a single entity (e.g., for internal migration). Nevertheless, as shown by the formal verifications, using hybrid key exchange can also lead to new attacks, and some further checks need to be performed, although those do not necessarily pose technical difficulties.

On the other hand, achieving post-quantum authentication is more challenging. Current post-quantum signatures tend to have larger signatures and/or slower verification time, which can lead to efficiency issues and make the migration less appealing. This is particularly problematic for the Web public key infrastructure, which relies on chains of certificates. While some ideas have been proposed to improve the protocols, those changes in the core of the protocols will require a consensus and take more time before the migration can be done. The new call by NIST specifically for post-quantum signatures will be of utmost important for this application.

On a positive note, there are scenarios where post-quantum signatures might be easily deployed, such as hardware root of trust systems such as *Trusted Platform Modules* (TPM). Here, a public key is directly burned in silicon, and signatures are verified for firmware updates. This is particularly suited for Internet of Things (IoT) devices, and may enable long term quantum-safe hardware.

6) Background on Primitives

Summary

The goal of this chapter is to aid library developers in selecting various primitives to include in their libraries and to help organisations understand which primitives to choose and how to configure them when migrating to a quantum-safe version of a protocol. It is also intended to aid asset discovery and risk assessments. Because of the intended audience and the information to be discussed, a reasonable amount of cryptographic background knowledge is assumed in this chapter.

We provide a list of the main cryptographic primitives in use. For each primitive, we present their main characteristics and whether or not they provide quantum security.

Table 6.1 shows the list of cryptographic primitives that are commonly used. This is not an exhaustive list, and it is imperative that any other cipher and cryptographic algorithm in use in the organisation is appropriately noted.

Symmetric	Asymmetric	Hash Functions	MAC	Stateful HBS
AES	RSA	SHA-2	HMAC	XMSS
ChaCha20	ECDH	SHA-3	CMAC	XMSS^{MT}
	ECDSA	Blake	BLAKE2-MAC	LMS
	EdDSA		CBC-MAC	HSS

Table 6.1 | Commonly used cryptographic primitives.

6.1) Quantum-Vulnerable Asymmetric Cryptography

In this section we list some asymmetric cryptography that is commonly used but vulnerable to a quantum computer.

ECDH

Description | ECDH is an elliptic curve variant of the Diffie-Hellman key exchange [NIST19a].

Public-Key Sizes (bits) | Depends on the curve used. For example, using NIST P-256P results in a 512-bit uncompressed public-key.

Private-Key Sizes (bits) | Depends on the curve used. For example, using NIST P-256P results in a 256-bit private-key.

Ciphertext Size (bits) | Double the length of the private-key.

Hardness Assumption | Decisional Diffie Hellman.

Crypto Functionality | ECDH is used for key exchange.

Applications | ECDH is incorporated into protocols that require key exchange.

Further Comments | ECDH is used in the Signal Protocol.

Standardisation Documents | NIST, SP, 800-56A [NIST19a] rev. 3, ANSI X9.63 [ANSI17a], SECG SEC-1 [Bro09].

Quantum-safe? | No.

ECDSA

Description | ECDSA is an elliptic curve variant of the Digital Signature Algorithm standardised by NIST [NIST23].

Public-Key Sizes (bits) | This depends on the curve used. For example, using NIST P-256P results in a 512-bit uncompressed public-key.

Private-Key Sizes (bits) | This depends on the curve used. For example, using NIST P-256P results in a 256-bit private-key.

Signature Size (bits) | Double the length of the private-key.

Hardness Assumption | Discrete Logarithm.

Crypto Functionality | ECDSA is used for digital signatures.

Applications | ECDSA is used in a wide range of both software and hardware domains.

Further Comments | ECDSA is one of the *de facto* standards for digital signatures.

Standardisation Documents | FIPS 186-5 [NIST23], ANSI X9.63 [ANSI17a], ANSI X9.142 [ANSI20], ISO/IEC 14888-32018 [ISO18b], SECG SEC-1 [Bro09].

Quantum-safe? | No.

EdDSA

Description | EdDSA is an elliptic curve variant of the Digital Signature Algorithm standardised by NIST. In EdDSA, twisted Edwards curves are used, such as Curve25519 [JL17].

Public-Key Sizes (bits) | This depends on the curve used. For example, using Curve25519 results in a 512-bit uncompressed public-key.

Private-Key Sizes (bits) | This depends on the curve used. For example, using Curve2559 results in a 256-bit private-key.

Signature Size (bits) | Double the length of the private-key.

Hardness Assumption | Discrete Logarithm.

Crypto Functionality | EdDSA is used for digital signatures.

Applications | EdDSA is suitable for general use.

Further Comments | EdDSA is based on the Schnorr signatures and used in, e.g., GnuPG and OpenSSH.

Standardisation Documents | FIPS 186-5 [NIST23], RFC 8032 [JL17].

Quantum-safe? | No.

RSA

Description | RSA is a very popular general use asymmetric cipher based on the difficulty of factoring a number into two primes [MKJR16].

Public-Key Sizes (bits) | ≥2048.

Private-Key Sizes (bits) | Approximately the sizeofthe public key.

Ciphertext Size (bits) | At most the size of the public key.

Hardness AssumptionInteger | Factorisation.

Crypto Functionality | RSA is used for key encapsulation and digital signatures.

Applications | RSA is used in a wide range of both software and hardware domains.

Further Comments | -

Standardisation Documents | FIPS 186-5 [NIST23], NIST SP 800-56B [NIST19a] rev 2, RFC 8017 [MKJR16], ANSI X9.44 [ANSI17b], PKCS #1 [MKJR16], ISO/IEC 14888-2:2008 [ISO08], ISO/IEC 11770-3:2021 [ISO10c], ISO/IEC 9796-2:2010 [ISO10a], ISO/IEC 18033-2 [ISO10a].

Quantum-safe? | No.

6.2) Quantum-Safe Asymmetric Cryptography

In this section we list some asymmetric cryptography that are quantum-safe.

6.2.1 Key Exchange and Key Encapsulation Mechanisms

Recall that there is a subtle difference in the functionality provided by key exchanges and key encapsulation mechanisms. This difference is outside the scope of this document, and thus these primitives are grouped together. Additionally, note that this section does not treat former NIST candidate SIKE, as it has been broken [CD23].

ML-KEM (CRYSTALS-Kyber)

Description | ML-KEM, also known as CRYSTALS-Kyber, is a lattice-based and the primary KEM that is now standardised by NIST [NIST24a].

Parameter sizes (in bits) | Sizes of keys and ciphertexts of ML-KEM:

Security category	Parameter set	Public-key	Private-key	Ciphertext
1	ML-KEM-512	6,400	13,056	6,144
3	ML-KEM-768	9,472	19,200	8,704
5	ML-KEM-1024	12,544	25,344	12,544

Hardness Assumption | Module Learning with Errors (MLWE).

Further Comments | NIST recommends ML-KEM-768 (Category 3) by default. European security agencies also recommend *at least* category 3.

Standardisation Documents | [NIST24a].

Quantum-safe? | Yes.

BIKE

Description | BIKE [ABBB+21] is a code-based KEM. It is currently a candidate in Round 4 of the NIST competition.

Parameter sizes (in bits) | Claimed to achieve a certain NIST security category:

Security category	Parameter set	Public-key	Private-key	Ciphertext
1	BIKE-L1	12,323	2,244	12,579
3	BIKE-L3	24,659	3,346	24,915
5	BIKE-L5	40,973	4,640	41,229

Hardness Assumption | Quasi-Cyclic Syndrome Decoding problem.

Further Comments | NIST Round 4 candidate.

Standardisation Documents | BIKE website [ABBB+21].

Quantum-safe? | Yes.

Classic McEliece

Description | Classic McEliece [ABCC+20] is a conservative code-based KEM that is based on the 1978 original McEliece cryptosystem [McE78]. It is a NIST round 4 candidate and is considered for standardisation by ISO.

Parameter sizes (in bits) | Claimed to achieve a certain NIST security category:

Security category	Parameter set	Public-key	Private-key	Ciphertext
1	Classic-McEliece-348864	2,088,960	51,936	768
3	Classic-McEliece-460896	4,193,280	108,864	1,248
5	Classic-McEliece-6688128 Classic-McEliece-6960119 Classic-McEliece-8192128	8,359,936 8,378,552 10,862,592	111,456 111,584 112,960	1,664 1,552 1,664

Hardness Assumptions | Syndrome Decoding Problem (message security) and Goppa code recovery (key security).

Further Comments | NIST round 4 candidate. Classic McEliece requires very large key sizes but small ciphertexts, so probably not usable for low storage systems such as smartcards or IoT. Nevertheless, it has whithstood major cryptanalysis for decades and European security agencies are confident in its security.

Standardisation Documents | Official website [ABCC+20].

Quantum-safe? | Yes.

FrodoKEM

Description | FrodoKEM is a lattice-based KEM that supports conservative, yet practical constructions. It will not be standardised by NIST [ABDL+21].

Parameter sizes (in bits) | Claimed to achieve a certain NIST security category:

Security category	Parameter set	Public-key	Private-key	Ciphertext
1	FrodoKEM-640-AES	76,928	159,104	78,016
3	FrodoKEM-976-AES	125,056	250,368	126,336
5	FrodoKEM-1344-AES	172,160	344,704	173,568

Hardness Assumption | Plain Learning with Errors (LWE).

Further Comments | Currently, FrodoKEM will not be standardised by NIST, but it is considered for standardisation by ISO, and is recommended by European security agencies.

Standardisation Documents | Documents Official website [ABDL+21].

Quantum-safe? | Yes.

HQC

Description | HQC [MABL+21] is a code-based KEM currently a candidate in Round 4 of the NIST competition.

Parameter sizes (in bits) | Claimed to achieve a certain NIST security category:

Security category	Parameter set	Public-key	Private-key	Ciphertext
1	HQC-L1	17,992	448	35,976
3	HQC-L2	36,176	512	72,336
5	HQC-L3	57,960	576	115,880

Hardness Assumption | Decisional Quasi-Cyclic Syndrome Decoding Problem.

Further Comments | HQC is a NIST Round 4 candidate. It can be considered as a code-based analogue of ML-KEM.

Standardisation Documents | HQC website [MABL+21].

Quantum-safe? | Yes.

6.2.2 Stateful Digital Algorithms

LMS and HSS

Description | Leighton-Micali Signatures is a stateful hash-based signature scheme that uses LM-OTS for one-time signatures and is based on Merkle hash trees. HSS is a variant that has multiple hash trees [NIST20a].

Public-Key Sizes (bits) | 384-448 (only for LMS, no standardised parameter for number of hash trees in HSS).

Private-Key Sizes (bits) | Multiple one-time private keys that are dependent on many variables and assumptions, difficult to estimate.

Signature Size (bits) | 6240-74592 (only for LMS, no standardised parameter for number of hash trees in HSS).

Hardness Assumption | Collision Resistance.

Further Comments | Careful state management is essential and the main issue with the algorithm.

Standardisation Documents | SP800-208 [NIST20a], RFC 8554 [IETF19].

Quantum-safe? | Yes.

XMSS and XMSS^{MT}

Description | The eXtended Merkle Signature Scheme (XMSS) is a stateful hash-based signature scheme that uses WOTS+ for one-time signatures and is based on Merkle hash trees. XMSS^{MT} is a variant that has multiple hash trees [NIST20a].

Public-Key Sizes (bits) | 384-1024.

Private-Key Sizes (bits) | Multiple one-time private keys that are dependent on many variables and assumptions.

Signature Size (bits) | 11936-221504.

Hardness Assumption | Collision Resistance.

Further Comments | Careful state management is essential and the main issue with the algorithm.

Standardisation Documents | SP800-208 [NIST20a], RFC 8391 [IETF18].

Quantum-safe? | Yes.

6.2.3 Stateless Digital Signature Algorithms

ML-DSA (CRYSTALS-Dilithium)

Description | ML-DSA, also known as CRYSTALS-Dilithium, is a lattice-based and the primary signature scheme that is now standardised by NIST [NIST24b].

Parameter Sizes (in bits) | Sizes of keys and signatures of ML-DSA:

Security category	Parameter set	Public-key	Private-key	Ciphertext
2	ML-DSA-44	10,496	20,480	19,360
3	ML-DSA-65	15,616	32,256	26,472
5	ML-DSA-87	20,736	39,168	37,016

Hardness Assumption | Module Small Integer Problem (MSIS) and Module Learning with Errors (MLWE).

Further Comments | ML-DSA is a digital signature counterpart to the public-key ML-KEM, which is also NIST standardised. European security agencies recommend to use parameters corresponding to security category at least 3.

Standardisation Documents | FIPS 204 [NIST24b].

Quantum-safe? | Yes.

FN-DSA (Falcon)

Description | FN-DSA, also known as Falcon [FHKP+21], is a lattice-based signature scheme that was selected by NIST for standardisation.

Parameter Sizes (in bits) | Claimed to achieve a certain NIST security category:

Security category	Parameter set	Public-key	Private-key	Ciphertext
1	Falcon-padded-512	7,176	10,248	5,328
5	Falcon-padded-1024	14,344	18,440	10,240

Hardness Assumption | Short integer solution (SIS) problem over NTRU lattices.

Further Comments | NIST's primary signature scheme is ML-DSA. FALCON uses floating point arithmetic, which is not very common in cryptography. In particular, it is considered difficult to securely implement it in order to resist side-channel attacks and is not recommended by European security agencies.

Standardisation Documents | Falcon website [FHKP+21].

Quantum-safe? | Yes.

SLH-DSA (SPHINCS+)

Description | SLH-DSA, also known as SPHINCS+, is a stateless hash-based signature scheme that is now standardised by NIST [NIST24c].

Parameter sizes (in bits) | Sizes of keys and signatures of SLH-DSA:

Security category	Parameter set	Public-key	Private-key	Ciphertext
2	SLH-DSA-SHA2-128s	256	512	62,848
3	SLH-DSA-SHA2-192s	384	768	129,792
5	SLH-DSA-SHA2-256s	512	1,024	238,336

Hardness Assumption | Second-preimage resistance.

Further Comments | NIST's primary signature scheme is ML-DSA.

Standardisation Documents | FIPS 205 [NIST24c].

Quantum-safe? | Yes.

6.3) Symmetric Cryptography

In this section we list some symmetric cryptography of which there exist quantum-safe versions.

6.3.1 Ciphers

AES

Description | AES is a block cipher that is standardised by NIST [NIST01b].

Supported Key Lengths (bits) | 128, 192, 256.

Applications | AES is used in a wide range of both software and hardware implementations.

Further Comments | AES is the *de facto* standard for symmetric ciphers.

Standardisation Documents | FIPS 197 [NIST01b], ISO/IEC 180330-3:2010 [ISO10b].

Quantum-safe? | Yes.

ChaCha20

Description | ChaCha20 is a stream cipher that is normally combined with Poly1305 [NL18] when used in TLS.

Supported Key Lengths (bits) | 128, 256.

Applications | ChaCha20 is used in a variety of protocols such as TLS and S/MIME (generally, in the software domain).

Further Comments | ChaCha20 is known for its speed and simplicity of implementation.

Standardisation Documents | RFC 8439 [NL18].

Quantum-safe? | Yes.

6.3.2 Hash Functions

SHA-3 (Keccak)

Description | SHA-3, also known as Keccak, is a set of hash functions standardised by NIST.

Hash Output Sizes (bits) | 224, 256, 384, 512.

Applications | SHA-3 is used in a wide range of both software and hardware domains.

Further Comments | SHA-3 is the *de facto* standard for hash algorithms. SHA-3 is the successor of SHA-2 and SHA-1. Both SHA-3 and SHA-2 are recommended, while SHA-1 is insecure deprecated.

Standardisation Documents | FIPS 180-4 [NIST15a], NIST SP 800 107 Rev. 1 [NIST12], RFC 6234 [HE11], ISO/IEC 10118-3:2018 [ISO11] (SHA2), FIPS 180-4 [NIST15a], FIPS 202 [NIST15b], NIST SP 800 107 Rev. 1 [NIST12], ISO/IEC 10118-3:2018 [ISO11] (SHA3).

Quantum-safe? | Yes.

SHA-2

Description | SHA-2 is a set of hashes standardized by NIST and originally designed by the NSA [NIST02], which supersedes SHA-1.

Hash Output Sizes (bits) | 224, 256, 384, 512.

Applications | SHA-2 is used in a wide range of both software and hardware domains.

Further Comments | SHA-3 is the successor of SHA-2 and SHA-1. Both SHA-3 and SHA-2 are recommended, while SHA-1 is insecure and deprecated.

Standardisation Documents | FIPS 180-4 [NIST15a], NIST SP 800 107 Rev. 1 [NIST12], RFC 6234 [HE11], ISO/IEC 10118-3:2018 [ISO11] (SHA2), FIPS 180-4 [NIST15a], FIPS 202 [NIST15b], NIST SP 800 107 Rev. 1 [NIST12], ISO/IEC 10118-3:2018 [ISO11] (SHA3).

Quantum-safe? | Yes.

BLAKE2

Description | BLAKE2 is a hash function that has better software performance than SHA-3 [BLAKE217]. It comes in two “flavours”, BLAKE2b and BLAKE2s.

Hash Output Sizes (bits) | ≤ 512 (BLAKE2b), ≤ 256 (BLAKE2s).

Applications | BLAKE2 is used both in cryptographic and non-cryptographic settings.

Further Comments | SHA-3 and SHA-2 are recommended. BLAKE2 has received significantly less analysis than SHA-3 and SHA-2.

Standardisation Documents | RFC 7693 [SA15].

Quantum-safe? | Yes, if BLAKE2b is used.

6.3.3 Message Authentication Codes (MACs)

CMAC

Description | CMAC is another way to construct a MAC from a block cipher [ISLP06].

MAC Key Sizes (bits) | This depends on the chosen block cipher.

MAC Output Size (bits) | This depends on the chosen block chiper.

Applications | CMAC is not as widely used as CBC-MAC.

Further Comments | Recommended to use with AES. CMAC-AES is recommended by NIST instead of CBC-MAC.

Standardisation Documents | NIST SP 800-38B [NIST16a], RFC 4493 [ISLP06], ISO/IEC 9797-1:2011 [ISO18a].

Quantum-safe? | Yes, if the underlying hash is quantum-safe.

HMAC

Description | HMAC is a way to construct a MAC from cryptographic hashes [KBC97].

MAC Key Sizes (bits) | Arbitrary.

MAC Output Sizes (bits) | This depends on the chosen hash. Applications HMAC is used in IPSec, SSH and TLS protocols. Further Comments HMAC may suffer from performance issues.

Standardisation Documents | FIPS 198-1 [NIST08], RFC 2104 [KBC97].

Quantum-safe? | Yes, if the underlying hash is quantum-safe.

KMAC

Description | KMAC is-a MAC with variable length output size based on SHA-3 [NIST16b].

MAC Key Sizes (bits) | ≥ 128.

MAC Output Sizes (bits) | Variable.

Applications | Symmetric authentication.

Further Comments | -

Standardisation Documents | NIST SP 800-185 [NIST16b].

Quantum-safe? | Yes.

BLAKE2-MAC

Description | BLAKE2 does not need to use the HMAC transformation to be used as a MAC as it already includes a keying mechanism [SA15].

MAC Key Sizes (bits) | Arbitrary.

MAC Output Sizes (bits) | ≤ 512 (BLAKE2b), ≤ 256 (BLAKE2s).

Applications | BLAKE2-MAC is used in the software domain.

Further Comments | HMAC-SHA-2 and KMAC are recommended. BLAKE2-MAC is faster than HMAC due to its built-in keying mechanism.

Standardisation Documents | RFC 7693 [SA15].

Quantum-safe? | Yes, if Blake2b is used.

CBC-MAC

Description | CBC-MAC is a way to construct a MAC from a block cipher [ISO11].

MAC Key Sizes (bits) | This depends on the chosen block cipher.

MAC Output Sizes (bits) | This depends on the chosen block cipher.

Applications | CBC-MAC is normally used for fixed-length messages.

Further Comments | CBC-MAC is superseded by CMAC.

Standardisation Documents | ISO/IEC 9797-1 [ISO11].

Quantum-safe? | Yes, if the underlying block-cipher is quantum-safe, but consider using HMAC or CMAC instead.

6.4) Comparison of Post-Quantum Cryptography

In this section we will compare several post-quantum cryptography schemes both in performance and underlying mathematical problems.

Table 6.2 shows the strengths and weaknesses ofcertain Key Exchange (KE) algorithms and Key Encapsulation Mechanisms (KEMs). Similarly, Table 6.3 shows the relative strengths and weaknesses of certain Digital Signature Algorithms (DSA). Dark green indicates a strength, light green indicates a mild strength, orange indicates a mild weakness and red indicates a weakness. We compare the post-quantum schemes at NIST security level 5, while for RSA we use the 3072 bit variant and for EdDSA we use Curve25519.
The standardised column is dark green for NIST standardised schemes, light green for schemes that are in the process of being standardised by NIST or ISO, and orange for schemes for which it is unsure whether they will be standardised. The confidence column reflects the level of trust the scientific community places in the cryptographic scheme. For example, some schemes are based on more conservative assumptions, and others have undergone more extensive scrutiny, both of which enhance the confidence level.
The speed benchmarks were produced using the Open Quantum Safe benchmarking suite [OQS23] and Botan [BSI24a]. They were run on a server with an Intel® Xeon® Gold 6248 CPU, and our results and code are available at [Ste]. There are several publicly available benchmarks of cryptographic implementations as well, for example at eBACS [BL] or OQS [OQS23]. The relative performance of the schemes can differ between machines and implementations. Moreover, future implementations of some schemes could gain a larger speed improvement from optimisation than others. Depending on how critical speed is to an application, we suggest making application-specific benchmarks.

		Features		Speed			Size		
QUANTUM-SAFE		STANDARDISED	CONFIDENCE	KEY GENERATION	ENCRYPTION	DECRYPTION	PUBLIC KEY	PRIVATE KEY	CIPHERTEXT
🟥	X25519	🟩	🟩	🟩	🟢	🟢	🟩	🟩	🟩
🟥	RSA	🟩	🟩	🟥	🟢	🟧	🟩	🟢	🟩
🟩	BIKE	🟧	🟧	🟢	🟢	🟧	🟢	🟢	🟢
🟩	Classic McEliece (s)	🟢	🟩	🟥	🟢	🟢	🟥	🟥	🟩
🟩	Classic McEliece (f)	🟢	🟩	🟥	🟢	🟢	🟥	🟥	🟩
🟩	FrodoKEM-AES	🟢	🟩	🟢	🟧	🟧	🟧	🟥	🟧
🟩	FrodoKEM-SHAKE	🟢	🟩	🟢	🟧	🟧	🟧	🟥	🟧
🟩	HQC	🟧	🟧	🟧	🟥	🟥	🟢	🟩	🟧
🟩	ML-KEM	🟩	🟢	🟩	🟩	🟩	🟩	🟧	🟩

Table 6.2 | Strengths and weaknesses of various KE(M)s.

		Features		Speed			Size		
QUANTUM-SAFE		STANDARDISED	CONFIDENCE	KEY GENERATION	SIGNATURES	VERIFICATION	PUBLIC KEY	PRIVATE KEY	SIGNATURE
🟥	EdDSA	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
🟥	RSA	🟩	🟩	🟥	🟧	🟩	🟢	🟢	🟢
🟩	FN-DSA	🟢	🟢	🟧	🟢	🟩	🟧	🟧	🟧
🟩	ML-DSA	🟩	🟢	🟩	🟩	🟩	🟧	🟧	🟧
🟩	SLH-DSA-SHA (s)	🟩	🟩	🟢	🟧	🟧	🟩	🟢	🟥
🟩	SLH-DSA-SHA (f)	🟩	🟩	🟧	🟥	🟧	🟩	🟢	🟥
🟩	LMS*	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟧
🟩	XMSS*	🟩	🟩	🟥	🟧	🟧	🟩	🟧	🟧

Table 6.3 | Strengths and weaknesses of various DSAs.

*Stateful scheme.

The sources for the sizes of the keys, signatures and ciphertexts can be found in the previous sections of this chapter. These tables do not take into account means to compress the private key, for example by storing the seed to a deterministic random number generator used to generate the private key instead of the private key itself. See for example Section A.2.3 in [NIST23] for EdDSA.

To help in understandanding which post-quantum scheme better fits a use case, we refer to the PQChoiceAssistant [TC24]. This tool functions as an interactive questionnaire, guiding users through a series of questions about performance and security requirements. The intended audience for this tool is people with generic security knowledge and high level overview of their use cases. For users with cryptographic knowledge, there are expert questions that are more detailed. Based on the responses, the tool suggests suitable PQC algorithms, providing scores and detailed explanations on the match between the use case and the algorithms. The PQChoiceAssistant currently supports the algorithms ML-KEM, FrodoKEM, Classic McEliece, HQ-C and BIKE for KEM, and ML-DSA, FN-DSA, SLH-DSA, and XMSS for DSA.

6.4.1 Overview of Post-Quantum Cryptography

In the past decades, academic research identified five general families of mathematical domains susceptible to giving rise to suitable quantum-resistant hard problems that can be used to build post-quantum cryptography.

Lattice-Based Cryptography | The main computational problem at the core lattice-based cryptography is the *Learning With Errors* (LWE) problem, which consists of solving anoisy linear system of equations over a finite field, with the additional constraint that *all* the coefficients of the solutions should be *small*. For suitable parameters, LWE can be shown to be as hard as finding a *short* vector in *any* Euclidean lattice. The latter problem is known as *Shortest Vector Problem* (SVP) and has been studied for decades. As such, its complexity is well understood and we have high confidence that the problem remains hard even for full-scale quantum computers. Another well-understood computational problem, used to construct lattice-based cryptographic primitives, is the NTRU problem. Lattice-based approaches provide very competitive schemes with good performance in terms of bandwidth, and efficiency.

Code-Based Cryptography | Code-based cryptography is based on the hardness of a similar problem from linear algebra, with the main difference being that the additional constraint is now that the vector solution should have a specific Hamming weight. In general, the solution is asked to have a *low* Hamming weight. This problem is equivalent to decoding a random linear code, a problem that has been introduced and studied since the early days of telecommunications in the 1950s. Classic McEliece is a cryptosystem based on an original construction by McEliece in 1978 [McE78]. In particular, it is the oldest cryptosystem still unbroken (even using quantum) and therefore benefits from high confidence in its security. On the other hand, this strong security comes at the expense of a large public key.

Multivariate Polynomial Systems | Both previous families are based on the hardness of solving constrained, but *linear*, systems over a finite field. On the other hand, Multivariate Quadratic cryptography (MQ) is based on the hardness of solving a system of polynomial equations of degree two over a finite field. One of the main MQ cryptographic constructions is known as *Oil and Vinegar* (sometimes referred to as *unbalanced Oil and Vinegar*, and denoted UOV) introduced in [KPG99]. MQ approaches are especially suitable for digital signatures and typically produce one of the shortest signatures. However, MQ schemes usually suffer from larger key sizes and various attempts to improve on this resulted in weaker schemes than expected, as shown by the attacks breaking certain NIST candidates, e.g., [Beu22].

Isogeny-Based Cryptography | Traditional cryptography using elliptic curves is based on the so-called Discrete Logarithm Problem, and is known to be vulnerable to quantum attacks. However, it has been conjectured that computing special maps between elliptic curves, known as *isogenies* remains hard, even with the help of quantum computers. Isogeny-based cryptography is, by far, the most recent design principle for post quantum cryptography, and usually suffers from expensive operations resulting in slower cryptographic schemes. Additionally, a recent breakthrough in isogeny-based cryptanalysis [CD23] broke one of the NIST finalists, further reducing the confidence in the security of isogeny-based schemes. After the breakthrough, a new line of work, focusing on the so-called *higher-dimensional isogenies*, provided a new direction for the development of isogeny-based schemes. Given such a turbulent recent history, the dominant opinion of the cryptographic community is that further study is necessary before standardising isogeny-based schemes. Nevertheless, the community recognises the added value in further studies of these schemes given their intrinsic difference from the previously mentioned problems.

Hash-Based Cryptography | Cryptographic hash functions have been used to build signature schemes since the late 1970s using the basic concepts of hash trees and the selective opening of preimages of hashes. Their security is well understood and based on the hardness of finding a (second) message that hashes to a given hash. There are various *stateful* hash-based signature schemes, where it is very important to remember which private key parts have been used, i.e., to maintain a state. If two signatures are generated from the same private key part then this may facilitate forgeries. In many application scenarios, appropriate state management is difficult, if not impossible. More recently, stateless hash-based signature schemes have been introduced, eliminating the main disadvantage of their stateful counterparts. Stateful schemes can still be preffered over stateless schemes for their faster signature generation.

Structured vs Unstructured | Code-based and lattice-based cryptography are both based on solving linear systems over finite fields, with additional non-linear constraints. However, this usually leads to schemes with low efficiency. To overcome a lack of efficiency, one might restrict those problems to linear systems whose underlying matrix has a special structure, for example, formed by multiple circulant (or anti-circulant) submatrices. In the context of lattice-based cryptography, this variant is known as *Module* Learning With Errors and is at the core of both ML-KEM (Kyber) and ML-DSA (Dilithium). The other lattice-based digital signature selected by NIST for stadardisation, namely FN-DSA (Falcon), also makes use of some *structured* lattice known as an NTRU lattice. Analogous structured problems are also used in code-based cryptography, under the name *Quasi-Cyclic Syndrome Decoding* (QCSD) and are at the core of both BIKE and HQC still competing in the last round of the NIST competition. The advantage of using such structured variants is that they result in more efficient and competitive cryptographic schemes with shorter keys, ciphertexts and signatures. On the other hand, this additional structure may reduce the difficulty of the underlying mathematical problem, weakening the cryptographic primitives. For this reason, some agencies such as NLNCSCA, the German BSI and the French ANSSI advocate for the standardisation of additional unstructured schemes such as Classic McEliece (code-based) and FrodoKEM (lattice-based) rather than solely relying on structured variants.

6.5) Security of Implementations

To deploy cryptographic primitives in practice, an implementation is necessary. In this section we want to reiterate about the fact that even if the design of a primitive is theoretically very secure, there are many weaknesses that can be introduced by a careless practical implementation, of which we give some examples. Specific security implementation requirements can include, but are not limited to, protection against Side-Channel Analysis (SCA), Fault Injection (FI) and Differential Fault Analysis (DFA). For a more detailed overview of SCA and FI on lattice-based schemes, it is possible to consult [RCDB24].

Side-Channel Analysis | Side-Channel Analysis (SCA) is a cryptographic implementation attack that extracts secret information by observing more than simply the input and output data during execution of a program. This applies to the cryptographic primitives, but also includes other security sensitive operations, such as transportation of a key into a hardware cryptographic coprocessor.
An example of a side-channel weakness that can be exploited is a loop that iterates a number of times depending on a secret. By looking at the response time of the program, a *timing attack*, an attacker could estimate the number of iterations and thus gain information on the secret. If security relevant information

is found in a side-channel this is often referred to as *leakage*. To prevent timing attacks, cryptographic implementations should run in constant time or the runtime should be completely independent of any secrets. Besides time, other well-known side-channels are power consumption and electromagnetic radiation. In some cases temperature, sound or light have also leaked information regarding processes executing on a device. In most cases a side-channel needs to be measured in close proximity to the device processing the secret data. However, a timing attack can be run from a remote location, for example from the device of the other party in the communication.

In most SCA attacks the attacker will monitor and record the side-channel during multiple executions of the algorithm and apply statistical analysis on the recorded data to extract information related to the secret key that was used. In some cases, even partial information on the key can be enough for a feasible attack to reconstruct the entire key. There are also SCA attacks that require only observation of a single execution of an algorithm, or make use of machine learning to extract secret data.

Preventing side-channel analysis attacks from being successful can be challenging. Even if a cryptographic algorithm is designed to run in constant time, the compiler might introduce weaknesses through optimisation, causing performance variations. For example a recent vulnerability found in the reference implementation of ML-KEM [BBBC+24], and also in many other implementations, demonstrates this issue: secret dependent operations caused leakage of the secret key which was reconstructed within a few minutes. As this was a software implementation, the vulnerability has been promptly patched. Even though this is not the most important or relevant work on SCA for PQC, the fact that it was found later in the standardisation process underscores the importance of staying informed and vigilant about the threat of implementation vulnerabilities.

Moreover, standard hardening techniques against SCA are not always compatible with the design of some candidates. For instance, the digital signature algorithm FN-DSA involves floating point arithmetic, which is very challenging to protect against side-channel attacks. This complexity delayed its standardisation [Moo24].

Fault Injection | Fault Injection (FI) is an implementation attack that aims to introduce corruption in the normal operation of the device. An example of such attack is a *safe-error attack*, where the attacker injects a fault that sets a bit of the secret key held by the target. By verifying whether the result of the corresponding computation was modified, it is possible to determine the value of the targeted bit of the secret key, resulting in leakage.

Well known fault injection techniques include: clock or reset glitching, voltage fault injection (manipulation of the power supply voltage or Body Bias Injection), laser fault injection (for targeting semiconductors), and exposure to electromagnetic radiation. These techniques can be applied to the full device, or specifically target a dedicated Integrated Circuit (chip) inside a device.

Differential Fault Analysis | Differential Fault Analysis (DFA) is a type of implementation attack where corrupted computations of an algorithm are analysed to extract secret data. An FI attack is needed to introduce the corruptions in the computation.

For some DFA attacks multiple faults are required for the analysis, in the case of most attacks on symmetric algorithms, and other attacks require only one faulty response, such as the well-known Bellcore attack on RSA-CRT [SvdBFG+12]. DFA attacks do not work on all cryptographic algorithms, but publications do exist related to DFA attacks on post-quantum cryptographic algorithms, such as FN-DSA [BD23] and MLDSA [CBH24].

It is crucial to determine to which extent the application needs to be protected against SCA, FI and DFA. Resistance against timing attacks is essential, but it is important to note that including SCA, FI and DFA countermeasures will impact the size and performance of the implementation. It is imperative that protected implementations fit the application without causing issues or bottlenecks.

Because of the many weaknesses that can be introduced into an implementation of a cryptographic algorithm, it is strongly advised to leave implementation to experts. It is therefore essential to deploy production-ready implementations that have undergone thorough security evaluation, such as those certified under FIPS 140 [NIST01a; NIST19c] or ISO/IEC 19790 [ISO12] for cryptographic modules or ISO/IEC 15408 [ISO22b], also known as Common Criteria (CC) and the Dutch Baseline Security Product Assessment (BSPA) [BSPA20] for generic cryptographic and security implementations. Security evaluations should be performed by accredited security evaluation labs that provide certification services. These labs can also provide trainings and tools to perform in-house security evaluations.

6.6) PQC Implementations

The goal of this section is to understand the state of the art in cryptography to assist in choosing one of the available cryptographic libraries. To this end we provide an overview of several libraries implementing post-quantum primitives.

Note that not every library provides an implementation of every cryptographic primitive. Although for example all key encapsulation mechanisms are equivalent in terms of functionality, other factors such as speed and memory use can be relevant. A library may or may not provide an interface to the programming language or framework the project is built upon, or could be intended for specialised use cases, such as embedded systems.

Development Progress | All submissions to the NIST post-quantum cryptography standardisation competition in 2016 already included reference implementations of the candidates. Later, optimised implementations were made available. Many submissions were eventually broken, most notably round 4 candidate SIKE in 2023 [CD23]. It is not impossible that other candidates can be broken, which for now is an argument to use hybrid cryptography, see Section 4.1. These reference implementations can be found in their respective standardisation documents listed in the previous sections. However, they are not intended to be used in a production setting. For example, there has recently been an attack on ML-KEM's reference implementation [BBBC+24], affecting various other implementations as well.

Reference implementations can however be used as a stand-in during the development process of the migration until more reliable implementations become available. This too requires some degree of cryptographic agility. Within a single library, this is generally achieved through a 'universal' interface to the cryptography. For example, for OpenSSL replacing the DES cipher by the AES cipher can be done by replacing the function call EVP_CIPHER_fetch(0,"DES-CBC",0) by EVP_CIPHER_fetch(0,"AES-256-CBC",0). To facilitate migration, Open Quantum Safe (OQS) provides post-quantum implementations that can be similarly used within OpenSSL. Note that just as for the reference implementations, OQS currently does not recommend using its library in a production setting.

There are libraries providing post-quantum cryptography that are ISO or FIPS certified, which can be a requirement for example when one of the end-users is a government organisation. The new post-quantum schemes approved by NIST will most likely obtain FIPS 140-3 certification over FIPS 140-2, since no new FIPS 140-2 validations are being granted.

Hardware Implementations | In general, hardware implementations are designed to leverage parallel execution to enhance performance. Unlike software solutions that typically run on a single processing core, hardware can perform multiple operations simultaneously. This parallelism is achieved through various mechanisms such as dedicated processing units, pipeline architecture, and custom circuits. As a downside, additional hardware can be costly.

A dedicated coprocessor implemented in hardware will outperform a software implementation, but can (usually) not be updated in case an issue is identified in the field. Hardware acceleration can provide a solution in between a full software and dedicated hardware implementation. In this case either a CPU has dedicated instructions or a coprocessor is used to perform parts of the calculation that are time consuming in a pure software implementation.

Software Implementations | Table 6.4 lists several common cryptographic libraries with some additional information related to compatibility and security. This list is not intended to be complete nor an endorsement of any specific library. Moreover, this list is prone to being out-dated, and thus the current version of this table should only be consulted by those migrating in the near future. The PKI Consortium keeps a similar table at https://pkic.org/pqccm.

Organisation	Git repository	Stateful DSA	Stateless DSA	KE(M)	Hybrid option	Certification	Language interfaces
Botan	[BSI24a]	✓	✓	✓	✓	–	C, C++, D, Python, Rust, Ruby, Haskell
Bouncy Castle	[BC24b]	✓	✓	✓	✓	FIPS 140-3	C#, Java, Kotlin
Crypto++	[Dai23]				–	–	C++
FoxCrypto	[Fox23]	✓			–	CC	C
GnuTLS	[GnuTLS24]				–	FIPS 140-2	C
KyberLib	[Rou24]			✓	–	–	Rust
LibreSSL	[LibreSSL24]				–	–	C
Libsodium (NaCl)	[Libsodium13]				–	–	C, C++
Nettle	[Nettle24]				–	–	C
OpenSSL	[OpenSSL03]				–	FIPS 140-2	C
OpenSSL-OQS	[OQSprovider24]		✓	✓	–	–	C
OQS	[OQS24]	✓	✓	✓	–	–	C, Python, Rust, Java
PQM4	[KPRS+22]		✓	✓	–	–	C (ARM MCU)
PQClean	[PQClean23]		✓	✓	–	–	C
RustTLS	[Rust24]	✓	✓	✓	–	–	Rust
WolfSSL	[Wol24a]		✓	✓	–	FIPS 140-3	C (Embedded systems)

Table 6.4 | Several common cryptographic libraries (October 9, 2024).

The columns 'stateful DSA', 'stateless DSA' and 'KE(M)' contain a checkmark if the library implements at least one corresponding post-quantum scheme.

Advice for Integrators | We briefly enumerate some practical advice for those integrating post-quantum cryptography.

- Stay up-to-date with the developments of standards Now that the standards for ML-KEM [NIST24a], ML-DSA [NIST24b] and SLH-DSA [NIST24c] have been released, secure implementations are expected to become available soon;
- Stay up-to-date with the developments of certifications if relevant to specific applications;
- Stay up-to-date with publications related to SCA, FI, DFA, and other vulnerabilities during all phases of the product's life-cycle. See for example a Common Vulnerabilities and Exposure database like https://nvd.nist.gov/;
- Consider a hybrid approach of using a combination of software and hardware solutions;
- Investigate the usage of (re)configurable hardware (e.g., FPGA or IC with a partial configurable logic portion) when the application demands in the field update capabilities.

Bibliography

[ABBB+21] Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor, Vasseur. Valentin, Santosh Ghosh, and Jan Richter-Brokmann. BIKE Website. https://bikesuite.org/. [Accessed 22/08/2022]. 2021.

[ABCC+20] Martin Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece Website. https://classic.mceliece.org/index.html. [Accessed 23/05/2022]. 2020.

[ABDL+21] Erdem Alkim, Joppe Bos, Léo Ducas, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, Douglas Stebila, Karen Easterbrook, and Brian LaMacchia. FrodoKEM Website. https://frodokem.org/. [Accessed 23/05/2022]. 2021.

[ABNS24] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), and Swedish Armed Forces Swedish National Communications Security Authority. Position Paper on Quantum Key Distribution. Accessed 2024-07-16. 2024. url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4.

[AIVD23] AIVD. AIVD-jaarverslag 2023. https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2024/04/22/jaarverslag-2023. 2023.

[ANSI10] American National Standards Institute (ANSI). ANSI X9.98-2010 Lattice-Based Polynomial Public Key Establishment Algorithm For The Financial Services Industry. ANSI X9.98-2010. American National Standards Institute, 2010. url: https://webstore.ansi.org/standards/ascx9/ansix9982010.

[ANSI17a] American National Standards Institute. Key Agreement and Key Transport Using Elliptic Curve Cryptography. Standard. ANSI, Feb. 2017.

[ANSI17b] American National Standards Institute. Key Establishment Using Integer Factorization Cryptography. Standard. ANSI, Nov. 2017.

[ANSI20] American National Standards Institute. Financial services - Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm - ECDSA. Standard. ANSI, Sept. 2020.

[ANSSI20] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Technical Position Paper QKD v2.1 - Should Quantum Key Distribution be Used for Secure Communications? https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/. 2020.

[ANSSI23] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Migration to Post-Quantum Cryptography Recommendations and Guidelines. https://www.ssi.gouv.fr/en/guide/migration-to-post-quantum-cryptography/. Jan. 2023.

[Apple24] Apple. iMessage PQ3 Quantum-Secure Messaging at Scale. https://security.apple.com/blog/imessage-pq3/. Accessed 2024-07-31. 2024.

[ASWH+23] Nouri Alnahawi, Nicolai Schmitt, Alexander Wiesmaier, Andreas Heinemann, and Tobias Grasmeyer. "On the State of Crypto-Agility". In Cryptology ePrint Archive (2023).

[AVW23] Suleman Ahmad, Luke Valenta, and Bas Westerbaan. Cloudflare now uses post-quantum cryptography to talk to your origin server. 2023. url: https://blog.cloudflare.com/post-quantum-to-origins.

[BBBC+24] Daniel J. Bernstein, Karthikeyan Bhargavan, Shivam Bhasin, Anupam Chattopadhyay, Tee Kiah Chia, Matthias J. Kannwischer, Franziskus Kiefer, Thales Paiva, Prasanna Ravi, and Goutam Tamvada. KyberSlash Exploiting secret-dependent division timings in Kyber implementations. Cryptology ePrint Archive, Paper 2024/1049. url: https://eprint.iacr.org/2024/1049. 2024.

[BC24a] Legion of the Bouncy Castle Inc. Bouncy Castle Cryptography APIs. 2024. url: https://bouncycastle.org.

[BC24b] The Legion of the Bouncy Castle. The Bouncy Castle for Java. https://github.com/bcgit/bc-java. Tag r1rv78v1. Apr. 2024.

[BD23] Sven Bauer and Fabrizio De Santis. "A differential fault attack against deterministic falcon signatures". In International Conference on Smart Card Research and Advanced Applications. Springer. 2023, pp. 43–61.

[Beu22] Ward Beullens. "Breaking Rainbow Takes a Weekend on a Laptop". In Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. Lecture Notes in Computer Science. Springer, 2022, pp. 464–479.

[BJKS24] Karthikeyan Bhargavan, Charlie Jacomme, Franziskus Kiefer, and Rolfe Schmidt. "Formal Verification of the PQXDH Post-Quantum Key Agreement Protocol for End-to-End Secure Messaging". In USENIX Security Symposium 2024. 2024.

[BL] Daniel J. Bernstein and Tanja Lange, eds. eBACS: ECRYPT Benchmarking of Cryptographic Systems. Accessed: 14 October 2024. url: https://bench.cr.yp.to.

[BLAKE217] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. BLAKE2 – fast secure hashing. https://www.BLAKE2.net/. [Accessed on 24-03-2022]. 2017.

[BLS24] David Basin, Felix Linker, and Ralf Sasse. A Formal Analysis of the iMessage PQ3 Messaging Protocol. Technical Report. 2024. url: https://security.apple.com/assets/files/A_Formal_Analysis_of_the_iMessage_PQ3_Messaging_Protocol_Basin_et_al.pdf.

[Bro09] Daniel Brown. Elliptic Curve Cryptography. Standard. SEC 1. Standards for Efficient Cryptography Group, May 2009.

[BSI22] Bundesamt für Sicherheit in der Informationstechnik (BSI). Quantum-safe Cryptography - fundamentals, current developments and recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html. May 2022.

[BSI24a] Bundesamt für Sicherheit in der Informationstechnik (BSI). Botan Crypto and TLS for modern C++. https://botan.randombit.net/. Version 3.5.0. 2024.

[BSI24b] Bundesamt für Sicherheit in der Informationstechnik (BSI). Cryptographic Mechanisms Recommendations and Key Lengths. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?blob=publicationFile&v=7. Feb. 2024.

[BSPA20] AIVD. Baseline Security Product Assessment (BSPA. https://www.aivd.nl/onderwerpen/informatiebeveiliging/certificeringen/baseline-security-product-assessment. Assessed: 2024-10-11. 2020.

[CBH24] Andersson Calle Viera, Alexandre Berzati, and Karine Heydemann. “Fault Attacks Sensitivity of Public Parameters in the Dilithium Verification”. In: Smart Card Research and Advanced Applications. Cham: Springer Nature Switzerland, 2024, pp. 62–83.

[CD23] Wouter Castryck and Thomas Decru. “An Efficient Key Recovery Attack on SIDH”. In Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 423–447. doi: 10.1007/978-3-031-30589-4_15. url: https://doi.org/10.1007/978-3-031-30589-4_15.

[Cha23] Walker Chablott. Addressing post-quantum cryptography with CodeQL. https://github.blog/2023-12-05-addressing-post-quantum-cryptography-with-codeql/. Accessed 2024-06-11. 2023.

[CISA23] Cybersecurity and Infrastructure Security Agency (CISA). Quantum-readiness Migration to Post-Quantum Cryptography. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography. Accessed 2024-06-17. Aug. 2023.

[CW21] Sofía Celi and Thom Wiggers. KEMTLS Post-Quantum TLS Without Signatures. 2021. url: https://blog.cloudflare.com/kemtls-post-quantum-tls-without-signatures.

[Cyc24] CycloneDX Project. CycloneDX A Standard for Bill of Materials. Accessed 2024-07-03. 2024. url: https://cyclonedx.org/.

[Dai23] Wei Dai. Crypto++ Library. https://github.com/weidai11/cryptopp. v8.9. Oct. 2023.

[dVBDvV24] Manon de Vries, Sven Bootsma, Vincent Dunning, and Marc van Vliet. Quantum risicomethodologie voor cryptografie. https://publications.tno.nl/publication/34642390/EUY5Mh/TNO-2024-R10707.pdf. 2024.

[EMVW22] Andre Esser, Alexander May, Javier Verbel, and Weiqiang Wen. “Partial Key Exposure Attacks on BIKE, Rainbow and NTRU”. In Advances in Cryptology – CRYPTO 2022. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Cham Springer Nature Switzerland, 2022, pp. 346–375. isbn 978-3-031-15982-4.

[ET05] Pasi Eronen and Hannes Tschofenig. Pre-shared key ciphersuites for transport layer security (TLS). RFC 4279. Dec. 2005. doi: 10.17487/RFC4279. url: https://www.rfc-editor.org/info/rfc4279.

[ETSI18] ETSI. Quantum-Safe Virtual Private Networks. Standard. TR 103 617. Valbonne, FR ETSI, Sept. 2018.

[ETSI20a] ETSI. Migration strategies and recommendations to Quantum Safe schemes. https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes. 2020.

[ETSI20b] European Telecommunications Standards Institute. CYBER; Quantum-safe Hybrid Key Exchanges. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Dec. 2020.

[ETSI20c] European Telecommunications Standards Institute. Migration strategies and recommendations to Quantum Safe schemes. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Aug. 2020.

[ETSI21a] European Telecommunications Standards Institute. CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Oct. 2021.

[ETSI21b] European Telecommunications Standards Institute. CYBER; Quantum-Safe Signatures. Technical Report. Sophia Antipolis, France European Telecommunications Standards Institute, Sept. 2021.

[EU16a] European Parliament and Council of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union L 194, 19 July 2016, pages 1-30. 2016. url: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[EU16b] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union L 119, 4 May 2016, pages 1-88. 2016. url: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[EU18] European Parliament. Directive (EU) 2018/1972 of the European Parliamentand of the council of 11 December 2018 establishing the European Electronic Communications Code. 2018. url: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX32018L1972.

[EU22a] European Parliament and Council of the European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union L 333, 27 December 2022, pages 80-152. 2022. url: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[EU22b] European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union L 333, 27 December 2022, pages 1-79. 2022. url: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

[EU24] European Commission. Commission Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJL_202401101. Official Journal of the European Union, L 1101, 12 April 2024. Apr. 2024.

[FHKP+21] Pierre-Alain Fouque, Jeffrey Hoffstein, Vadim Kirchner Paul Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON Website. https://falcon-sign.info/. [Accessed 23/05/2022]. 2021.

[Fiche24] Dutch Ministry of the Interior and Kingdom Relations. Fiche 1 Aanbeveling Routekaart Post-Quantumcryptografie. 2024. url: https://www.rijksoverheid.nl/documenten/publicaties/2024/04/11/fiche-1-aanbeveling-routekaart-post-quantumcryptografie.

[FK11] Sheila Frankel and Suresh Krishnan. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071. Feb. 2011. doi: 10.17487/RFC6071. url: https://www.rfc-editor.org/info/rfc6071.

[FKMS20] Scott Fluhrer, Panos Kampanakis, David McGrew, and Valery Smyslov. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security. RFC 8784. June 2020. doi: 10.17487/RFC8784. url: https://www.rfc-editor.org/info/rfc8784.

[Fox23] Fox Crypto. XMSS C Library. https://github.com/FoxCryptoNL/xmss. Version 1.0.0. Apr. 2023.

[GLRS16] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. “Applying Grover’s Algorithm to AES: Quantum Resource Estimates”. In: PQCrypto. Vol. 9606. Lecture Notes in Computer Science. Springer, 2016, pp. 29–43.

[GnuTLS24] GnuTLS. https://gitlab.com/gnutls/gnutls. v3.8. Oct. 2024.

[Google17] Google. Application Layer Transport Security. 2017. url: https://cloud.google.com/docs/security/encryption-in-transit/application-layer-transport-security.

[Google22a] Google. Messages End-to-End Encryption Overview (Technical Paper). Feb. 2022. url: https://www.gstatic.com/messages/papers/messages_e2ee.pdf.

[Google22b] Google. Securing tomorrow today Why Google now protects its internal communications from quantum threats. Nov. 2022. url: https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms.

[Gro24] The Tcpdump Group. TCPDUMP & LIBPCAP. 2024. url: https://www.tcpdump.org/.

[Gro96] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In STOC. ACM, 1996, pp. 212–219.

[GSMA24] GSM Association. Post Quantum Cryptography – Guidelines for Telecom Use Cases. https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf. Accessed 2024-06-19. Feb. 2024.

[HE11] Tony Hansen and Donald E. Eastlake 3rd. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234. May 2011. doi: 10.17487/RFC6234. url: https://www.rfc-editor.org/info/rfc6234.

[Hou02] Russ Housley. Cryptographic Message Syntax (CMS). RFC 3369. Sept. 2002. doi: 10.17487/RFC3369. url: https://www.rfc-editor.org/info/rfc3369.

[HRSS17] Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. NTRU-HRSS-KEM-Submission to the NIST post-quantum cryptography project. 2017. url: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/NTRU_HRSS_KEM.zip.

[IBM24] IBM. Examples from CBOM repository. https://github.com/IBM/CBOM/blob/main/EXAMPLES.md. Accessed 2024-07-04. 2024.

[IETF07] Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney L. Thayer, and David Shaw. OpenPGP Message Format. RFC 4880. Nov. 2007. doi: 10.17487/RFC4880. url: https://www.rfc-editor.org/info/rfc4880.

[IETF09] Mohamad Badra. Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode. RFC 5487. Mar. 2009. doi: 10.17487/RFC5487. url: https://www.rfc-editor.org/info/rfc5487.

[IETF18] Andreas Huelsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen. XMSS eXtended Merkle Signature Scheme. RFC 8391. May 2018. doi: 10.17487/RFC8391. url: https://www.rfc-editor.org/info/rfc8391.

[IETF19] David McGrew, Michael Curcio, and Scott Fluhrer. Leighton-Micali Hash-Based Signatures. RFC 8554. Apr. 2019. doi: 10.17487/RFC8554. url: https://www.rfc-editor.org/info/rfc8554.

[IETF24] Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-10. Internet Engineering Task Force, Apr. 2024. url: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/.

[ISLP06] Tetsu Iwata, Junhyuk Song, Jicheol Lee, and Radha Poovendran. The AES-CMAC Algorithm. RFC 4493. June 2006. doi: 10.17487/RFC4493. url: https://www.rfc-editor.org/info/rfc4493.

[ISO06] International Electrotechnical Commission International Organization for Standardization. Information technology – Security techniques – Encryption algorithms – Part 2 Asymmetric ciphers. ISO/IEC 18033-2. 2006. url: https://www.iso.org/standard/38788.html.

[ISO08] International Organization for Standardization. Information Technology – Security Techniques – Digital Signatures with Appendix – Part 2 Integer Factorization Based Mechanisms. Standard. Geneva, CH, Apr. 2008.

[ISO10a] International Organization for Standardization. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2 Integer factorization based mechanisms. Standard. ISO/IEC 9796-22010. Geneva, CH International Organization for Standardization, Dec. 2010.

[ISO10b] International Organization for Standardization. Information technology – Security techniques – Encryption algorithms – Part 3 Block ciphers. Standard. ISO/IEC 29167-212018. Geneva, CH International Organization for Standardization, Dec. 2010.

[ISO10c] International Organization for Standardization. Information technology – Security techniques – Key management – Part 1 Framework. Standard. Geneva, CH International Organization for Standardization, Apr. 2010.

[ISO11] International Organization for Standardization. IT Security techniques – Hash-functions - Part 3: Dedicated hash-functions. Standard. Geneva, CH: International Organization for Standardization, Mar. 2011.

[ISO12] International Electrotechnical Commission International Organization for Standardization. Information technology – Security techniques – Security requirements for cryptographic modules. ISO/IEC 19790. 2012. url: https://www.iso.org/standard/52906.html.

[ISO18a] International Organization for Standardization. Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1 Mechanisms using a block cipher. Standard. ISO/IEC 10118-32018. Geneva, CH International Organization for Standardization, Oct. 2018.

[ISO18b] International Organization for Standardization. Information Technology – Security Techniques – Digital signatures with Appendix – Part 3 Discrete Logarithm Based Mechanisms. Standard. Geneva, CH, Nov. 2018.

[ISO22a] International Organization for Standardisation. Information technology – Security techniques – Information security management systems – Requirements. Standard. ISO/IEC 270012022. Geneva, CH International Organization for Standardisation, Oct. 2022.

[ISO22b] International Electrotechnical Commission International Organization for Standardization. Information security, cybersecurity and privacy protection - Evaluation criteria for IT security. ISO/IEC 15408-1. 2022. url: https://www.iso.org/standard/72891.html.

[ISO24] International Electrotechnical Commission International Organization for Standardization. Information Security - Digital Signatures with Appendix. ISO/IEC 14888. 2024. url: https://www.iso.org/standard/80492.html.

[ITU19] International Telecommunication Union (ITU). Information technology - Open Systems Interconnection - The Directory Public-key and attribute certificate frameworks. Standard. Geneva, Switzerland ITU-T, Oct. 2019.

[Jac24] Frederic Jacobs. “Designing iMessage PQ3 Quantum-Secure Messaging at Scale”. In Real World Crypto Symposium 2024. Toronto, Canada, Mar. 2024.

[JACC+21] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. SIKE Website https://sike.org/. [Accessed 22/08/2022]. 2021.

[JL17] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032. Jan. 2017. doi: 10.17487/RFC8032. url: https://www.rfc-editor.org/info/rfc8032.

[JNRV20] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. “Implementing Grover Oracles for Quantum Key Search on AES and LowMC”. In EUROCRYPT (2). Vol. 12106. Lecture Notes in Computer Science. Springer, 2020, pp. 280–310.

[KBC97] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC Keyed-Hashing for Message Authentication. RFC 2104. Feb. 1997. doi: 10.17487/RFC2104. url: https://www.rfc-editor.org/info/rfc2104.

[KHNE+14] Charlie Kaufman, Paul E. Hoffman, Yoav Nir, Pasi Eronen, and Tero Kivinen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296. Oct. 2014. doi: 10.17487/RFC7296. url: https://www.rfc-editor.org/info/rfc7296.

[KJB24] Ini Kong, Marijn Janssen, and Nitesh Bharosa. Organizational Readiness Model for Quantum-safe Transition. https://hapkido.tno.nl/deliverables/organizational-readiness-model-quantum/. Accessed 2024-7-16. 2024.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. “Unbalanced Oil and Vinegar Signature Schemes”. In Advances in Cryptology - EUROCRYPT ’99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Ed. by Jacques Stern. Vol. 1592. Lecture Notes in Computer Science. Springer, 1999, pp. 206–222. doi: 10.1007/3-540-48910-X_15. url: https://doi.org/10.1007/3-540-48910-X_15.

[KPMS23] Stefan Kölbl, Anvita Pandit, Rafael Misoczki, and Sophie Schmieg. “Crypto Agility and Post-Quantum Cryptography @ Google”. In Real World Crypto Conference 2023. Tokyo, Japan, Mar. 2023. url: https://rwc.iacr.org/2023/.

[KPRS+22] Matthias J. Kannwischer, Richard Petri, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. PQM4 Post-quantum crypto library for the ARM Cortex-M4. https://github.com/mupq/pqm4. Round3. July 2022.

[KSFH+20] Panos Kampanakis, Douglas Stebila, Markus Friedl, Torben Hansen, and Dimitrios Sikeridis. Post-quantum public key algorithms for the Secure Shell (SSH) protocol. Internet-Draft draft-kampanakis-curdle-pq-ssh-00. Work in Progress. Internet Engineering Task Force, Oct. 2020. 13 pp. url: https://datatracker.ietf.org/doc/html/draft-kampanakis-curdle-pq-ssh-00.

[LibreSSL24] LibreSSL. https://github.com/libressl/portable. v4.0.0. Oct. 2024.

[Libsodium13] Frank Denis. The Sodium cryptography library. June 2013. url: https://download.libsodium.org/doc/.

[LTAN+24] Sheran Lin, Jolene Tan, Ajanthan Asogamoorthy, Kyle Nekritz, Rafael Misoczki, and Sotirios Delimanolis. Post-quantum readiness for TLS at Meta. https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/. 2024.

[LY06] Chris M. Lonvick and Tatu Ylonen. The Secure Shell (SSH) Protocol Architecture. RFC 4251. Jan. 2006. doi: 10.17487/RFC4251. url: https://www.rfc-editor.org/info/rfc4251.

[Lyo24] Gordon Lyon. Nmap Network Mapper. 2024. url: https://nmap.org/.

[MABL+21] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Bidoux. Loïc, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Lacan. Jerome, Robert. Jean-Marc, and Pascal Veron. HQC Website. http//pqc-hqc.org/. [Accessed 22/08/2022]. 2021.

[Mar13] Moxie Marlinspike. Advanced Cryptographic Ratcheting. Signal Blog. Technical Whitepaper. Nov. 2013. url: https://signal.org/blog/advanced-ratcheting/.

[McE78] Robert J. McEliece. "A Public-Key System Based on Algebraic Coding Theory". In DSN Progress Report 44. Jet Propulsion Lab, 1978, pp. 114–116.

[Meta24] Meta. Fizz a TLS 1.3 Implementation. https://github.com/facebookincubator/fizz. v2024.08.19.00. Aug. 2024.

[Mil24] Jon Millican. "Shipping End-to-End Encryption to Billions". In Real World Crypto Symposium 2024. Contributed Talk. International Association for Cryptologic Research (IACR). Toronto, Canada, Mar. 2024.

[MJ21] Nikos Mavrogiannopoulos and Simon Josefsson. [Accessed 22/02/2022]. 2021. url: https://www.gnupg.org/index.html.

[MKJR16] Kathleen Moriarty, Burt Kaliski, Jakob Jonsson, and Andreas Rusch. PKCS #1 RSA Cryptography Specifications Version 2.2. RFC 8017. Nov. 2016. doi: 10.17487/RFC8017. url: https://www.rfc-editor.org/info/rfc8017.

[Moo24] Dustin Moody. Are We There Yet? An Update on the NIST PQC Standardization Project. https://csrc.nist.gov/csrc/media/Presentations/2024/update-on-the-nist-pqc-standardization-project/images-media/moody-are-we-there-yet-pqc-pqc2024.pdf. Accessed 2024-07-05. 2024.

[MP16] Moxie Marlinspike and Trevor Perrin. The X3DH Key Agreement Protocol. Signal Blog. Technical Wihtepaper. 2016. url: https://signal.org/docs/specifications/x3dh/.

[MP23] Michele Mosca and Marco Piani. 2023 Quantum Threat Timeline Report. https://globalriskinstitute.org/publications/2023-quantum-threat-timeline-report/. 2023.

[MvH20] Frank Muller and Maran van Heesch. Migration to Quantum-safe Cryptography. https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/trusted-ict/quantum/quantum-safe-crypto/. 2020.

[NCCoE23] National Cybersecurity Center of Excellence. Migration to Post-Quantum Cryptography. Quantum Readiness Cryptographic Discovery. Tech. rep. NIST SP 1800-38B. U.S. Department of Commerce, Dec. 2023. url: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

[NCSC-NL23] Dutch National Cyber Security Centre. Maak je organisatie quantumveilig. https://www.ncsc.nl/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig. 2023.

[NCSC-NL24] Dutch National Cyber Security Centre. Het crypto-agilitymonster op een bierviltje. https://www.ncsc.nl/actueel/weblog/weblog/2024/het-crypto-agilitymonster. Accessed: 20-06-2024. 2024.

[NCSC-UK20a] National Cyber Security Centre (NCSC-UK). Whitepaper: Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography. 2020.

[NCSC-UK20b] National Cyber Security Centre (NCSC-UK). Whitepaper: Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies. 2020.

[NCSC-UK22] National Cyber Security Centre (NCSC-UK). Government Cyber Security Strategy: 2022 to 2030. Accessed: 2024-07-08. 2022. url: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

[NCSC-UK23] National Cyber Security Centre (NCSC-UK). Next Steps in Preparing for Post-Quantum Cryptography. Accessed: 2024-07-08. 2023. url: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography.

[NCTV22] AIVD, MIVD, and NCTV. Dreigingsbeeld Statelijke Actoren 2. https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2. 2022.

[Nettle24] Nettle. https://git.lysator.liu.se/nettle/nettle. v3.10. June 2024.

[NIST01a] National Institute of Standards and Technology. FIPS 197 Advanced encryption standard (AES). Standard. FIPS 197. Gaithersburg, MD: NIST, Nov. 2001.

[NIST01b] National Institute of Standards and Technology. FIPS 197: Advanced encryption standard (AES). Standard. FIPS 197. Gaithersburg, MD: NIST, Nov. 2001.

[NIST02] National Institute of Standards and Technology. Announcing Approval of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard; a Revision of FIPS 180-1. Notice. NIST, Aug. 2002.

[NIST08] National Institute of Standards and Technology. FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC). Standard. Gaithersburg, MD: NIST, July 2008.

[NIST12] Quynh Dang. Recommendation for Applications Using Approved Hash Algorithms. Special Publication. SP 800-107 Rev. 1. Gaithersburg, MD: NIST, Aug. 2012.

[NIST15a] National Institute of Standards and Technology. FIPS 180-4 Secure Hash Standard (SHS). Standard. FIPS 180-4. Gaithersburg, MD: NIST, Aug. 2015.

[NIST15b] National Institute of Standards and Technology. FIPS 202 SHA-3 Standard Permutation-Based Hash and Extendable-Output Functions. Standard. Gaithersburg, MD: NIST, Aug. 2015.

[NIST16a] Morris Dworkin. Recommendation for Block Cipher Modes of Operation the CMAC Mode for Authentication. Special Publication. SP 800-38B. Gaithersburg, MD: NIST, June 2016.

[NIST16b] National Institute of Standards and Technology. Report on Post-Quantum Cryptography. Tech. rep. National Institute of Standards and Technology Internal Report 8105 15 pages (April 2016). Washington, D.C.: U.S. Department of Commerce, 2016. doi: 10.6028/NIST.IR.8105.

[NIST16c] National Institute of Standards and Technology. IR8105: Report on Post-Quantum Cryptography. Tech. rep. National Institute of Standards and Technology Internal Report 8105 15 pages (April 2016). Washington, D.C.: U.S. Department of Commerce, 2016. doi: 10.6028/NIST.IR.8105.

[NIST19a] Elaine Barker, Lily Chen, Allen Roginsky, Apostol Vassilev, Richard Davis, and Scott Simon. Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. Special Publication. SP 800-56B. Gaithersburg, MD: NIST, Mar. 2019.

[NIST19b] National Institute of Standards and Technology. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Tech. rep. National Institute of Standards and Technology Internal Report 8240, 27 pages (January 2019). Washington, D.C.: U.S. Department of Commerce, 2019. doi: 10.6028/NIST.IR.8240.

[NIST19c] National Institute of Standards and Technology. FIPS 140-3: Security Requirements for Cryptographic Modules. Standard. FIPS 140-3. Gaithersburg, MD: NIST, Mar. 2019.

[NIST20a] David Cooper, Daniel Apon, Quynh Dang, Michael Davidson, Morris Dworkin, and Carl Miller. Recommendation for Stateful Hash-Based Signature Schemes. Special Publication. Gaithersburg, MD: NIST, Oct. 2020.

[NIST20b] National Institute of Standards and Technology. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Tech. rep. National Institute of Standards and Technology Interagency or Internal Report 8309, 39 pages (July 2020). Washington, D.C.: U.S. Department of Commerce, 2020. doi: 10.6028/NIST.IR.8309.

[NIST21] National Institute of Standards and Technology. Getting Ready for Post-Quantum Cryptography Exploring Challenges associated with Adopting and Using Post-quantum Cryptographic Algorithms. Tech. rep. Washington, D.C.: U.S. Department of Commerce, 2021. doi: 10.6028/NIST.CSWP.04282021.

[NIST22] National Institute of Standards and Technology. IR8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Proces. Tech. rep. National Institute of Standards and Technology Interagency or Internal Report NIST IR 8413-upd1, 102 pages (July 2022). Washington, D.C.: U.S.

[NIST23] National Institute of Standards and Technology. FIPS 186-5: Digital Signature Standard (DSS). Standard. FIPS 186-5. Gaithersburg, MD: NIST, Feb. 2023.

[NIST24a] National Institute of Standards and Technology. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard. Standard. Gaithersburg, MD: NIST, Aug. 2024. url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf.

[NIST24b] National Institute of Standards and Technology. FIPS204 Module-Lattice-Based Digital Signature Standard. Standard. Gaithersburg, MD: NIST, Aug. 2024. url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf.

[NIST24c] National Institute of Standards and Technology. FIPS205 Stateless Hash-Based Digital Signature Standard. Standard. Gaithersburg, MD: NIST, Aug. 2024. url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf.

[NL18] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. June 2018. doi: 10.17487/RFC8439. url: https://www.rfc-editor.org/info/rfc8439.

[NLNCSA21] Netherlands National Communications Security Agency (NLNCSA). Bereid je voor op de dreiging van quantumcomputers. https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers. 2021.

[NSA21a] National Security Agency (NSA). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). NSA Announcement, 19 July 2021. 2021. url: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.

[NSA21b] NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. 2021.

[OBr23] Devon O'Brien. Protecting Chrome Traffic with Hybrid Kyber KEM. 2023. url: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.

[OGPK+24a] Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, and Scott Fluhrer. Composite ML-DSA for use in Internet PKI. Internet-Draft draft-ietf-lamps-pq-composite-sigs-02. Work in Progress. Internet Engineering Task Force, July 2024. 51 pp. url: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/02/.

[OGPK+24b] Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, and Scott Fluhrer. Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS. Internet-Draft draft-ietf-lamps-pq-composite-kem-04. Work in Progress. Internet Engineering Task Force, July 2024. 42 pp. url: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/04/.

[OPAB+19] David Ott, Christopher Peikert, Reza Azarderakhsh, Shannon Beck, Andy Bernat, Matt Campagna, Khari Douglas, Ann Drobnis, Roberta Faux, Shay Gueron, Shai Halevi, Peter Harsha, Mark Hill, Jeff Hoffstein, David Jao, Sandip Kundu, Hugo Krawczyk, Brian LaMacchia, Susan Landau, David McGrew, Ilya Mironov, Rafael Misoczki, Dustin Moody, Kenny Paterson, Radia Perlman, Tom Ristenpart, Vladimir Soukharev, Helen Wright, and Rebecca Wright. "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility". In CoRR abs/1909.07353 (2019).

[OpenSSL03] The OpenSSL Project. OpenSSL The Open Source toolkit for SSL/TLS. Apr. 2003. url: https://www.openssl.org/.

[OQS S/MIME24] OQS S/MIME. Open Quantum Safe CMS and S/MIME Fork. https://openquantumsafe.org/applications/smime.html. Oct. 2024.

[OQS23] Open Quantum Safe (OQS). OQS algorithm performance visualizations. https://openquantumsafe.org/benchmarking/. 2023.

[OQS24] Open Quantum Safe. liboqs v0.11.0. https://github.com/open-quantum-safe/liboqs. Sept. 2024.

[OQSprovider24] OQSProvider. Open Quantum Safe provider for OpenSSL - v0.7.0. https://github.com/open-quantum-safe/oqs-provider. Oct. 2024.

[OWA24] OWASP. OWASP CycloneDX Authoritative Guide to CBOM. Accessed 2024-07-01. 2024. url: https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf.

[PCI22] PCI Security Standards Council. Payment Card Industry Data Security Standard (PCI DSS) Version 4.0. url: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf. Accessed 2024-06-19. Mar. 2022.

[PQClean23] Matthias J. Kannwischer, Peter Schwabe, Douglas Stebila, and Thom Wiggers. PQClean. https://github.com/PQClean/PQClean. Apr. 2023.

[RCDB24] Prasanna Ravi, Anupam Chattopadhyay, Jan Pieter D'Anvers, and Anubhab Baksi. "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results". In: 23.2 (Mar. 2024). doi: 10.1145/3603170. url: https://doi.org/10.1145/3603170.

[Res18] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Aug. 2018. doi: 10.17487/RFC8446. url: https://www.rfc-editor.org/info/rfc8446.

[Res24] Santander Security Research. CryptoBOM Forge. Accessed 2024-07-02. 2024. url: https://github.com/Santandersecurityresearch/cryptobom-forge.

[Rou24] Sebastien Rousseau. KyberLib. https://github.com/sebastienrousseau/kyberlib. v0.0.6. May 2024.

[Rust24] Joseph Birr-Pixton. RustTLS. https://github.com/rustls/rustls. v0.23.12. July 2024.

[SA15] Markku-Juhani O. Saarinen and Jean-Philippe Aumasson. The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). RFC 7693. Nov. 2015. doi: 10.17487/RFC7693. url: https://www.rfc-editor.org/info/rfc7693.

[Sho94] Peter W. Shor. “Algorithms for Quantum Computation Discrete Logarithms and Factoring”. In FOCS. IEEE Computer Society, 1994, pp. 124–134.

[Signal24a] Signal. Quantum Resistance and the Signal Protocol. Signal Blog. 2024. url: https://signal.org/blog/pqxdh/.

[Signal24b] Signal. The PQXDH Key Agreement Protocol. Jan. 2024. url: https://signal.org/docs/specifications/pqxdh/.

[SM16] Douglas Stebila and Michele Mosca. “Post-quantum key exchange for the internet and the open quantum safe project”. In International Conference on Selected Areas in Cryptography. Springer. 2016, pp. 14–37.

[SRT19] Jim Schaad, Blake C. Ramsdell, and Sean Turner. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. RFC 8551. Apr. 2019. doi: 10.17487/RFC8551. url: https://www.rfc-editor.org/info/rfc8551.

[SSW20] Peter Schwabe, Douglas Stebila, and Thom Wiggers. “Post-Quantum TLS Without Handshake Signatures”. In CCS ’20 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM, 2020, pp. 1461–1480. doi: 10.1145/3372297.3423350. url: https://doi.org/10.1145/3372297.3423350.

[Ste] Marc Stevens. pqc benchmarking. Accessed: 14 October 2024. url: https://github.com/cr-marc-stevens/pqc_benchmarking.

[SvdBFG+12] Andrey Sidorenko, Joachim van den Berg, Remko Foekema, Michiel Grashuis, and Jaap de Vos. Bellcore attack in practice. Cryptology ePrint Archive, Paper 2012/553. 2012. url: https://eprint.iacr.org/2012/553.

[TC24] TNO and CWI. PQChoiceAssistant. https://tno.github.io/PQChoiceAssistant/. Accessed 2024-07-18. 2024.

[TGFK+18] Alexander Truskovsky, Daniel Van Geest, Scott Fluhrer, Panos Kampanakis, Mike Ounsworth, and Serge Mister. Multiple Public-Key Algorithm X.509 Certificates. Internet-Draft draft-truskovsky-lamps-pq-hybrid-x509-01. Work in Progress. Internet Engineering Task Force, Aug. 2018. 24 pp. url: https://datatracker.ietf.org/doc/draft-truskovsky-lamps-pq-hybrid-x509/01/.

[Uni02] United States Congress. Federal Information Security Management Act of 2002 (FISMA). Public Law 107-347, 107th Congress. 2002. url: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma.

[US22] US White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. 2022. url: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[US24] Executive Office of the President of the United States. Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No 117-260. 2024. url: https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

[US96] United States Congress. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191, 104th Congress. 1996. url: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

[VK19] Luke Valenta and Kris Kwiatkowski. The TLS Post-Quantum Experiment. 2019. url: https://blog.cloudflare.com/the-tls-post-quantum-experiment.

[WBKG+24] Thom Wiggers, Kaveh Bashiri, Stefan Kölbl, Jim Goodman, and Stavros Kousidis. Hash-based Signatures State and Backup Management. Internet-Draft draftwiggers-hbs-state-00. Work in Progress. Internet Engineering Task Force, Feb. 2024. 20 pp. url: https://datatracker.ietf.org/doc/draft-wiggers-hbs-state/00/.

[Wei21] Adam Weinberg. Analysis of top 11 cyber attacks on critical infrastructure. https://www.first-point-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/. [Accessed 05/04/2022]. 2021.

[Wes21] Bas Westerbaan. Sizing Up Post-Quantum Signatures. 2021. url: https://blog.cloudflare.com/sizing-up-post-quantum-signatures.

[Wet24] Dirk Wetter. testssl.sh. https://testssl.sh/. v3.0.9. June 2024.

[Wha16] WhatsApp. WhatsApp Encryption Overview. Technical Whitepaper. Apr. 2016. url: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

[Wir24] Wireshark Foundation. Wireshark Network Protocol Analyzer. 2024. url: https://www.wireshark.org/.

[Wol24a] WolfSSL. Embedded SSL/TLS Library. https://github.com/wolfSSL/wolfssl. v5.7.2. July 2024.

[Wol24b] Inc. WolfSSL. wolfCrypt Embedded Crypto Engine. 2024. url: https://www.wolfssl.com/wolfcrypt/.

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

Revised and Extended Second Edition

AIVD | CWI | TNO